Ideen-Skizze im Dialog für Cybersicherheit

Arbeitstitel/Thema	CyberHub - Zentrale Verknüpfungsplattform für Cybersicherheitswissen und Praxislösungen für Länder, Kommunen und Organisationen

Problem-/Fragestellung inkl. Bezug zur IT-/Cybersicherheit	**Gesamtgesellschaftliche Relevanz**
Cybersicherheits-Frameworks wie MITRE ATT&CK, das NIST Cybersecurity Framework, der BSI IT-Grundschutz sowie internationale Lösungen (wie MISP, CVE und CSAF) strukturieren Cybersicherheitswissen in ihren jeweiligen Domänen. Diese Frameworks und Ressourcen sind jedoch oft schwer zugänglich und ihre inhaltlichen Zusammenhänge bleiben Praktiker:innen häufig unklar. Eine zentrale Plattform, die Standards und praktische Lösungserfahrungen verknüpft und gleichzeitig eine niedrigschwellige „Was bedeutet das für mich?"-Navigation für Länder, Kommunen und (privatwirtschaftliche) Organisationen ermöglicht, ist nicht verfügbar. Dadurch wird es für diese schwierig, zu verstehen, welche Sicherheitsmaßnahmen für ihre spezifische Situation relevant sind. Das Problem bei einfachen Suchmaschinen ist, dass Nutzer:innen im Bereich Cybersicherheit oft nicht wissen, welche Themen überhaupt relevant sind. Was ist in dieser spezifischen Situation prioritär, was ist ergänzend wichtig und was kann vernachlässigt werden? Welche Lösungen gibt es und welche Anlaufstellen sind die passenden? Es fehlt auch ein strukturierter Mechanismus, durch den Expert:innen neue Bedrohungen in die bestehende Framework-Landschaft einordnen und ihre Einschätzung im Laufe der Zeit verfeinern können, um sie für Praktiker:innen verständlich zu machen.	- Die zunehmende Digitalisierung führt zu einer exponentiell wachsenden Komplexität der Cybersicherheitslandschaft. Länder, Kommunen und Organisationen stehen vor der Herausforderung, aus einem unübersichtlichen Feld verschiedenster Standards, Richtlinien und Empfehlungen die für ihre spezifische Situation relevanten Sicherheitsmaßnahmen zu identifizieren. - Gleichzeitig fehlt eine zentrale Sammelstelle für bewährte Cybersicherheitslösungen aus der Praxis. Länder, Kommunen und Organisationen entwickeln oft parallel ähnliche Lösungsansätze, ohne voneinander zu lernen. Eine Plattform, die nicht nur Standards und Ressourcen verknüpft, sondern auch praktische Implementierungen dokumentiert und durchsuchbar macht, würde redundante Entwicklungsarbeit vermeiden und bewährte Praktiken systematisch verbreiten. - Neue Technologien wie KI-Agenten und Model Context Protocols entstehen schneller, als sie in bestehende Cybersicherheits-Frameworks eingeordnet werden können. Ursprünglich datenschutzrechtlich unbedenkliche Lösungen entwickeln durch die Integration von neuen Technologien plötzlich neue Risikodimensionen. Ohne systematische Einordnungsmechanismen bleiben kritische Sicherheitsaspekte neuer Technologien zu lange unzureichend dokumentiert und kommuniziert. - Ein vereinfachtes Interface macht bestehende Cybersicherheits-Ressourcen zugänglicher und navigierbarer.

Mögliche Herangehensweise
Phase 1 – Framework-Analyse und Verknüpfungsmodell: Systematische Analyse bestehender Cybersicherheits-Frameworks zur Identifikation von Überschneidungen und inhaltlichen Verbindungen. Entwicklung eines strukturierten Verknüpfungsmodells, das die Beziehungen zwischen verschiedenen Sicherheitsbereichen, Bedrohungen und Schutzmaßnahmen abbildet, ohne die bewährten Standards und Frameworks selbst zu verändern (in Workstream-Laufzeit enthalten). Phase 2 – Nutzerfreundliche Navigationsplattform: Entwicklung einer intuitiven Benutzeroberfläche für kontextuelle "Was bedeutet das für mich?"-Abfragen verschiedener Zielgruppen. Die Plattform bietet nicht nur direkte Antworten, sondern zeigt auch verwandte Themen, Prioritäten und praktische Lösungsansätze auf. Nutzer:innen erhalten sowohl theoretische Einbettung als auch Erfahrungsberichte darüber, welche Maßnahmen andere Länder, Kommunen oder Organisationen bereits erfolgreich umgesetzt haben (in Workstream-Laufzeit enthalten). Phase 3 – Community-basierte Wissenserweiterung: Aufbau eines strukturierten Systems zur Integration neuer Erkenntnisse durch Fachexpert:innen und Praktiker:innen. Neue Bedrohungen oder bewährte Lösungen können über einfache Eingabeformulare systematisch erfasst und in die bestehende Wissensstruktur eingeordnet werden, wodurch die Plattform kontinuierlich aktuell bleibt (Ausbaustufe).

Zielgruppe(n)	**Geschätzte Laufzeit**
- Länder, Kommunen, privatwirtschaftliche Organisationen und NGOs für framework-basierte aber verständliche Cybersicherheitsinformationen und situationsspezifische Navigation - Cybersicherheits-Expert:innen für framework-übergreifende Navigation und systematische Bedrohungseinordnung	keine Schätzung möglich

Angestrebte Ergebnisse	**Diskussionspunkte / Offene Fragen / ggf. weitere Stakeholder**
- Navigationsplattform zur Verknüpfung von Cybersicherheits-Frameworks, thematischen Bereichen und praktischen Lösungserfahrungen - Community-Plattform für den Austausch bewährter Cybersicherheitslösungen zwischen Ländern, Kommunen und Organisationen - Zielgruppen-spezifische Navigationsschnittstelle mit "Was bedeutet das für mich?"-Funktionen für Länder, Kommunen und Organisationen - Strukturiertes Eingabesystem für systematische Integration neuer Bedrohungstypen durch Experteneinbindung und bewährter Lösungen durch Praktiker:innen	- Qualitätssicherung: Welche Mechanismen gewährleisten die Validität und Neutralität von Expertenbeiträgen bei der Einordnung neuer Bedrohungen und Community- Mitgliedern bei der Eingabe von existierenden Lösungen? - Nachhaltigkeit und Wartung: Welche institutionellen Strukturen sind für die langfristige Pflege und Aktualisierung der semantischen Verknüpfungen erforderlich?