Ideen-Skizze im Dialog für Cybersicherheit

Arbeitstitel/Thema	Umsetzung eines Zero Trust Sicherheitsmodells in Hochschulen

Problem-/Fragestellung inkl. Bezug zur IT-/Cybersicherheit	Gesamtgesellschaftliche Relevanz
Hochschulen betreiben komplexe IT-Systeme, in denen Mitarbeitende täglich mit sensiblen Verwaltungs- und Personaldaten arbeiten. Traditionelle Sicherheitsmodelle vertrauen Geräten und Nutzenden innerhalb des Hochschulnetzwerks – ein Ansatz, der angesichts von Homeoffice zunehmend unsicher ist. Ein einziger kompromittierter Account kann bereits ausreichen, um interne Systeme zu gefährden. Das Zero-Trust-Modell setzt hier an: Es vertraut weder Geräten noch Nutzenden automatisch, sondern überprüft jeden Zugriff fortlaufend. Wie kann Zero Trust in Hochschulen umgesetzt werden, um Identitäten, Geräte und Anwendungen der Mitarbeitenden wirksam zu schützen – ohne deren Arbeitsalltag zu behindern?	Jeden Tag arbeiten Hochschulmitarbeitende mit sensiblen Verwaltungsdaten. Schon ein einziger kompromittierter Account kann weitreichende Folgen haben: Daten werden gestohlen oder manipuliert. Ein Zero-Trust-Ansatz löst dieses Problem direkt: Jeder Zugriff wird kontinuierlich überprüft, ungewohnte Aktivitäten werden sofort erkannt, und Mitarbeitende können weiterhin effizient arbeiten, ohne ständig komplexe Sicherheitsmaßnahmen manuell umzusetzen. Dieser Schutz erhöht nicht nur die Cybersicherheit innerhalb der Hochschule, sondern das entwickelte Konzept würde mit geringfügigen Anpassungen auch von anderen Bildungseinrichtungen übernommen werden, um deren Schutz vor Cyberangriffen zu verbessern.

Mögliche Herangehensweise
- Analyse der IT-Infrastruktur und Sicherheitslage der Hochschulen. - Entwicklung eines Zero Trust-Rahmenkonzepts. - Workshops und Interviews mit Stakeholdern. - Test von MFA- und Geräte-Compliance-Lösungen. - Erstellung von Schulungs- und Awareness-Materialien. - Erarbeitung eines Implementierungsplans mit Pilotprojekten.

Zielgruppe(n)	Geschätzte Laufzeit
Hochschulen, Interessensvertretungen, Dienstleister	mehr als 6 Monate

Angestrebte Ergebnisse	Diskussionspunkte / Offene Fragen / ggf. weitere Stakeholder
- Sichere Arbeitsumgebung für Mitarbeitende - Praxisnahes Zero-Trust-Konzept: Konzipiert für Mitarbeitende, mit der Möglichkeit, es später auf weitere Hochschulkontexte oder Bildungseinrichtungen zu übertragen. - Steigerung der Nutzerkompetenz: Erarbeitung von Leitlinien zur Nutzerakzeptanz und Schulung. - Messbare Wirksamkeit: Weniger erfolgreiche Phishing-Angriffe, schnellere Reaktionszeiten.	- Welche technischen Herausforderungen ergeben sich bei der Integration von Zero Trust? - Welche Rollen haben IT, Datenschutz, Studierende, Lehrende und andere relevante Akteure? - Welche Fördermöglichkeiten unterstützen die Umsetzung?