Aufbau eines Cybersecurity Lab im Landkreis Konstanz

AUSGANGSLAGE

Aktuelle Studien und Lageberichte berichten von einer dramatischen Zunahme an Cyberangriffen, die immer professioneller und weitreichender werden. So zeigt etwa ein Bericht des Bundesamts für Sicherheit in der Informationstechnik, dass täglich rund 300.000 neue Schadprogramm-Varianten im Umlauf sind und Ransomware-Angriffe besonders Kommunen und kleine und mittlere Unternehmen (KMU) treffen. Auch KI-basierte Angriffe, Multi-Channel-Phishing und Lücken in Software-Lieferketten werden in den kommenden Jahren weiter zunehmen. Die Schadenssummen steigen: Allein in Deutschland ist laut Branchenverband Bitkom im Jahr 2024 ein wirtschaftlicher Schaden von über 170 Milliarden Euro durch Cyberkriminalität entstanden.

Gleichzeitig vernachlässigen viele Organisationen das Thema Cybersicherheit häufig aus Kostengründen, fehlender Expertise oder einem falschen Sicherheitsgefühl. Gerade KMU sowie kommunale Einrichtungen stehen vor großen Herausforderungen, da oft weder die personellen noch die finanziellen Ressourcen vorhanden sind, um eigene hochprofessionelle Sicherheitsabteilungen einzurichten. Auch viele Privatpersonen oder Bildungseinrichtungen wissen nicht, an wen sie sich bei Fragen zur IT-Sicherheit wenden können.

All diese Fakten unterstreichen die Dringlichkeit, konkrete Maßnahmen zu ergreifen und die IT-Sicherheitslage im Landkreis Konstanz gezielt zu verbessern. Die Region in puncto Cybersicherheit gut aufzustellen ist ein Schlüssel, um die Zukunftsfähigkeit der Wirtschaft nachhaltig zu sichern. Vor diesem Hintergrund beantragt der cyberLAGO e.V. die finanzielle Förderung zur Errichtung eines Cybersecurity Lab, das als zentrale, neutrale Anlaufstelle fungiert und mit seinen Maßnahmen das IT-Sicherheitsniveau im gesamten Landkreis Konstanz erhöht.

cyberLAGO ist das Netzwerk der Digitalexperten am Bodensee und agiert grenzüberschreitend als Vertrauensplattform, Wegweiser, Impulsgeber, Transformationstreiber und zentrale Anlaufstelle bei Fragen rund um Digitalisierung, digitale Transformation, Innovation und IT. Die Clusterinitiative ist sehr erfahren in der Umsetzung von Projekten, wie jüngst das KI-Lab Bodensee oder der European Digital Innovation Hub. Was cyberLAGO von anderen Clusterinitiativen der Region unterscheidet, ist der branchenunabhängige Ansatz. So hat cyberLAGO einen interdisziplinären Charakter, der im Querschnitt alle wirtschaftlichen, wissenschaftlichen und gesellschaftlichen Akteure betrifft. Auch IT-Sicherheit ist kein branchenspezifisches Thema; Bedrohungen und Lösungen sind für alle gleich, Feinheiten, die überschaubar sind, gibt es lediglich bei gesetzlichen Vorgaben. Deshalb ist cyberLAGO prädestiniert dafür, das geplante Cybersecurity Lab im Landkreis Konstanz aufzubauen und als Anlaufstelle zu etablieren.

ZIEL

Die Ziele des Cybersecurity Lab leiten sich aus einer Analyse von Problem und Ursache ab, die sich folgendermaßen zusammenfassen lässt:

Problem	Ursache (Warum)	Ziel
Fehlende Risikobewertung und Sensibilisierung	Organisationen unterschätzen Cyberrisiken oder glauben, sie seien kein Ziel für Angriffe.	Bewusstsein für Cybersicherheit schaffen, IT-Sicherheit als strategisches Thema etablieren.
Mangelhafte Netzwerksicherheit und Schwachstellenmanagement	Veraltete Systeme, ungesicherte Netzwerke, fehlende Firewalls und Patch-Management.	Notwendiges Wissen aufbauen, um regelmäßige Sicherheitsupdates und Netzwerkschutz zu etablieren.
Fehlende Sicherheitsstrategien und Notfallpläne	IT-Sicherheit wird nicht als strategisches Thema betrachtet, Notfallpläne fehlen.	Befähigung zur Entwicklung einer IT-Sicherheitsstrategie und eines umsetzbaren Notfallplans.
Unzureichender Schutz vor Phishing & Social Engineering	Mitarbeitende sind nicht ausreichend geschult, Phishing-Angriffe werden nicht erkannt.	Mitarbeitende sensibilisieren und auf Social-Engineering-Angriffe vorbereiten.
Fehlende oder schwache Authentifizierungsmaßnahmen	Kein Bewusstsein für sichere Passwörter, fehlende Multifaktor-Authentifizierung.	Sichere Authentifizierungsmethoden einführen, Passwortrichtlinien verbessern.
Vernachlässigung der Cloud- und IoT-Sicherheit	Cloud- und IoT-Systeme werden ohne Sicherheitskonzept eingesetzt, fehlerhafte Konfigurationen und offene Ports werden zum Einfallstor.	Sichere Konfiguration und Nutzung von Cloud- und IoT-Diensten sicherstellen.
Unkenntnis über gesetzliche und regulatorische Anforderungen	KMU fehlt oft der Überblick über geltende Cyber-sicherheits- und Datenschutzvor-gaben wie NIS-2, DSGVO oder den Cyber Resilience Act. Zudem fehlen Ressourcen, um diese zu bewerten und umzusetzen.	Rechtliche Anforderungen kennen, verstehen und in die Sicherheitsstrategie integrieren.

(NEU) RELEVANZ UND ABGRENZUNG ZU BESTEHENDEN ANGEBOTEN

Das Cybersecurity Lab setzt **komplementär** zu bestehenden Strukturen an und schließt erkennbar drei Lücken: **Regionalität** (dauerhafte Anlaufstelle im Landkreis), **Kontinuität** (laufende Formate statt Einzelmaßnahmen) und **Umsetzungstiefe** (vom Wissen zur Anwendung). Konkret bietet es Erstberatung mit Leitfäden und Checklisten, regelmäßige Workshops, Learning Labs und eine jährliche Konferenz sowie ein fortlaufend gepflegtes Infoportal; hinzu kommen Erprobung im mobilen Showroom, bedarfsorientierter Technologietransfer und der regionale Expertenkreis zur Qualitätssicherung. So bündelt das Lab vorhandene Angebote, übersetzt sie in praxistaugliches Handeln und verankert sie vor Ort.

Kurze Einschätzung bestehender Angebote (Auswahl) mit Abgrenzung:

- **IHK Hochrhein-Bodensee „CyberWuP“**: Einstiegs-/Orientierungsberatung für KMU als einmaliger **60-Minuten-Check**; adressiert v. a. die Geschäftsführung, liefert eine Momentaufnahme und Basisempfehlungen. Wertvoll zur Erstorientierung, jedoch ohne kontinuierliche Begleitung, technische Vertiefung und regionale Vernetzungsstruktur. Das Lab setzt anschließend an (Vertiefung, Umsetzung, Training, Netzwerk).
- **Cybersicherheitsagentur Baden-Württemberg (CSBW)**: Landesweite Cyber-Ersthilfe BW als zentrale Meldestelle/Hotline für Vorfälle; zusätzlich Beratungsangebote insbesondere für Kommunen. Starke reaktive Unterstützung und zentrale Expertise, jedoch keine Präsenz im Landkreis und keine regional kuratierten Lern- und Übungsformate für KMU. Das Lab kann hier als lokaler Verstärker wirken (präventiv, hands-on, vernetzend) und kooperiert mit der CSBW.

Das Cybersecurity Lab schafft Schnittstellen, übernimmt lokal die Vertiefung, kontinuierliche Befähigung der Mitarbeitenden, praktische Erprobung sowie sichtbare Vernetzung der regionalen Akteure. Es ist **kein Parallelangebot**, sondern die fehlende Struktur, die Orientierung in Umsetzung verwandelt und Verantwortung vor Ort verankert. Mit dem Lab entsteht der **lokale Hebel**, der bestehende Angebote bündelt und in **konkrete Sicherheitsgewinne** übersetzt: weniger Vorfälle, kürzere Ausfallzeiten, belegbare Compliance sowie messbar höhere Resilienz – organisatorisch, technisch und personell.

