Digitale Souveränität und resiliente KRITIS-IT-Infrastrukturen in Europa

Ein Leitfaden von Mobotix sowie Grouplink IT Solutions und LANCOM Systems

secIT-Workshop

18. März 2026

Für eine praktische Umsetzung veranstalten die Partner Mobotix, Grouplink IT Solutions und LANCOM Systems einen Hands-On Workshop für KRITIS-Verantwortliche. Ziel ist die praktische Unterstützung beim Aufbau zukunftssicherer Infrastrukturen und Hinweise für Migrationspfade.

Die digitale Souveränität ist im Kontext kritischer Infrastrukturen (KRITIS) kein optionales Ziel, sondern eine angestrebte Voraussetzung für staatliche Resilienz, mehr IT-Sicherheit und Zukunftsfähigkeit in der Digitalisierung Europas. Das Whitepaper nimmt Bezug auf die Rolle europäischer IT-Lösungen als strategisches Mittel zur Erweiterung der Digitalen Souveränität. Es zeigt auf, wie europäische Hersteller mit zertifizierten, DSGVO-konformen und aufeinander aufbauenden Lösungen eine vertrauenswürdige IT-Infrastruktur schaffen können. Dazu wird die Bedeutung moderner, souveräner Standortvernetzung hervorgehoben – insbesondere durch SD-WAN-Technologien aus Europa.

Digitale Souveränität als strategisches Ziel

Digitale Souveränität bezeichnet die Fähigkeit von Staaten, Unternehmen und Organisationen, eigene digitale Prozesse, Datenflüsse und IT-Infrastrukturen kontrollieren und gestalten zu können. Sie grenzt sich ab von Autarkie und zielt nicht auf Isolation, sondern auf strategische Handlungsfähigkeit bei kalkulierbaren Risiken. Für KRITIS-Betreiber bedeutet das ein wachsendes Bewusstsein für Abhängigkeiten, die Kontrolle über eingesetzte Technologien, effektive Sicherheitsmechanismen in der IT-Security sowie einen resilienten IT-Betrieb.

Wachsende Berücksichtigung in den politischen Rahmenbedingungen

Der Koalitionsvertrag betont die Bedeutung der digitalen Souveränität insbesondere durch die Schaffung eines „Ministeriums für Digitales und Staatsmodernisierung", die Förderung der digitalen Infrastruktur (Glasfaserausbau, Rechenzentren), die Stärkung von Schlüsseltechnologien wie KI und die IT-Sicherheit, sowie durch Maßnahmen zur digitalen Verwaltung und zur Stärkung europäischer IT-Infrastrukturen und

Open-Source-Lösungen. In diesem Whitepaper konzentrieren wir uns auf die Stärkung der IT-Sicherheit sowie europäische IT-Infrastrukturen. Dabei unterstreichen auch die EU-Strategien „Digital Decade" und der „Cyber Resilience Act" die Notwendigkeit europäischer IT-Lösungen. Nationale Strategien wie die Cyber-Sicherheitsstrategie 2021, EU-Richtlinien für mehr IT-Sicherheit (NIS-2) oder BSI-Vorgaben (IT-Grundschutz, KRITIS-V) fordern nachweislich sichere und vertrauenswürdige Systeme.

Steigende Herausforderungen für KRITIS-Betreiber

KRITIS-Organisationen stehen vor einem Spannungsfeld: Administrativer sowie wirtschaftlicher Druck trifft auf hohe Sicherheits- und Compliance-Anforderungen. Bei einer nahezu gleichen Ausstattung an Ressourcen sind immer mehr Aspekte zu berücksichtigen und zu leisten. Dazu erschweren die noch in weiten Teilen bestehenden Abhängigkeiten von außer-europäischen Technologien den Einsatz von europäischen Alternativen, die aufgrund im Vergleich weitaus geringerer R&D-Budgets nicht immer eine Feature-Parität gewährleisten können. Gleichzeitig stellen IT-SiG 2.0, NIS-2 und die KRITIS-Verordnung hohe Anforderungen an Nachvollziehbarkeit, Transparenz und Reaktionsfähigkeit. In Summe ein durchaus herausforderndes Feld für die IT-Verantwortlichen in KRITIS-Organisationen.

