BW Bildungswesen

indevis

DAS CYBERSECURITY-PLAYBOOK FÜR BILDUNGSEINRICHTUNGEN

Eine Checkliste für Schulleitungen, IT-Verantwortliche, Datenschutzbeauftragte und Bildungsministerien

Warum dieses Playbook?

Ein Cyberangriff kann in Sekunden zerstören, was Bildungseinrichtungen über Jahre aufgebaut haben.
Fällt die IT von Lernplattformen oder Verwaltungssystemen aus, sind Unterricht, Prüfungen und Forschung unmittelbar betroffen – mit Folgen für ganze Semester oder Forschungsprojekte.

Laut dem IBM Cost of a Data Breach Report 2024 kostet eine Datenpanne im Bereich Higher Education & Training im Schnitt rund **3,4 Mio. Euro** pro Vorfall – einer der höchsten Werte weltweit.[1] Trotzdem bieten nur etwa **30 %** der Hochschulen Sicherheitsschulungen für Mitarbeitende und **10 %** für Studierende an, obwohl fast **97 %** der Hochschulleitungen Cyberangriffe als großes Risiko einschätzen.[2] Dieser Mangel an Awareness macht den Bildungssektor zu einem besonders attraktiven Ziel für Angreifer.

Die Erfahrung zeigt: Angriffe auf Bildungseinrichtungen nehmen zu und können für Träger und Hochschulen existenzgefährdend sein. Wochenlange IT-Ausfälle beeinträchtigen nicht nur den Bildungsbetrieb, sondern auch die Reputation und das Vertrauen von Studierenden, Eltern und Förderern. Zusätzlich steigen die Anforderungen durch DSGVO und für Hochschulen und Forschung durch die NIS-2-Richtlinie.

Cybersicherheit ist daher keine Option mehr, sondern eine notwendige Investition in die Zukunftsfähigkeit des Bildungswesens.

Für Entscheidungsträger im Bildungswesen ist es heute wichtiger denn je zu erkennen: Mangelnde Cyber-Resilienz stellt ein existenzielles Risiko für Schulen, Hochschulen und Forschungseinrichtungen dar.

Die Incident-Response- und Threat-Intelligence-Teams von indevis haben hunderte Angriffe auf öffentliche Einrichtungen, Universitäten und Bildungsorganisationen analysiert und daraus die wichtigsten Lehren gezogen – einschließlich Maßnahmen, die sich viele Einrichtungen im Nachhinein gewünscht hätten. Dieses Playbook fasst diese Erkenntnisse zusammen und bietet eine praxisorientierte Anleitung, wie sich Bildungseinrichtungen auf Cyber-Vorfälle vorbereiten, sie bewältigen und erfolgreich überstehen können.

Neben einer fünfstufigen Checkliste, die Ihnen hilft, Cyber-Resilienz systematisch aufzubauen, erhalten Sie mit der Cyber-Sicherheitsampel ein Instrument zur schnellen Bewertung des Sicherheitsstatus Ihrer Einrichtung.

Business Impact: Cybersecurity als Garant für Bildungs- und Forschungskontinuität

Cybersecurity ist im Bildungswesen längst vom IT-Thema zum strategischen Überlebensfaktor geworden. Fehlende Schutzmaßnahmen verursachen nicht nur hohe Kosten, sondern gefährden Unterricht, Prüfungen und Forschung.

Die Universität Duisburg-Essen musste Ende 2022 nach einem Ransomware-Angriff ihren Lehr- und Verwaltungsbetrieb **über Wochen** stark einschränken: gestohlene Daten tauchten im Darknet auf, mit gravierenden Folgen für Studierende und Mitarbeitende.[3]

Noch kritischer sind Angriffe, die ganze IT-Infrastrukturen lahmlegen. So waren Anfang 2025 in Rheinland-Pfalz rund **45** Schulen betroffen, nachdem ein externer IT-Dienstleister Opfer eines Ransomware-Angriffs wurde. Für mehrere Tage waren die Schulen offline und konnten digitale Dienste nicht nutzen.[4]

77 %

betrug der Anstieg der wöchentlichen Angriffe auf Bildungseinrichtungen in Deutschland – auf durchschnittlich 2.041 pro Woche.[5]

85%

der Ransomware-Angriffe auf Schulen führten 2024 zur erfolgreichen Datenverschlüsselung (bei Hochschulen 77 %).[6]

Nachweisbare Compliance – etwa durch ISO 27001 oder die Einhaltung von DSGVO- und NIS-2-Vorgaben, stärkt das Vertrauen von Schüler:innen, Studierenden, Eltern und Förderern. Studien zeigen: Für Bildungseinrichtungen sind etablierte Cybersecurity-Standards entscheidend, um den Bildungsbetrieb zu sichern und Reputation sowie Fördermittel langfristig zu erhalten.

