Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

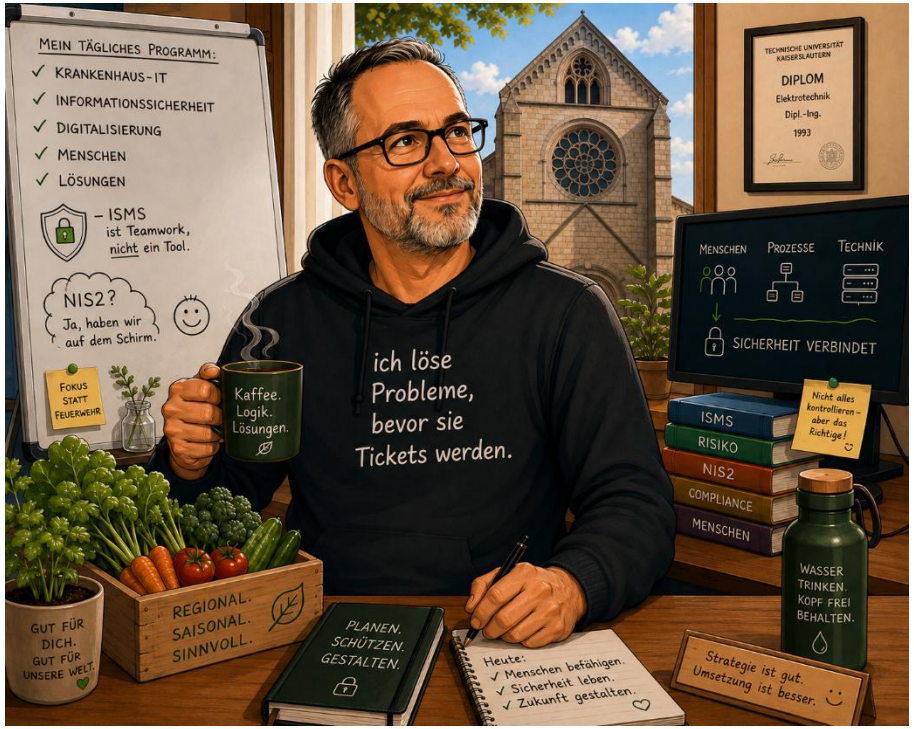
Cybersicherheit und NIS-2-Richtlinie

Resiliente Kliniken: Sicherheit als Führungsaufgabe

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

Vorstellung



Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

Einführung

Quelle: BDO/DKI-Studie 2025: Cybersicherheit im Krankenhaus, S. 6, 10–13

Einführung


Nicht jeder Sicherheitsvorfall ist ein Cyberangriff.
Informationssicherheitsvorfälle können viele Ursachen haben.
MENSCH
Fehlbedienung
Fehlkonfiguration
falsche Berechtigung
TECHNIK
Hardwaredefekt
Softwarefehler
Strom-/Netzwerk-ausfall
ANGRIFF
Phishing
Malware
Ransomware
DRITTE
Cloud
Dienstleister
Lieferkette
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
Phishing
Täuschung
Ransomware
Erpressung
RANSOMWARE
DDoS
Überlastung
Hacker
Unbefugter Zugriff
Cyber-Risiken
Systemfehler
Technische Störungen
Update-Pfusch
Fehlerhafte Updates
Menschlicher Fehler
Unachtsamkeit & Fehlbedienung
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.

Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

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 BSI-Gesetzes
am 6. 12.2025 um.

Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

Roadmap durch das BSIG

Die wichtigsten Paragraphen.

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§28 - Einrichtungsarten

§28 BSIG – Einordnung von Einrichtungen

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

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. €**

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


Krankenhäuser

Universitätskliniken


Rehabilitationskliniken


Medizinische Versorgungszentren (MVZ)


Arztpraxen


Zahnarztpraxen


Dialysezentren


Labore (medizinische Labore)


Physiotherapie-, Ergotherapie- oder Logopädiepraxen


Hebammenpraxen


Apotheken (für die Abgabe von Arzneimitteln)


Pflegeeinrichtungen (in der Regel nicht)

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§28 - Sind Sie betroffen?