IT-Security im europäischen Ecosystem

Das aktuelle Allianz-Risk-Barometer bescheinigt auch für 2025: Cybervorfälle wie Datenschutzverletzungen, Ransomware-Attacken und IT-Ausfälle, wie der CrowdStrike-Vorfall im Sommer, sind für Unternehmen weltweit in diesem Jahr erneut das größte Risiko[1]. Es mangelt in der heutigen Zeit nicht mehr an IT-Tools, aber diese werden doch eher in der Minderheit von europäischen Unternehmen gestellt. Dabei bergen globale Abhängigkeiten Risiken – in diesem Zusammenhang seien Datenschutz, kalkulierbare Lizenzpolitik oder auch das Thema Backdoor-Freiheit zu nennen. Europäische Hersteller bieten hier Vorteile: Rechtskonforme Entwicklung, nachvollziehbare Sicherheit und enge regulatorische Einbettung.

[1] https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2025/de.html

Sicherheitsarchitekturen im IT Security Ecosystem

Wir leben in einer Zeit der weiter zunehmenden Spezialisierung in der Wirtschaft. Unternehmen fokussieren sich auf ihre Kernkompetenzen, um überdurchschnittliche Produkte und Lösungen zu realisieren. Dieses Prinzip lässt sich auch auf ein europäisch ausgerichtetes IT Security Ecosystem anwenden. Denn die Vielzahl von Sicherheitskomponenten auf den unterschiedlichen Dimensionen der IT-Sicherheit im Bereich IT-Netzwerke ist umfassend. Je nach Schutzbedarf der jeweiligen KRITIS-Organisation bzw. Use-Cases wird das IT Security Ecosystem modular aufgebaut mit vertrauenswürdigen Partnern, die europäischen Datenschutz- und Sicherheitsstandards entsprechen und so die Digitale Souveränität in Europa fördern.

Moderne Standortvernetzung für resiliente KRITIS IT-Infrastrukturen

Eine KRITIS-Standortvernetzung zielt auf die Unterstützung reibungsloser Arbeitsabläufe ab – im Kern geht es dabei um den sicheren Transport von Daten. Die Souveränität und Performance in der Weiterleitung der Daten muss insbesondere im KRITIS-Umfeld die höchsten Prioritäten haben. Das bedeutet, dass KRITIS-IT-Netzwerke hochverfügbar, skalierbar und gegen Angriffe robust sein müssen. Dabei wird die Datenverarbeitung von einer ganzen Reihe von Anwendungen übernommen, gerade für kritische Kernprozesse – diese stellen eine hohe Anforderung an Performance, Latenz und Redundanz.

Software-Defined WAN (SD-WAN) aus europäischer Hand

SD-WAN-Technologien bieten gegenüber klassischen WANs Vorteile wie dynamisches Routing, zentrale Steuerung, Policy-basierte Sicherheit und Cloud-Optimierung. Europäische Anbieter ermöglichen DSGVO-konforme SD-WAN-Lösungen mit tiefem Netzwerk- und Sicherheits-Know-how. Ein gut funktionierendes IT-Netzwerk ist das Herz einer jeden KRITIS-Organisation. Es aufzubauen und zu steuern kann jedoch zeitaufwändig und fehleranfällig sein. In einer IT-Welt mit zunehmender Komplexität und einem allumfassenden Fachkräftemangel werden daher zuverlässige Netzwerk-Managementsysteme benötigt, die den Netzwerkbetrieb automatisiert steuern und optimieren. So ermöglichen Cloud-basierte Steuerungssysteme aus Europa Remote-Troubleshooting – ohne teure Vor-Ort-Einsätze, Zero-touch-Inbetriebnahme ganzer Standorte, selbstlernende WLAN-Automationslösung sowie die schnelle Bereitstellung neuer Netze und Dienste.

Implementierungsstrategien

In den seltensten Fällen startet ein KRITIS-Unternehmen auf der „grünen Wiese“ mit einer komplett neuen IT-Infrastruktur. Sprich, der Status quo besteht aus einer umfangreichen, teilweise heterogenen Installationsbasis verschiedener Hersteller-Komponenten. Dazu kommen sicherlich noch langlaufende Lizenzvereinbarungen.