„Einhundert Prozent Cybersicherheit gibt es nicht und wird es nie geben. Die Frage ist deswegen nicht ob, sondern wann ein erfolgreicher Cyberangriff stattfindet. Wir müssen das Cybersicherheitsniveau in Deutschland daher insgesamt substantiell erhöhen.“[7]

Claudia Plattner, BSI-Präsidentin

Cybersecurity in 5 Schritten

Cyber-Resilienz ist heute ein zentraler Pfeiler verantwortungsvoller Leitung - besonders für Schulen, Hochschulen und andere Bildungseinrichtungen.
Wer Cyber-Risiken wirksam steuern will, darf sie nicht isoliert als reines IT-Thema betrachten, sondern muss sie fest im strategischen Steuerungsrahmen der Einrichtung verankern. Genau hier setzt unsere Checkliste an: Sie bietet Entscheidungsträger:innen einen klaren, praxisnahen Fahrplan, um Cyber-Resilienz systematisch aufzubauen, Risiken zu minimieren und die Kontinuität von Unterricht, Prüfungen und Forschung dauerhaft zu sichern.

Cyber-Risiken in die Leitungs- und Verwaltungsstrukturen integrieren

Cyber-Resilienz beginnt in der Leitung. Damit Sicherheitsfragen nicht isoliert in der IT betrachtet werden, sollte die Hochschul- bzw. Schulleitung gemeinsam mit der Verwaltung ein Governance-Modell etablieren, in dem Cyber-Risiken als fester Bestandteil der Gesamtsteuerung verankert sind. Die Verantwortung für Cybersicherheit muss klar zugewiesen, regelmäßig überprüft und in Leitungs- bzw. Gremiensitzungen sichtbar gemacht werden.

Kernmaßnahmen zur Umsetzung:

Durchführung einer Cyber-Resilience- / Risikoanalyse (CRA)

- Einschätzung der Sicherheitslage mittels Threat-Led Profiling
- Gap-Analyse zur Abdeckung bestehender Risiken durch die Cyber-Versicherung
- Penetrationstests zur Validierung der Verteidigungsmechanismen
- Klassifizierung technischer Risiken nach der OWASP Top 10 Infrastructure Security Risks, z. B. unzureichende Zugangskontrollen, fehlende Netzwerksegmentierung, unsichere Standardkonfigurationen, schwaches Patch-Management
- Bewertung der identifizierten Bedrohungen anhand von Eintrittswahrscheinlichkeit und wirtschaftlichem Schaden

Einführung eines quartalsweisen Cyber-Reportings zur

- Analyse der aktuellen Bedrohungslage
- Bewertung von Erkennungsleistung und Resilienzgrad
- Aktualisierung von Notfallplänen und Reaktionsrichtlinien

2. Cyber-Resilienz-Strategie entwickeln

Eine gute Strategie erkennt nicht nur Risiken – sie priorisiert, schützt, reagiert und stellt im Ernstfall alles wieder her. Das Ziel ist eine Resilienzarchitektur, die dem Prinzip folgt: „Identify, Protect, Detect, Respond, Recover."

Vorgehensweise:

Risikoanalyse und Bedrohungsbewertung durchführen

- Risiken identifizieren und quantifizieren
- Finanzielle, operative und reputationsbezogene Auswirkungen erfassen
- Berichte als Grundlage für Investitionsentscheidungen nutzen (NCSC-Empfehlungen)

Prioritäten und Ressourcen festlegen

- Höchste Risiken priorisieren und ressourcenschonend adressieren
- Investitionsumfang und Budgetplanung mit dem Board abstimmen

Strategie mit Geschäftszielen verbinden

- Sicherheitsvision für den Exit festlegen
- Gap-Analyse zwischen Ist- und Soll-Zustand durchführen
- Wertvollste Assets identifizieren und absichern
- BCDR-Pläne (Business Continuity & Disaster Recovery) aktualisieren und regelmäßig testen

3. Schulungen & Awareness auf Managementebene

Kontinuierliche Schulungen stellen sicher, dass das Management und die wichtigsten Teams Cyber-Risiken besser einschätzen und im Ernstfall angemessen reagieren können.