PRÜFUNG: BESONDERS WICHTIGE EINRICHTUNG

START

1 Bin ich ein Betreiber einer kritischen Anlage?
- JA → BESONDERS WICHTIGE EINRICHTUNG
- NEIN ↓

2 Zähle ich zu einer in der Anlage 1 BSIG nach Sektoren geliederten Einrichtungsart?
- NEIN → KEINE BESONDERS WICHTIGE EINRICHTUNG. Prüfung notwendig, ob wichtige Einrichtung!
- JA ↓

3 Habe ich mehr als 250 Mitarbeitende?
- JA → BESONDERS WICHTIGE EINRICHTUNG
- NEIN ↓

4 Habe ich einen Jahresumsatz von über 50 Mio. € UND zudem eine Jahresbilanzsumme von über 43 Mio. €?
- JA → BESONDERS WICHTIGE EINRICHTUNG
- NEIN → KEINE BESONDERS WICHTIGE EINRICHTUNG. Prüfung notwendig, ob wichtige Einrichtung!

→ JA = weiter / Ergebnis erreicht
→ NEIN = weiter zur nächsten Frage bzw. andere Prüfung notwendig

PRÜFUNG: WICHTIGE EINRICHTUNG

START

1 Zähle ich zu einer in der Anlage 1 und Anlage 2 BSIG nach Sektoren geliederten Einrichtungsart?
- NEIN → KEINE WICHTIGE EINRICHTUNG
- JA ↓

2 Habe ich mehr als 50 Mitarbeitende?
- JA → WICHTIGE EINRICHTUNG
- NEIN ↓

3 Habe ich einen Jahresumsatz von über 10 Mio. € UND zudem eine Jahresbilanzsumme von über 10 Mio. €?
- JA → WICHTIGE EINRICHTUNG
- NEIN → KEINE WICHTIGE EINRICHTUNG

→ JA = weiter / Ergebnis erreicht
→ NEIN = weiter zur nächsten Frage bzw. anderes Ergebnis

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§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

KRANKENHAUS MUSTERSTADT
z. B. GmbH
HRB 123456

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.

BSI | BBK

MVZ
§ 28 BSIG

natürliche oder **juristische** Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft

MVZ

Eigenständige Registrierung

- Eigenständige juristische Person
- Eigenständige Verantwortung nach § 28 BSIG
- Abhängigkeit Krankenhaus bzgl. der Size-Cap-Rule

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§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

- 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

- 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

- 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

Schutz der Systeme | Schutz der Daten | Schutz der Menschen | Schutz der Prozesse | Resilienz und Vertrauen stärken

Impliziert

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§30 – Maßnahmen

1 Risikoanalyse und Sicherheit in der Informationstechnik

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

4 RISIKOBEHANDLUNGSMÖGLICHKEITEN

Ziel jeder Risikobehandlung: Risiken auf ein akzeptables Niveau bringen und den Wert sowie die Erreichung der Ziele schützen.

Kontext
Analyse von
- Internen & externen Einflüssen
- Anforderungen
- Stakeholder

Assets
- Assets identifizieren
- Schutzbedarf feststellen
- Bedrohungen & Schwachstellen identifizieren
- Schwachstellen erkennen

Bewertung
- Risikoeigentümer festlegen
- Eintrittswahrscheinlichkeit & Schadensauswirkung
- Risikomatrix
- Risikoakzeptanzkriterien definieren