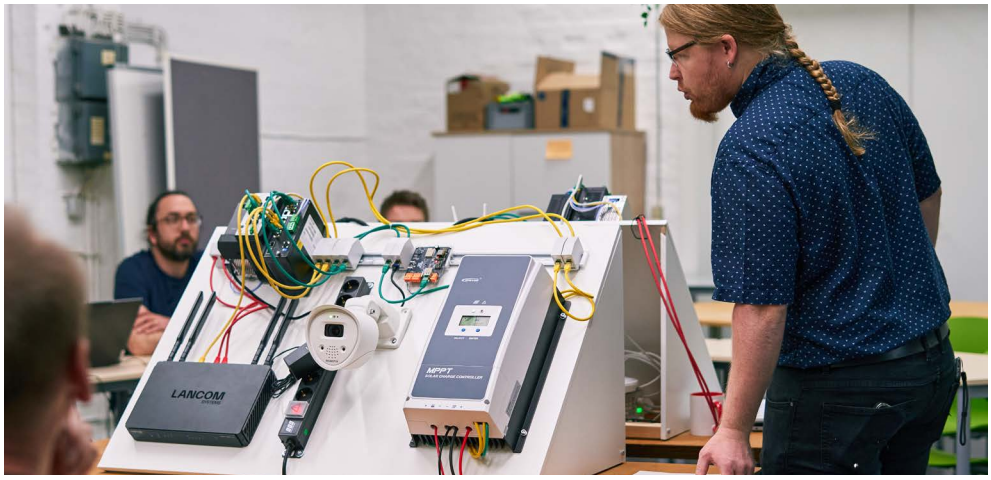
Ein schrittweiser Migrationspfad ermöglicht KRITIS-Betreibern den Übergang von der heutigen IT-Infrastruktur zu einer sicheren, leistungsfähigen und digital souveränen Architektur. Hybrid-Modelle können dabei den Parallelbetrieb alter und neuer Infrastrukturen ermöglichen. An erster Stelle steht aber zunächst die Bestandsaufnahme sowie die Zielsetzung, was die KRITIS-Organisation durch eine Veränderung bzw. Modernisierung der IT-Infrastruktur erreichen möchte – eine „Digital Sovereignty Roadmap“ schafft Klarheit über Prioritäten, Ressourcenbedarf und Meilensteine. Führen Sie eine umfassende Dependency-Analyse durch: Welche Ihrer kritischen Systeme stammen von außereuropäischen Herstellern? Wo bestehen Single Points of Failure in der Lieferkette? Berücksichtigen Sie dabei nicht nur die direkten Abhängigkeiten, sondern auch die zugrunde liegenden Subkomponenten und genutzten Cloud-Services.

Dabei können erfahrene Systemhaus-Partner durch ihre umfassende Erfahrung realisierbare und wirtschaftlich tragfähige Migrationspfade aufzeigen. Sie helfen durch ein professionelles Change-Management mit Risikobewertung, schrittweiser Implementierung sowie Schulung und Betriebsunterstützung der operativen Teams.

Hands-On Workshop für IT-Teamleiter und IT-Administratoren

Ein Mehr an Digitaler Souveränität entsteht nicht im Alleingang, sondern durch starke Partnerschaften. Evaluieren Sie gezielt europäische Alternativen, die nachweislich KRITIS-Anforderungen erfüllen. Denn europäische Partner bieten nicht nur technologische Alternativen, sondern auch bessere Rechtssicherheit, kürzere Kommunikationswege und ein gemeinsames Verständnis für compliance-relevante Anforderungen. Dabei helfen wir Ihnen als Team.

Im Hands-On Workshop teilen wir die Teilnehmer in zwei Gruppen: 1. Praktischer Aufbau und Sicherheits-Optimierung einer IT-Infrastruktur (Zielgruppe IT-Administratoren) und 2. Was sind die Herausforderungen und Themen im Alltag des IT-Teams (Zielgruppe IT-Teamleiter, IT-Projektleiter).



1. Praktischer Aufbau und Sicherheits-Optimierung einer IT-Infrastruktur

KRITIS IT-Administratoren stehen vor der Herausforderung, lokale IT-Aufgaben wie Updates, Rechteverwaltung und Sicherheitsmanagement effizient zu bewältigen – auch hinsichtlich regulatorischer Anforderungen und hohem Datenaufkommen. Im Rahmen unserer Gruppenarbeit beim Hackathon validiert die Gruppe eine vor Ort aufgebaute „Secure Edge Computing“ Lösung mit Geräte-Komponenten, beispielsweise zur Vernetzung von Wind- und Solarparks, basierend auf typischen KRITIS-Anwendungsfällen wie Update-Handling, Zugriffssteuerung und der Umsetzung gängiger Sicherheitskonzepte im Arbeitsalltag eines IT-Administrators.