Vorgehensweise:

- Regelmäßige Management-Trainings zu aktuellen Cyber-Bedrohungen und regulatorischen Pflichten durchführen
- Awareness-Programme für alle Mitarbeitenden etablieren, mit Fokus auf Phishing, Passwortsicherheit und Incident-Reporting
- Spezialisierte Vertiefungstrainings für Hochrisikobereiche wie IT, Recht und Finanzen anbieten
- Einen Cyber-Verantwortlichen ernennen, der Zuständigkeiten definiert und regelmäßig an das Board berichtet

4. Incident-Response-Bereitschaft herstellen

Eine vorbereitete und getestete Incident-Response-Strategie ermöglicht es, Schäden zu begrenzen und Ausfallzeiten zu minimieren, wenn ein Angriff eintritt.

Vorgehensweise:

- Incident-Response-Plan (IR) entwickeln und regelmäßig durch Simulationen (z. B. Tabletop-Übungen) testen
- Krisenkommunikation vorbereiten: interne und externe Kommunikationswege (Kunden, Medien, Behörden) definieren
- Externe Incident-Response-Dienste frühzeitig vertraglich sichern und in Notfallprozesse einbinden
- Nach Tests Lessons Learned dokumentieren und Pläne fortlaufend optimieren

5. Kontinuierlich überwachen und anpassen

Da sich Bedrohungen und regulatorische Anforderungen ständig ändern, muss die Cybersicherheitsstrategie laufend überprüft und angepasst werden.

Vorgehensweise:

- 24/7-Überwachung über MDR (Managed Detection and Response) / SOC (Security Operations Center)-Services etablieren, um Angriffe frühzeitig zu erkennen
- Regelmäßige Schwachstellenscans und Audits durchführen und Prioritäten dynamisch anpassen
- KPIs wie Reaktionszeit und Wiederherstellungszeit messen und verbessern
- Neue Vorgaben (z. B. NIS-2, DSGVO, IT-SiG) fortlaufend integrieren

Neue Cybersecurity-Pflichten: Was Unternehmen aus Industrie und Fertigung wissen müssen

In der DACH-Region steigen die regulatorischen Anforderungen an Cybersicherheit – mit direkter Auswirkung auf Unternehmenswert und Haftungsrisiken.

Strengere Pflichten

- Mit NIS-2 sind nun auch viele Hochschulen und Forschungseinrichtungen zu verbindlichem Cyber-Risikomanagement verpflichtet – inklusive präventiver Maßnahmen und kontinuierlicher Überwachung.
- Im Falle eines Cyberangriffs gelten strenge Meldepflichten ähnlich wie bei der DSGVO (Datenschutz-Grundverordnung).
- Gefordert sind einheitliche europäische Mindeststandards: u. a. technische Schutzmaßnahmen, Notfallpläne, regelmäßige Audits und Risikobewertungen.
- Die **DSGVO** regelt den Umgang mit personenbezogenen Daten, inklusive Meldepflichten bei Datenschutzverletzungen.
- Das **IT-Sicherheitsgesetz** enthält ergänzende Anforderungen für Betreiber kritischer Infrastrukturen (KRITIS), darunter insbesondere zusätzliche Nachweis- und Meldepflichten gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Sanktionen

Bis zu
20 Mio. €
oder 4 % Umsatz

- **Bußgelder:** Bis zu 10 Mio. Euro oder 2 % Umsatz nach NIS-2; bis zu 20 Mio. Euro oder 4 % Umsatz nach DSGVO
- **Aufsichtsmaßnahmen:** Prüfungen, Audits oder im Extremfall Betriebseinschränkungen durch Behörden
- **Reputationsrisiken:** Öffentlich gewordene Verstöße führen zu Vertrauensverlust bei Studierenden, Eltern, Lehrkräften und Förderern
- **Zivilrechtliche Folgen:** Schadenersatzforderungen von Betroffenen, Partnern oder Fördermittelgebern
- **Persönliche Haftungsfolgen:** Schulleitung, Hochschulrektorat, Verwaltungsleitung oder Gremienmitglieder können persönlich haften, wenn sie ihrer Pflicht zur Umsetzung von Cybersicherheitsmaßnahmen nicht nachkommen.