GANZHEITLICHER ANSATZ

Im Rahmen des Cybersecurity Lab setzt cyberLAGO auf einen ganzheitlichen Ansatz, der sich am bewährten Dreiklang aus Prävention, Detektion und Reaktion orientiert – **branchenunabhängig für alle Organisationen**, denn Cyberbedrohungen sowie grundlegende Abwehrstrategien sind im Kern stets vergleichbar. Spezifische

rechtliche und regulatorische Vorgaben (z. B. NIS-2, CRA, KRITIS) werden dabei beachtet und gezielt in die jeweiligen Maßnahmen integriert.

Prävention zielt darauf ab, Sicherheitsrisiken bereits im Vorfeld zu minimieren. Dies wird erreicht durch Kow-how-Aufbau, Awareness-Kampagnen und standardisierte Checklisten, die KMU und öffentliche Einrichtungen in die Lage versetzen, proaktiv gegen Cyberangriffe vorzugehen.

Detektion bedeutet die frühzeitige Erkennung von Cyberbedrohungen mittels moderner digitaler Überwachungsmöglichkeiten und Alarmsystemen. Das Lab wird den Zugang zu innovativen Diagnosetechnologien ermöglichen, sodass verdächtige Aktivitäten umgehend identifiziert werden können.

Reaktion umfasst alle Maßnahmen, die im Ernstfall ergriffen werden, um Schäden schnell und effizient zu begrenzen. Hierzu zählen koordinierte Incident-Response-Prozesse, forensische Analysen und eine strukturierte Krisenkommunikation, die in Zusammenarbeit mit regionalen IT-Sicherheitsexperten durchgeführt werden.

MASSNAHMEN

Die geplanten Angebote des Cybersecurity Lab umfassen:

ANLAUFSTELLE & ERSTBERATUNG – Das Cybersecurity Lab wird zur Anlaufstelle im Landkreis Konstanz bei allen Fragen rund um IT-Sicherheit. Unkomplizierte Erstberatung erfolgt z. B. über praxisorientierte Leitfäden, Checklisten und passgenaue Empfehlungen zu regionalen Cybersecurity-Experten.

INFORMATION & SENSIBILISIERUNG – Das Angebot umfasst eine Reihe von Veranstaltungen wie Workshops, vertiefende Learning Labs, interaktive Seminare und eine jährlich stattfindende Cybersecurity Konferenz, in denen aktuelle Themen, Bedrohungen und praxisnahe Lösungsansätze vermittelt werden. Ergänzend dazu wird eine Website als zentrales Infoportal erstellt und betrieben, die kontinuierlich mit News, fundiertem Cybersecurity-Fachwissen, weiterführenden Wissensquellen sowie einer übersichtlichen Darstellung regionaler Angebote und Experten aktualisiert wird. Regelmäßiger Content auf Social Media und im Newsletter schafft konstante Sichtbarkeit des Themas und führt zu notwendiger Awareness im Bereich IT-Sicherheit.

ERPROBUNG – Ein mobiler Showroom ermöglicht einen spielerischen Zugang zu Cybersecurity-Themen. Mit interaktiven Demonstrationen und realitätsnahen Simulationen können Teilnehmer die Dynamiken von Cyberangriffen und Schutzmaßnahmen nachvollziehen. So wird auf niederschwellige Weise Wissen vermittelt und das Verständnis dafür geschärft, wie Sicherheitsrisiken entstehen und wirksam abgewehrt werden können. Diese Lernumgebung unterstützt

Organisationen dabei, ihre Mitarbeiter im Ernstfall zu stärken und eine nachhaltige Sicherheitskultur aufzubauen.

TECHNOLOGIETRANSFER – Vielen Betrieben fehlt das notwendige interne Fachwissen, um IT-Sicherheitsstrategien zu entwickeln und -maßnahmen erfolgreich umzusetzen. Daher wird das Cybersecurity Lab spezielle Angebote entwickeln, die gezielt Kompetenzen in den Unternehmen aufbauen und die jeweiligen Mitarbeiter dazu befähigen, potenzielle Schwachstellen zu erkennen, den Umgang mit Sicherheitsbedrohungen zu verstehen und die Möglichkeiten sicherer Digitalisierung voll auszuschöpfen.