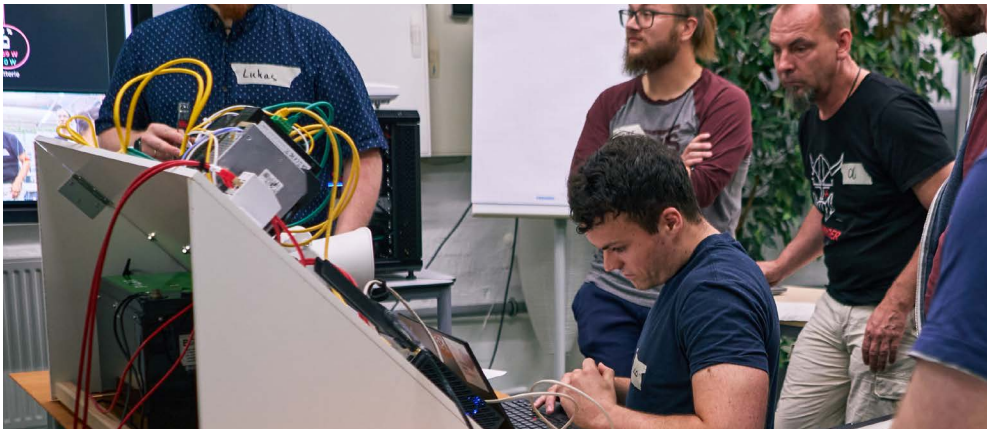


Abb. Aufbau einer KRITIS-Umgebung am Beispiel Windpark / Solarpark

2. Herausforderungen und Themen im Alltag des IT-Teams

Im Rahmen unserer Gruppenarbeit beim Hands-On Workshop entwickeln wir auf Basis realer Herausforderungen von IT-Admins in KRITIS-Umgebungen praktikable Ansätze zur Optimierung von Prozessen, um den Alltag spürbar zu entlasten. Ziel ist es, über den Austausch von Best Practices eine priorisierte Checkliste zu erarbeiten, die als Grundlage für konkrete Prozessverbesserung in einem kontinuierlichen Verbesserungsprozess dient.

Abb. Erstellung praktikabler Ansätze zur Optimierung von Prozessen

Exemplarischer Use-Case KRITIS-Objektüberwachung

MOBOTIX-Kameras Leistungsversprechen

- → Bereitstellung von zugelassenen Produkten (NIS-2, CRA, Cyber Security – Anforderungen) – die Kamera Cactus+ Edition ist bereits für kritische Infrastrukturen vorkonfiguriert.
- → Hohes KRITIS-Sicherheitsniveau garantiert: u.a. validierbares x.509 Zertifikat, erhöhter Identitäts- und Zugriffsschutz, Intrusion-Detection (Einbruchserkennung), Monitoring & Kameraausfall-Benachrichtigung.
- → Vertrauensvoller Service aus Deutschland: User-Training inklusive Alarm- und Ereignismanagement, DSGVO-konforme Videonutzung, Umgang mit Privacy-Zonen sowie Reporting und Dokumentation.

Der Aufbau eines autarken IT-Netzwerks zur Objektüberwachung ermöglicht den sicheren und unabhängigen Betrieb kritischer Sicherheitsfunktionen – losgelöst von produktiven Unternehmens- oder öffentlichen Netzen. Kameras, Melde- und Alarmsysteme sowie elektronische Schließ- und Zutrittssysteme werden in einem eigenständigen, abgeschotteten Netzwerk zusammengeführt und zentral gesteuert. Dadurch lassen sich Manipulationsrisiken, Abhängigkeiten und Ausfallwirkungen deutlich reduzieren.

Ein solches Netzwerk folgt dem Prinzip der digitalen Souveränität: Betreiber behalten jederzeit die Kontrolle über Datenflüsse, Zugriffe und eingesetzte Technologien. Segmentierung, rollenbasierte Zugriffssteuerung, verschlüsselte Kommunikation und lokale Management-Instanzen sorgen für hohe Sicherheit und Verfügbarkeit – auch bei Störungen externer Netze oder Cyberangriffen.

Der schrittweise Aufbau eines autarken Überwachungsnetzes stärkt eine resiliente Sicherheitsarchitektur, die kritische Objekte dauerhaft schützt und gleichzeitig die Grundlage für zukünftige Erweiterungen schafft.

Zur Realisierung einer IT-Vernetzung für die Objektüberwachung von Anlagen bzw. Betriebsgeländen kann ein autarkes IT-Netzwerk eingesetzt werden. Enthalten sind hier beispielsweise die Services: Confic-Service, Device-Service (Pairing), Login-Service, Rollout-Assistant, 4/5G Mobile Backup, Routing/Gateways, NAC/SIEM als Überwachung. Über ein NAC kann eine Portabschaltung erfolgen, ein optionales SIEM sorgt für ein Monitoring. Eine effiziente Objektüberwachung basiert auf einem autarken, segmentierten Netzwerk mit verschlüsselter Kommunikation, zentraler Steuerung und modularer Erweiterbarkeit.