Für Schulen, Hochschulen und Forschungseinrichtungen bedeutet die neue Regulatorik: Cybersecurity ist längst kein reines IT-Thema mehr, sondern zentraler Wert- und Risikofaktor. Wer die Anforderungen aus NIS-2, DSGVO und dem IT-Sicherheitsgesetz ignoriert, riskiert nicht nur hohe Bußgelder und persönliche Haftung, sondern auch den Ausfall von Lernplattformen, Prüfungs- und Verwaltungssystemen sowie massive Reputationsschäden. Frühzeitige Compliance schützt daher nicht nur vor Sanktionen, sondern stärkt auch das Vertrauen von Studierenden, Eltern, Lehrkräften, Förderern und staatlichen Stellen.

Ampel-Check für Bildungseinrichtungen

Die Cybersicherheitsampel ist ein kompaktes Bewertungsinstrument, um den Sicherheitsstatus von Bildungseinrichtungen schnell und vergleichbar einzuschätzen.
Sie basiert auf 10 Kernfragen zu entscheidenden Schutzmaßnahmen.
Wichtig: Kein „✓“ ohne Nachweis akzeptieren! Nur belegte Antworten (z. B. Berichte, Policies, Screenshots) zählen in die Bewertung ein.

10-Fragen-Ampel-Check

1. Ist ein 24/7 Security Operations Center (SOC) oder Managed Detection & Response (MDR) aktiv? ☐

Nachweis: Vertrag, SLA-Berichte

2. Gibt es einen Incident-Response-Plan, der getestet wurde? ☐

Nachweis: IR-Plan, Protokoll der letzten Übung

3. Wurde in den letzten 12 Monaten ein Penetrationstest durchgeführt? ☐

Nachweis: vollständiger Report inkl. Findings

4. Liegt eine dokumentierte IT-/OT-Risikobewertung vor? ☐

Nachweis: Board-Abnahme, Gap-Analyse

5. Werden regelmäßig Awareness-Trainings für Mitarbeitende durchgeführt? ☐

Nachweis: Teilnehmerlisten, Schulungskonzepte

6. Ist Multifaktor-Authentifizierung (MFA) für kritische Systeme implementiert? ☐

Nachweis: Screenshots, Audit-Bericht

7. Ist eine Netzwerksegmentierung umgesetzt, um kritische Systeme zu isolieren? ☐

Nachweis: Architekturdiagramm

8. Existiert ein dokumentiertes Schwachstellen-Management? ☐

Nachweis: Compliance-Reports

9. Wurden Backup- und Recovery-Tests innerhalb der letzten 12 Monate durchgeführt? ☐

Nachweis: Testprotokoll, RTO/RPO

10. Besteht eine aktive und geprüfte Cyberversicherung inklusive Sublimits? ☐

Nachweis: Versicherungspolice

Bewertungssystem:

- Rot (<6 ✓): Kritisch – hohe Risiken, sofortige Maßnahmen erforderlich
- Gelb (6–8 ✓): Mittel – moderate Risiken, Handlungsbedarf, mittelfristig optimierbar
- Grün (9–10 ✓): Sehr gut – geringe Risiken, hohe Resilienz

Roadmap to Security

Die Roadmap to Security bietet Bildungseinrichtungen einen klaren Fahrplan, um Cyber-Risiken zu erkennen, regulatorische Vorgaben umzusetzen und den kontinuierlichen Bildungs- und Forschungsbetrieb zu sichern. Sie verbindet umfassende Analysen mit konkreten Handlungsschritten und macht Cybersecurity zu einem steuerbaren Bestandteil von Leitung und Verwaltung, sowie zu einem entscheidenden Faktor für Vertrauen, Reputation und Zukunftsfähigkeit.