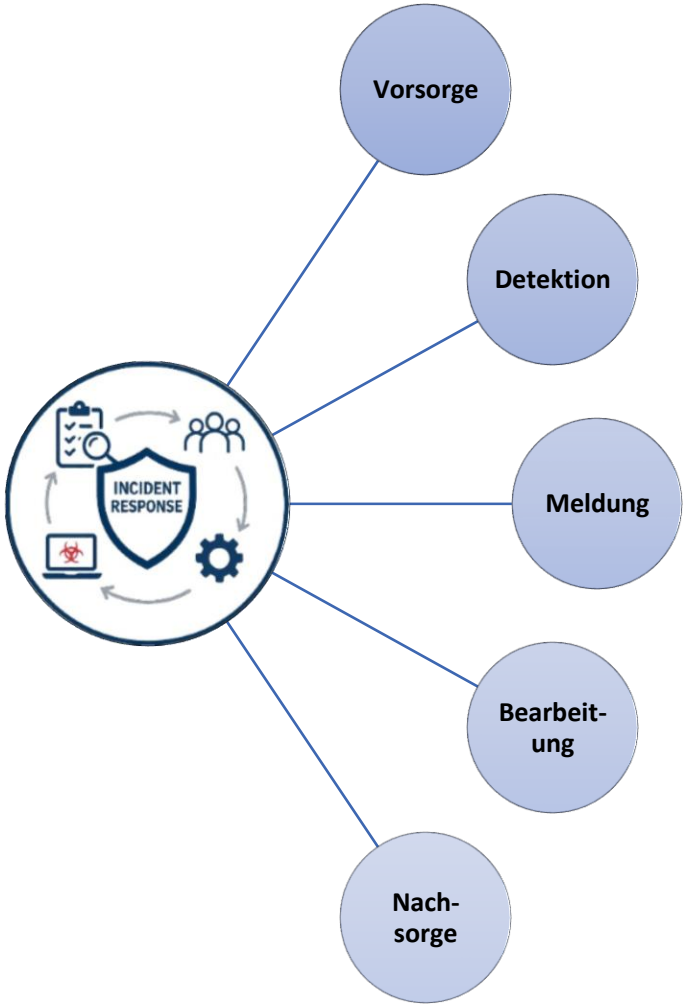
Behandeln
Das Risiko behandeln durch
- Vermeiden
- Verringern
- Übertragen
- Akzeptieren

Dokumentieren
- Ergebnisse der Risikoanalyse
- Nachvollziehbarkeit
- Auditrelevant

Überwachen
- Risiken und Maßnahmen überprüfen
- Regelhaft / kontinuierlich
- Nach Vorfällen
- Nach Änderungen in der Organisation

2 Bewältigung von Sicherheitsvorfällen

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



Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

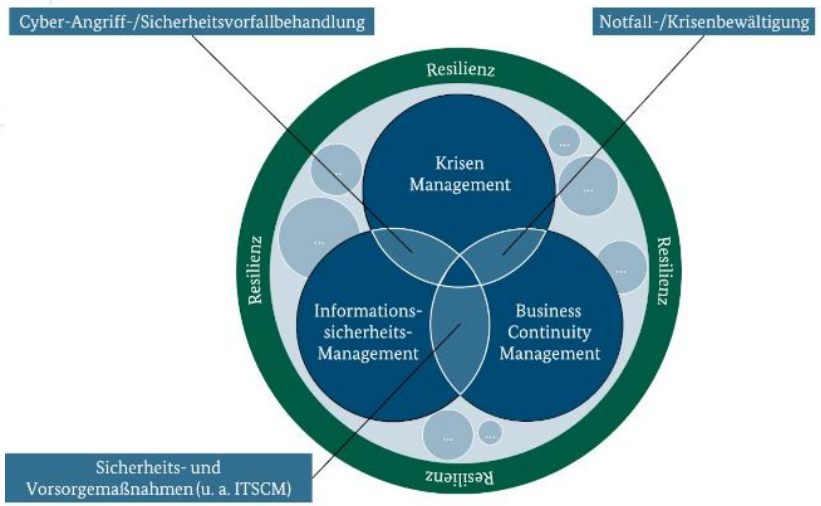
§30 – Maßnahmen

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



Cyber-Supply Chain Risk Management (C-SCRM)

