Zentrum der Brandenburgischen Hochschulen für Digitale Transformation

Informationssicherheit an Brandenburgs Hochschulen

Halbzeit in Sicht!

Tilmann Bock · ZDT-Verbundprojekt InfoSec · Europa-Universität Viadrina Frankfurt (Oder)

Rahmen und Ziel bis Ende 2028

Das MWFK fordert von allen acht brandenburgischen Hochschulen ein zertifizierbares Informationssicherheitsmanagementsystem (ISMS). Fachlicher Orientierungsrahmen: ISO/IEC 27001. Nachweis: externes Audit.

8

HOCHSCHULEN

im ZDT-Verbundprojekt InfoSec.

2028

ZIELJAHR

Nachweis zertifizierbares ISMS.

ISO/IEC 27001

ORIENTIERUNGSRAHMEN

Fachlicher Standard für das ISMS.

externes Audit

NACHWEIS

unabhängige Prüfung des Reifegrads.

Halbzeit: Was haben wir erreicht?

Die Halbzeit rückt näher — Zeit für eine ehrliche Zwischenbilanz: Was ist bereits konzeptionell verankert, und wo steht die Umsetzung im Hochschulalltag?

KONZEPTIONELL

Verankerung vorbereitet

ISMS-Grundlagen stehen: Verantwortlichkeiten, Richtlinien, Risiko-Perspektive sind an jeder Hochschule angelegt.

OPERATIV

Verbund arbeitet taktweise

ISB-Coaching, Konsortium, Workshops und Notfallplanspiele greifen ineinander — der Verbund hat einen gemeinsamen Rhythmus gefunden.

NÄCHSTE SCHRITTE

Umsetzung konsequent machen

Vom Konzept zum gelebten Sicherheitsmanagement: Risiken systematisch, Verantwortlichkeiten klar, Informationssicherheit nachhaltig.

Mehr als IT-Sicherheit

Informationssicherheit wird häufig stark aus technischer Perspektive gelesen. Sie geht jedoch deutlich über die IT-Sicherheit hinaus und umfasst die gesamte Hochschulorganisation.

HÄUFIGE SICHT

IT-Sicherheit

Firewalls, Patches, Backups.
Netz- und Endgeräteschutz.
Technische Maßnahmen im Rechenzentrum.
Zuständig: IT-Abteilung.

ERWEITERTE SICHT

Informationssicherheit

Umfasst IT, OT, Cyber- und physische Sicherheit — alles, was Informationen direkt oder indirekt tangiert.
Organisatorische Abläufe und Prozesse.
Verantwortlichkeiten in allen Bereichen.
Informationen — digital und analog.
Verantwortung: Hochschulleitung.

Low-Hanging Fruits – Umgehende Maßnahmen

Sechs Hebel mit überschaubarem Aufwand und spürbarer Wirkung — jede Hochschule kann hier kurzfristig nachziehen.

Mail-Hygiene 1

SPF, DKIM und DMARC gegen Spoofing und Ghost-Sender — Absenderdomänen konsequent signieren und erzwingen.

Web-Hygiene 2

CAA-Record setzen, damit nur berechtigte Certificate Authorities Zertifikate für die Domänen ausstellen können.

MFA 3

Multi-Faktor-Authentifizierung — Faktor meint Wissen + Besitz + Biometrie, nicht mehrere Geräte desselben Faktors.

Patches einspielen 4

Betriebssystem, Middleware und Anwendungen zeitnah und nachweisbar aktualisieren — Patch-Backlog aktiv abbauen.

Passwortmanager 5

Hochschulweit bereitstellen — Grundlage für lange, einzigartige Passwörter und sichere Weitergabe im Team.

Durchgehend SSO 6

Single Sign-On als Regel, Insel-Logins als Ausnahme — reduziert Angriffsfläche und Passwortmüdigkeit.

ISB im Alltag: Signal einordnen

Beispiel aus dem heutigen ISB-Signal-Prüf-Durchlauf (6. November 2026): Meldung zu sshhole.com — wer tut was?

„OpenSSH on musl Linux (Alpine, OpenWrt, Buildroot, Yocto — und viele gezogene Docker-Images) hat seit 2016 ein Problem. — sshhole.com

ROLLE

ISB

Meldung einordnen, Voraussetzungen verständlich benennen, Bewertung der eigenen Betroffenheit anstoßen, Maßnahmen nachhalten.

ROLLE

IT-Betrieb / Fachteam

Images, laufende Dienste, Versionen und Konfigurationen prüfen; betroffene Systeme aktualisieren oder absichern und das Ergebnis dokumentieren.

ROLLE

Leitung

Erforderliche Ressourcen bereitstellen und Verantwortung für wesentliche Sicherheitsentscheidungen übernehmen.