Die Roadmap umfasst:

Sicherheitsbewertung:
Umfassende Prüfung des aktuellen Cybersicherheits-Reifegrads der Bildungseinrichtung

Investitionsplanung:
5-Jahres-Plan für Cybersecurity-Maßnahmen mit CapEx/OpEx-Transparenz

Regulatorik-Check:
Identifikation relevanter Anforderungen aus NIS-2-Richtlinie

Ampelbericht & Maßnahmenplan:
Standardisierte Reifegradbewertung und priorisierte Handlungsschritte

Workshop mit Leitung und Verwaltung:
Gemeinsame Abstimmung der Maßnahmen und Verantwortlichkeiten

Integration von IT- und OT-Sicherheit:
Berücksichtigung von Produktions- und IoT-Umgebungen

Nutzen für Entscheidungsträger

- Cyber-Resilienz ist keine reine IT-Initiative mehr, sondern schafft eine belastbare Grundlage für die Strategie und Steuerung von Bildungseinrichtungen.
- Kostentransparenz und Planbarkeit durch mehrjährige Investitionsplanung (z. B. 5-Jahres-Plan für IT-Sicherheit, Infrastruktur und Schulungen).
- Standardisierte Sicherheitsarchitektur mit messbaren KPIs auch für digitale Lern- und Forschungssysteme (z. B. Vorfallreaktionszeit, Wiederanlaufzeiten, Compliance).
- Stärkt Vertrauen bei Schüler:innen, Studierenden, Lehrkräften, Förderern und staatlichen Stellen durch nachweisbare Cyber-Compliance.

Ihr Partner für Cyber-Resilienz

Die **indevis GmbH** vereint technische Stärke, operative Verlässlichkeit und rechtliche Expertise, um Unternehmen und öffentliche Einrichtungen in einer zunehmend vernetzten Welt ganzheitlich zu schützen.

Unser Leistungsversprechen:

- Ein 24/7 Security Operations Center (SOC) mit Standort in Deutschland
- ISO-27001-zertifizierte Prozesse für höchste Sicherheits- und Compliance-Standards
- Incident Response & Digitale Forensik – schnelle Reaktion und Analyse im Ernstfall
- Regulatorik-Expertise: NIS-2 und DSGVO im Blick für Unternehmens-Compliance

SOS >>>> **Notfallkontakt (24/7):** +49 (0) 89 45 24 24-112

Mehr erfahren – tiefer einsteigen:
Für weitere Informationen besuchen Sie uns auf unserer Website - einfach den QR-Code scannen oder über:
www.indevis.de/roadmap-to-security

SCAN ME

Bereit, Ihre Bildungseinrichtung cyber-resilient zu machen?

Warten Sie nicht auf den nächsten Angriff – handeln Sie jetzt.
Ob Gap-Analyse, Ampel-Check oder Roadmap-Entwicklung – wir zeigen Ihnen, wo Ihre Bildungseinrichtung heute steht und wie Sie Cybersecurity gezielt einsetzen können, um Unterricht, Forschung und Verwaltung nachhaltig zu schützen.

sales@indevis.de
+49 (0) 89 45 24 24-100
indevis

Quellen

1. IBM Security (2024). Cost of a Data Breach Report 2024. Durchschnittskosten für „Higher Education & Training“: ca. $ 3,7 Mio. ≈ 3,4 Mio. € pro Vorfall: https://www.ibm.com/de-de/reportshttps://www.highereddive.com/news/data-breaches-cost-higher-education-colleges/689499/data-breach
2. Stifterverband / Hochschul-Barometer 2024 – Cyber-Sicherheitslage an Hochschulen: https://www.forschung-und-lehre.de/management/hochschulen-unzureichend-auf-cyber-angriffe-vorbereitet-6852
3. CSO Online: Ransomware: Hackerangriff legt Uni Duisburg-Essen lahm (2023): https://www.csoonline.com/article/3492960/ransomware-hackerangriff-legt-uni-duisburg-essen-lahm.html
4. heise Online (2025): Cyberangriff auf Schulen in Rheinland-Pfalz – sind Lockbit verantwortlich? – Bericht über rund 45 betroffene Schulen, die temporär offline waren.. https://www.heise.de/news/Cyberangriff-auf-Schulen-in-Rheinland-Pfalz-Steckt-Lockbit-dahinter-10254814.html
5. PKF Consulting (2024) nach Check Point Research: Cyber Security an Hochschulen – ein wachsendes Risiko im digitalen Zeitalter: https://www.pkf-consulting.de/artikel/cyber-security-an-hochschulen-ein-wachsendes-risiko-im-digitalen-zeitalter?
6. Sophos (2024): State of Ransomware in Education 2024 – zusammengefasst bei Sophos News: https://news.sophos.com/en-us/2024/07/11/the-state-of-ransomware-in-education-2024/
7. Plattner, Claudia (2024). Pressemitteilung: BSI will die „Cybernation Deutschland“ bauen. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/231010_it-sa_Cybernation.html