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

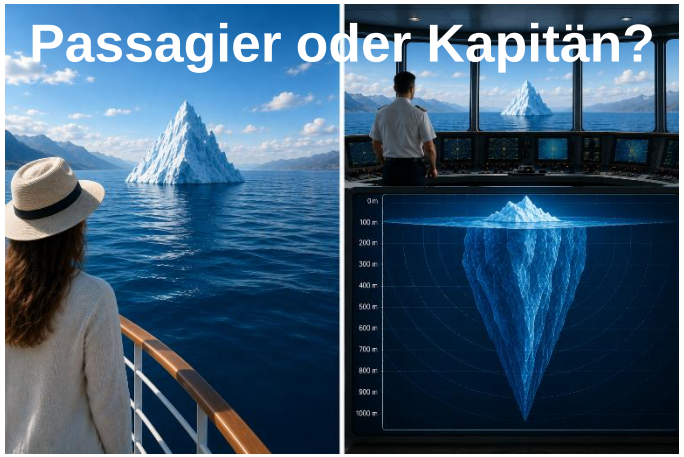
§30 – Maßnahmen

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



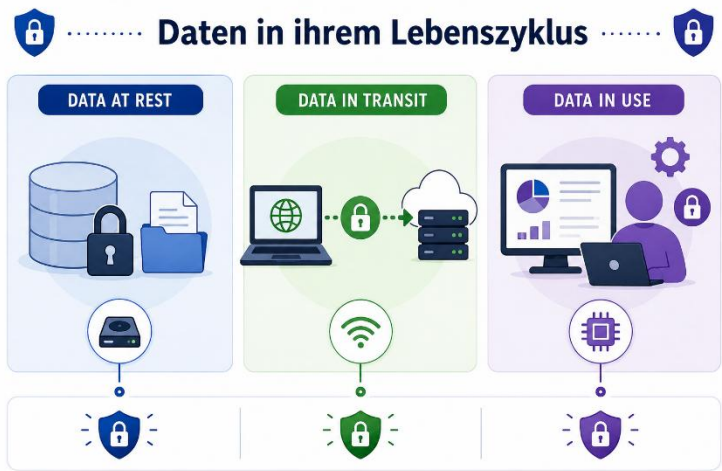
Regelmäßiger Managementtermin?

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

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§30 – Maßnahmen



Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§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

10 Multi-Faktor-Authentifizierung & gesicherte Kommunikation

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

2FA – ZWEI-FAKTOR-AUTHENTIFIZIERUNG

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

MFA – MULTI-FAKTOR-AUTHENTIFIZIERUNG

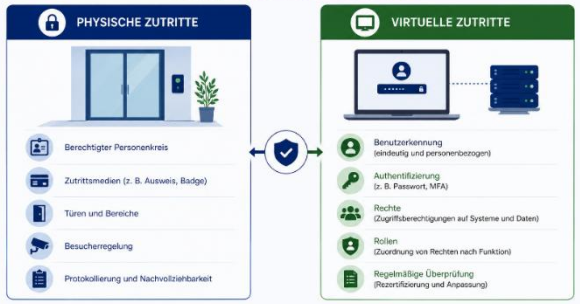
Drei oder mehr verschiedene Faktoren müssen bereitgestellt werden, um Zugriff zu erhalten.

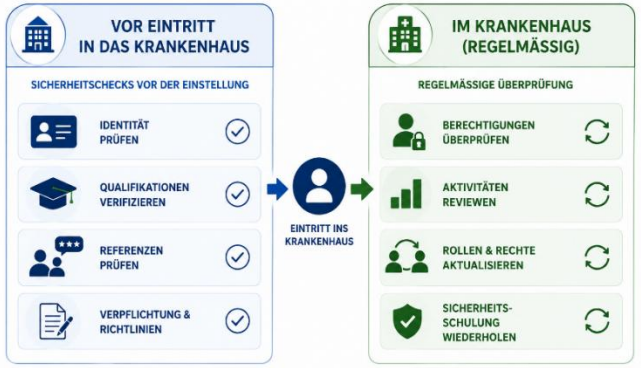
AUTHENTICATOR-APPS: SO FUNKTIONIERT ES

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

ZUTRITTSREGELUNGEN

PHYSISCHE UND VIRTUELLE ZUTRITTE





Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§32 Meldepflichten in Detail

§32 Meldepflichten

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

Meldepflicht für „erhebliche Sicherheitsvorfälle"

1. Schwerwiegende Betriebsstörung
2. Erhebliche wirtschaftliche Schäden
3. Erhebliche Schäden an Dritten

Die Meldefristen im Überblick

Sicherheitsvorfall erkannt (Stunde 0)

1. **Innerhalb 24 Stunden** – Erstmeldung absetzen
2. **Innerhalb 72 Stunden** – Meldung mit Bewertung
3. **Spätestens 1 Monat** – Abschlussmeldung

Interner Meldeweg – unsere Schritte

1. **Vorfallerkennen** – Hinweise und Ereignisse wahrnehmen und einordnen.
2. **Meldung über den internen Meldeweg** – An die zuständigen Personen.
3. **Vorfall prüfen und bewerten** – Relevanz, Schweregrad und Meldepflicht feststellen.
4. **Vorfall und Vorfallprüfung dokumentieren** – Vollständig und nachvollziehbar.
5. **Vorfall im BSI-Portal melden** – Innerhalb 24 Stunden Erstmeldung absetzen (weitere Meldungen gemäß Fristen).