FACHLICHE EINORDNUNG

Alpine und viele verbreitete Docker-Base-Images liefern OpenSSH nicht standardmäßig mit — betroffen sind nur Images, in denen OpenSSH gegen musl nachinstalliert ist. Deshalb: Betroffenheit konkret prüfen, nicht pauschal aus der Meldung ableiten.

KI verändert die Bedrohungslage

Sprachmodelle wirken auf beiden Seiten: Sie beschleunigen Angriffe — und können, lokal betrieben, zur Abwehr beitragen.

GEFAHR 1

LLM-Schwachstellenanalyse

Sprachmodelle durchforsten Code und Konfigurationen in Minuten — Angreifer-Recherche wird massiv billiger.

GEFAHR 2

Agentische Angriffe

Autonome Agenten ketten Aufklärung, Exploit und Lateral Movement ohne menschliche Taktung.

GEFAHR 3

IP-Abfluss an Frontier-Modelle

Forschung und Entwürfe landen in US-Cloud-Modellen; geistiges Eigentum ist dort weder vertraglich noch technisch geschützt.

GEFAHR 4

Ungehärteter KI-Code

KI-generierte Anwendungen laufen oft ohne SAST und Threat Modeling — Angriffsfläche skaliert schneller als Reviews.

GEFAHR 5

Ungeprüfte Ausarbeitungen

KI-Ausgaben wandern ungeprüft in Berichte und Richtlinien — Halluzinationen in verbindlichen Dokumenten.

GEFAHR 6

Chatbots ohne Prompt-Injection-Schutz

KI-Chatbots stehen in Portalen und Wissensbasen überall — systematische Härtung gegen Prompt-Injection fehlt fast immer.

GEGENMASSNAHME 7

Lokale Modelle zur Abwehr

Auf eigener Infrastruktur betriebene Modelle unterstützen Log-Analyse, Phishing-Erkennung und Incident-Triage — ohne Datenabfluss.

KI-Slop eindämmen: Verbund-Baseline

Ein zentrales Regelset, das überall greift, wo KI-Code entsteht — als Antwort auf die Gefahren 4 und 6 der vorigen Folie.

REGELSET

Baseline-Repo

OWASP LLM Top 10, OWASP ASVS und BSI-Grundschutz-Bausteine auf 1–2 Seiten je Tool-Format übersetzt:
• CLAUDE.md für Claude Code
• .cursorrules für Cursor
• instructions.md für Copilot
Eingebunden als Git-Submodule in jedem Projekt.

PIPELINE-GUARDS

Review automatisieren

Prompt-Regeln steuern nur die Generierung — das Review muss die Pipeline sichern:
• SAST (statische Code-Analyse)
• Dependency- und Lizenz-Scan
• Secret-Scan vor jedem Push
Fail-Build bei kritischen Funden.

PFLEGE IM VERBUND

Eine führt, acht nutzen

Zentrales Repo zdt-ai-coding-rules/ mit Pull-Request-Workflow und Versionierung.

Eine Hochschule übernimmt die Federführung, die anderen ziehen Updates per Submodule-Bump nach.

GRENZEN

Prompt-Regeln allein reichen nicht — zu lang fällt aus dem Kontext, zu kurz bleibt wirkungslos. Realistisch: ~200 Zeilen Muss-Regeln plus Verweis auf ausführliche Referenz.

Ausblick: Audit 2028 / Abschlussnotfallplanspiel 2008

Das Audit 2028 bietet die Gelegenheit, die erreichten Fortschritte sichtbar zu machen und die Wirksamkeit der umgesetzten Maßnahmen unabhängig bewerten zu lassen.

GEGENSTAND

Reifegrad des ISMS

Nicht einzelne Technik, sondern das Managementsystem — Prozesse, Verantwortlichkeiten, Dokumentation, Wirksamkeit.

MASSSTAB

ISO/IEC 27001

Internationaler Standard als fachlicher Orientierungsrahmen. Jede Hochschule weist ihren Stand entlang derselben Struktur nach.

★ ZIEL 2028

NACHWEIS

Externes Audit / Abschlussnotfallplanspiel

Unabhängige Prüfung durch externe Auditor:innen. Ergebnis: belastbare Aussage über Wirksamkeit — nicht nur Konzept.

Danke – und Ihre Fragen

Vom Ermöglichen zur eigenverantwortlichen Umsetzung.

Die Verantwortung liegt bei den Hochschulleitungen — der Verbund gibt den Rahmen.

KONTAKT

Tilmann Bock

Projektkoordination InfoSec
Europa-Universität Viadrina Frankfurt (Oder) · IKMZ
ZDT-Verbundprojekt „Informationssicherheit im Verbund (InfoSec)“