



Thorsten Kraft MSc, PhD EXECUTIVE SECURITY ARCHITECT

Ihr Ansprechpartner für alle Angebote

Seit 1996 herstellerneutrale Sicherheits- und Enterprise-Architekturen für Betreiber kritischer Infrastrukturen, Energieversorger, Telekommunikationsunternehmen, öffentliche Auftraggeber und Einrichtungen des Gesundheitswesens.

Entscheidungen unter Zeitdruck absichern

Angebot 04

Mein eigentliches Fachgebiet sind Sicherheits-, Assistenz- und Entscheidungsarchitekturen für Situationen mit hoher Informationsdichte, komplexen Abhängigkeiten und Zeitdruck. Ein Krisenstab ist nichts anderes: eine Entscheidungsarchitektur, die unter Belastung trägt oder eben nicht.

Dahinter stehen: Lagebildgenerierung, Situational Awareness, Decision Intelligence, Alarmierungs- und Eskalationskonzepte, integrierte Konzepte über Cyber, physische und organisatorische Sicherheit hinweg

Architekturen, die im Betrieb tragen

Angebot 02

Von der Risikoanalyse über die Zielarchitektur bis zu Ausschreibung, Qualitätssicherung und Abnahme – in einer Hand und ohne Produktinteresse. Dieselbe Frage, die in Verbünden und Konzernstrukturen entsteht, habe ich in Energie- und Telekommunikationsnetzen seit Jahren beantwortet: gemeinsame Identitäten, getrennte Netze, kontrollierte Datenräume.

Dahinter stehen: Enterprise Security Architecture, Zero Trust, IAM und PAM, Mikrosegmentierung, Cloud- und Rechenzentrumssicherheit, OT-, IoT- und Embedded Security

Künstliche Intelligenz nachvollziehbar halten

Querschnitt

Ich begleite die sichere Integration von KI und agentischen Systemen mit einem einzigen Anspruch: Entscheidungswege, Berechtigungen und Handlungsspielräume müssen jederzeit transparent, nachvollziehbar und kontrollierbar bleiben. Nachrüsten lässt sich das kaum – es ist eine Frage der Konstruktion.

Dahinter stehen: AI Governance und EU AI Act, agentische und Multi-Agent-Systeme, Human-in-the-Loop, AI Observability und Auditability, AI Red Teaming

Für Entscheider verständlich bleiben

Angebot 01 und 03

Strategische Beratung von Geschäftsführungen, CIOs und CISOs heißt vor allem, komplexe Sachverhalte so darzustellen, dass daraus eine Entscheidung werden kann. Das ist keine rhetorische Übung, sondern seit § 38 BSIG eine Pflicht der Leitungsebene – und die Voraussetzung dafür, dass Maßnahmen überhaupt gebilligt und überwacht werden können.

Dahinter stehen: Informationssicherheits-, Risiko- und Resilienzmanagement, Security Governance, ISO/IEC 27001, BSI IT-Grundschutz, Programm-, Projekt- und Interim-Management

Referenzen und Veröffentlichungen

Zero Trust in der Luftfahrt – Whitepaper gemeinsam mit Airbus, eco Verband und Deutscher Telekom, ergänzt um den Demonstrator FACIS zur nachvollziehbaren Autorisierung automatisierter Handlungen. Sicherheitskritisch, streng reguliert, Mensch in der Entscheidungsschleife – dieselben Anforderungen, die heute in Industrie, Versorgung und Gesundheitswesen entstehen.

Fachpublizistik zu agentischer KI, Nachweisführung nach § 30 BSIG und Zero-Trust-Architekturen, unter anderem zur Frage, wie sich Delegationsketten automatisierter Systeme prüfbar machen lassen.

REGULATORIK UND STANDARDS

NIS-2 / BSIG

KRITIS

DORA

ISO/IEC 27001

BSI IT-Grundschutz

VdS 10000 / 10100

EU AI Act

branchenspezifische Sicherheitsstandards

Gespräch vereinbaren – **direkt mit dem Architekten, nicht mit dem Vertrieb.**

DOIT AG · IT/TK Consulting

+49 (0) 40 808 190 530 · info@doitag.de · www.doitag.de