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

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

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§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

Hosp.DO.IT Hospitalgemeinschaft 10 Jahre JUBILÄUM

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§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

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§65 - Bußgelder

2 Bußgeldtatbestände (Beispiele)

Tatbestand	Rechtsgrundlage (§ 65 BSIG)	Höchst Bußgeld: Besonders wichtige Einrichtungen	Höchst Bußgeld: 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.

Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

Fazit

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

Aber auch eine mächtige Behörde

Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

Fazit

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

Geben Sie Ihren Mitarbeitenden den Freiraum zum üben.

Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

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.**

Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

Vielen Dank für Ihre Aufmerksamkeit

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.

Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

Das BSIG – 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 - BSIG) - 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	

Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§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 einen 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 getroffenen 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/

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§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 Risikomanagement-maßnahmen 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 gesellschafts-rechtlichen Bestimmungen keine Haftungs-regelung 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 Risiko-managementpraktiken im Bereich der IT-Sicherheit.

Auswirkungen beurteilen

Die Auswirkungen von Risiken und Risikomanagement-praktiken auf die von der Einrichtung erbrachten Dienste beurteilen.

Regelmäßig schulen

Regelmäßige Teilnahme an Schulungen sicherstellen und Kenntnisse aktuell halten.

Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

§61 – Rechte BSI

8 Weitere Anordnungen gegenüber besonders wichtigen Einrichtungen

Das Bundesamt

§35 Unterrichtungspflichten

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:

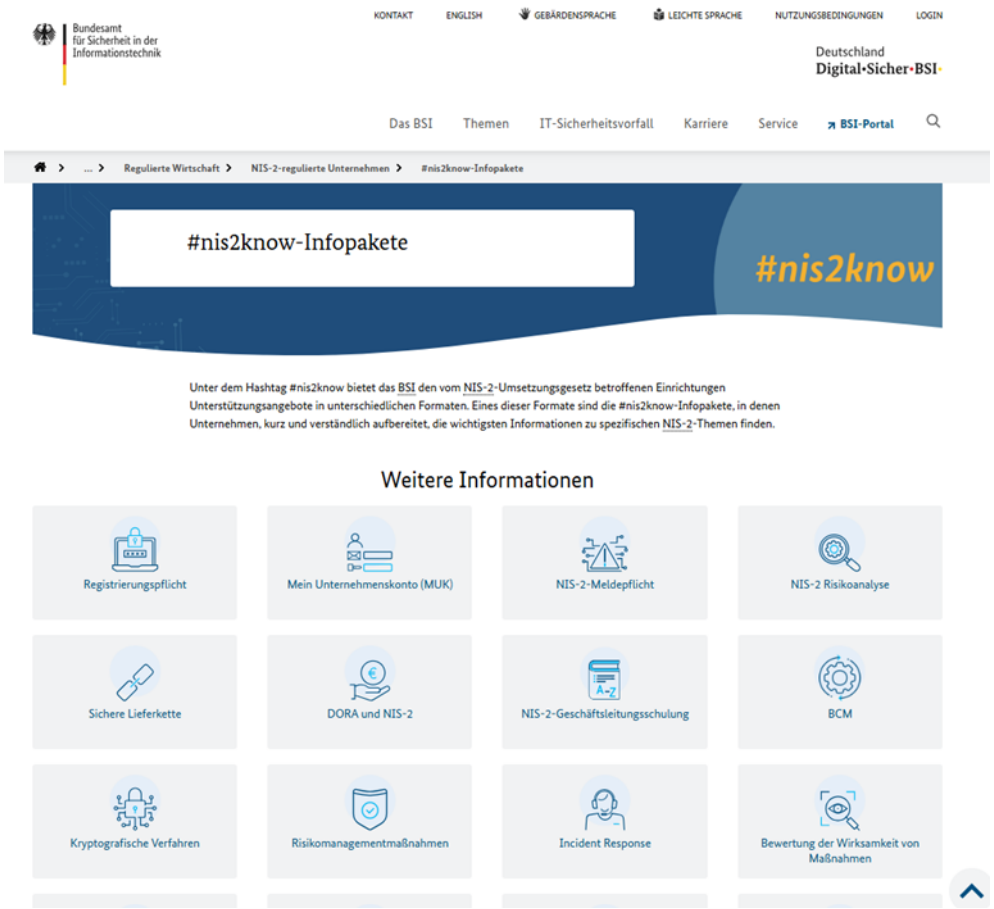
1. die erteilte Genehmigung nach dem jeweiligen Fachrecht vorübergehend ganz oder teilweise aussetzen.
2. unzuverlässigen Geschäftsleitungen die Ausübung der Tätigkeit, zu der sie berufen sind (§ 2 Nr. 13), vorübergehend untersagen.