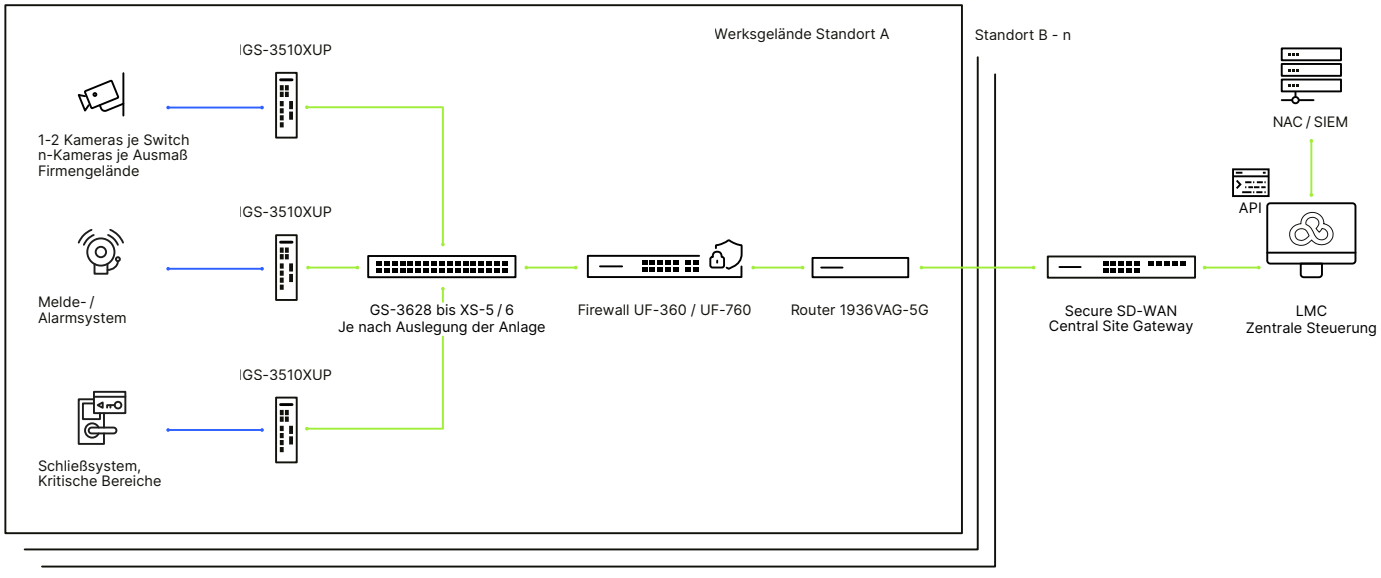


Abb. Exemplarische IT-Architekturskizze für die Objektüberwachung

Die Initiatoren des Hands-On Workshops

Mobotix steht seit 1999 für High-End-Videosysteme. Bereits der revolutionäre dezentrale Edge-Ansatz der ersten MOBOTIX IP-Kamera hat die Branche von Grund auf verändert. In der Tradition dieser Ingenieurskunst entwickeln, produzieren und programmieren wir Videosysteme und Software für wegweisende Komplettlösungen.

Durch MOBOTIX Videolösungen werden Unternehmen und Organisationen mit verwertbaren Daten versorgt, die die betriebliche Effizienz und die Sicherheit verbessern. Unseren Kunden möchten wir gezielt Nutzen stiften. Nutzen in Form von Sicherheit, Freiheit, Wachstum und Wohlstand. Wir sind fest entschlossen, die Welt jeden Tag ein kleines Stückchen besser zu machen.

LANCOM Systems ist führender europäischer Hersteller von sicheren, zuverlässigen und zukunftsfähigen Netzwerk- und Security-Lösungen (WAN, LAN, WLAN, Firewalls sowie Remote & Mobile Access) für Wirtschaft und Verwaltung. Das Unternehmen kombiniert Hardware-Geschäft mit virtuellen Netzwerkkomponenten und Cloud-basiertem Software-defined Networking (SDN). Daraus entsteht ein einzigartiges Angebot aus On-Premises- und Cloud-Lösungen mit einer zentralen Plattform für SD-WAN, Cloud-managed Networks & Security und SD-Branch.

Grouplink IT Solutions ist die erste Anlaufstelle für umfassende IT-Lösungen. Als langjährige Partner bieten wir verlässliche Strategien und Lösungen in den Bereichen Security, Infrastruktur & Cloud, Netzwerk, Managed Services, IT-Support sowie individueller Softwareentwicklung. Als strategischer Partner unterstützt die Grouplink IT Solutions Unternehmen in puncto Struktur, Sicherheit, Betrieb und Skalierung der eigenen IT.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de