VERNETZUNG – Alle Anlässe des Cybersecurity Lab dienen auch der Vernetzung, dem fachlichen und dem Erfahrungsaustausch. Das Lab versteht sich dabei als neutrale Vertrauensplattform, die einen direkten Draht zu Experten und Fachkräften aus Wirtschaft, Wissenschaft und Verwaltung ermöglicht und jedem einen einfachen Zugang zu einem starken, belastbaren Netzwerk bietet.

EXPERTENKREIS – Ein Kreis aus IT-Sicherheitsexperten aus Unternehmen, Startups und Wissenschaft wird sich regelmäßig treffen, um die Ausgestaltung der geplanten Maßnahmen des Cybersecurity Lab zu diskutieren und bereits erfolgte Maßnahmen zu bewerten. Dies stellt sicher, dass die Themen immer aktuell und relevant sind, lässt gemeinsame Aktivitäten und Synergien entstehen und trägt zur Qualitätssicherung und Effizienz der Maßnahmen bei. Auch an der Verstetigung des Lab wird der Expertenkreis mitarbeiten.

Im Rahmen des vom Land Baden-Württemberg zwei Mal geförderten KI-Lab Bodensee zeigte cyberLAGO, dass der Lab-Ansatz funktioniert, und kann die wesentlichen Erkenntnisse und Erfahrungen – z. B. mit dem mobilen KI-Showroom, der jährlich stattfindenden KI-Konferenz, der Begleitung durch den KI-Expertenkreis, den erfolgreichen Wissenstransfer- und Vernetzungsanlässen, die Einbindung bestehender regionaler Angebote – unmittelbar einfließen lassen.

FINANZIELLE AUSWIRKUNGEN

Der cyberLAGO e.V. beantragt eine projektbezogene Förderung in Höhe von **165.850 €** für **insgesamt zwei Jahre (11/2025 bis 10/2027)**. Die darüber hinausgehenden Kosten können durch Eigenmittel und die Unterstützung von cyberLAGO-Mitgliedern in Form von Sponsoring und kostenfreier Zuarbeit gedeckt werden.

Die Kosten bestehen einerseits aus Personalaufwand im Umfang von sechs Personenmonaten des Projektleiters und 16 Personenmonaten von Projektmitarbeitern; andererseits aus Sachkosten, die im ersten Halbjahr hoch sind, da dort die wesentliche Infrastruktur aufgebaut werden und die erste Konferenz stattfinden

soll. Ein detaillierter Finanzplan und die Auflistung der Sachkosten befindet sich im Anhang.

NUTZEN FÜR DEN LANDKREIS KONSTANZ

Zusammengefasst hätte das Cybersecurity Lab folgenden Nutzen:

- **Krisenresilienz**
  - Passgenaue Cybersecurity-Unterstützung für alle Organisationen
  - Reduzierung von Schäden durch Cyberangriffe durch bestmögliche Prävention, schnelle Detektion und optimale Reaktion
  - Stärkung der Wettbewerbs- und Zukunftsfähigkeit durch (Cyber-)Resilienz
- **Kompetenzaufbau und Kooperationen**
  - Qualifizierung von Fachkräften
  - Steigerung regionaler Wertschöpfung durch Zusammenarbeit von Organisationen mit regionalen Experten
  - Vernetzung von Wirtschaft, Wissenschaft und Verwaltung
  - Gemeinsame Entwicklung von Best Practices, Pilotprojekten und Lösungen
- **Standortattraktivität**
  - Langfristiges Ziel ist, dass der Landkreis Konstanz eine Kompetenzregion für IT-Sicherheit wird. So werden z. B. weitere Fachkräfte angezogen, die Wettbewerbsfähigkeit und regionale Wertschöpfung werden gesteigert.

Der Aufbau des Cybersecurity Lab im Landkreis Konstanz, der nur mit Fördermitteln möglich ist, ist somit eine zukunftsweisende Investition und ein wesentlicher Baustein für eine resiliente, zukunftssichere Region.