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.

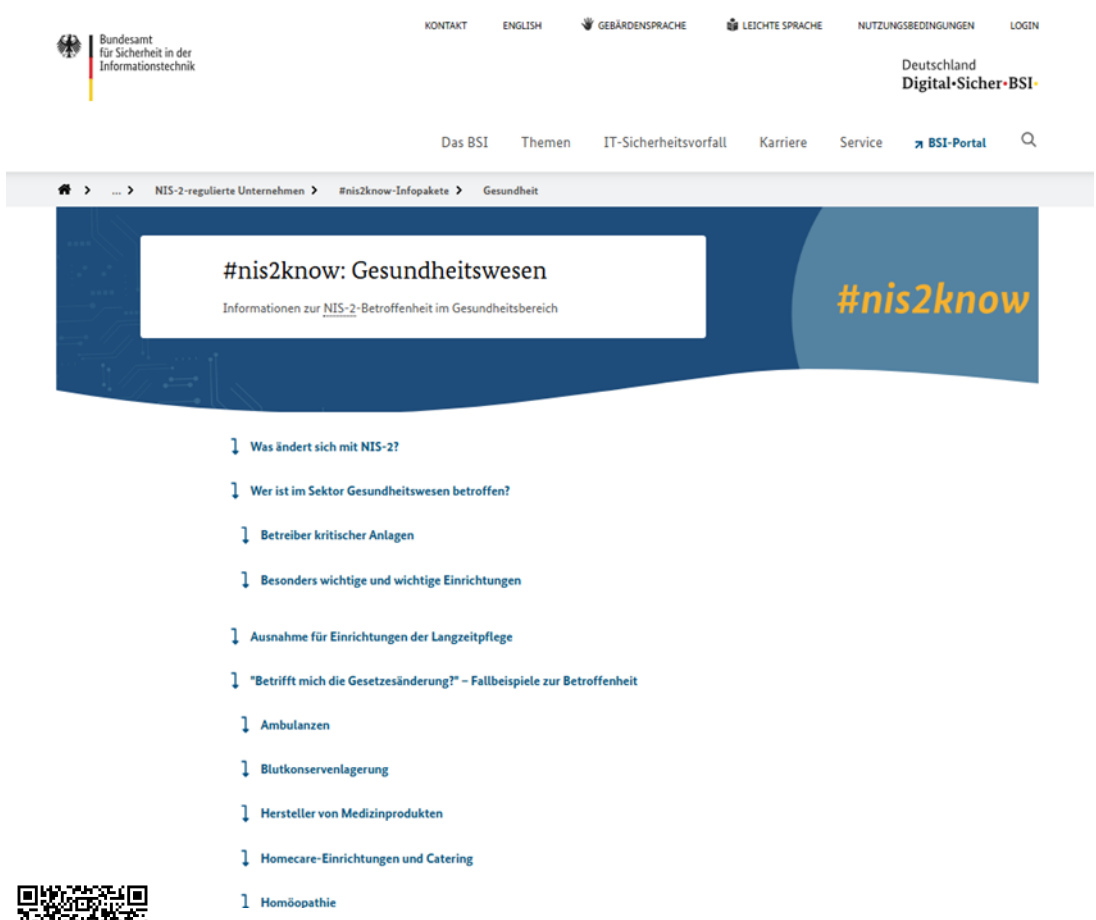
Westpfalz-Klinikum GmbH

Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

BSI - #nis2know-Infopakete



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



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

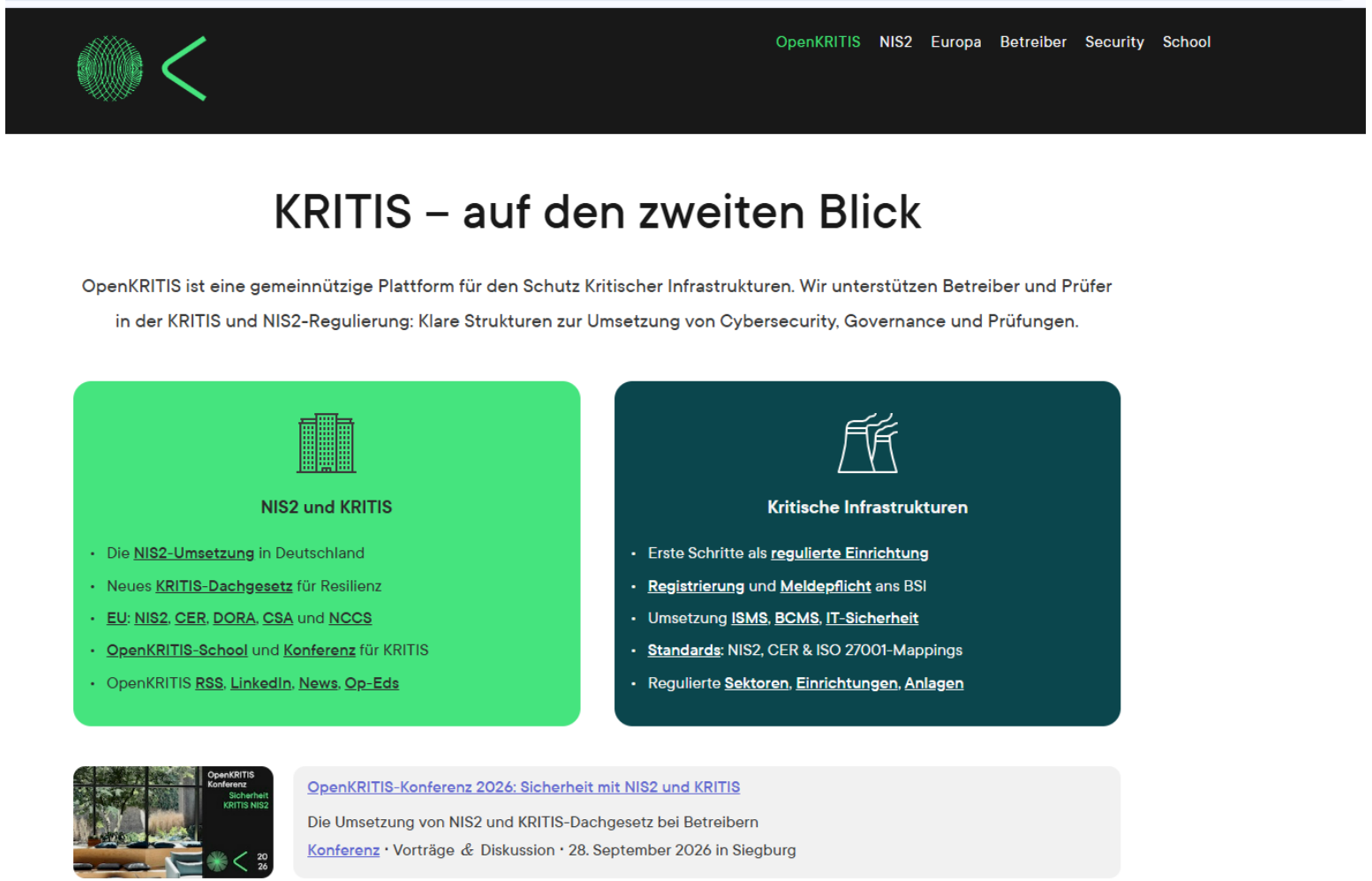
Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

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/



Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

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

Westpfalz-Klinikum GmbH
Akademisches Lehrkrankenhaus der Universitäten Mainz und Heidelberg

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/