SONDEREDITION für Freihoff Sicherheitsservice – inkl. Projekt-Checklisten und Ausblick KRITIS-Dachgesetz

Dallmeier

FREIHOFF 24 GRUPPE

VIDEOTECHNOLOGIE UND SICHERHEIT FÜR KRITISCHE INFRASTRUKTUREN

PRAXISLEITFADEN

Für Verantwortliche aus Organisationen der Kritischen Infrastruktur (KRITIS), für Planer, Channel-Partner, Facherrichter, Behörden und Politik

MADE IN GERMANY

See more.

INHALT

06/2023 . V1.0.1

EDITORIAL

Sehr geehrter Leser, sehr geehrte Leserin,

Kritische Infrastrukturen, kurz KRITIS genannt, haben in der öffentlichen Diskussion nochmals enorm an Aufmerksamkeit gewonnen. Ihre Bedeutung unter anderem für eine sichere Versorgung und für verlässliche öffentliche Prozesse ist gerade in den vergangenen Monaten nochmals stark in den Fokus gerückt.

Der Schutz von KRITIS ist eine gemeinsame Aufgabe von Unternehmen und dem Staat. Das KRITIS-Dachgesetz schafft einen einheitlichen Rahmen mit Mindestvorgaben für alle betroffenen Sektoren. Dieses Gesetz setzt ein Projekt aus dem Koalitionsvertrag um, um die Resilienz des Gesamtsystems zu stärken und für die Zukunft zu sichern.

Das Dachgesetz will kritische Infrastrukturen erstmals „systematisch und umfassend" identifizieren und „Mindestvorgaben im Bereich der physischen Sicherheit" vorschreiben. Als erste Priorität haben KRITIS-Betreiber, ob private Unternehmen oder öffentliche Einrichtungen, für ihre Geschäftsfähigkeit Sorge zu tragen.

Neben der IT-Sicherheit regelt der Gesetzestext erstmals auch den physischen Schutz. Der bislang verfolgte kooperative Ansatz wird dazu mit dem KRITIS-Dachgesetz durch verpflichtende Schutzstandards um die physische Sicherheit erweitert. Der Vorteil: Die Betreiber erhalten auf diese Weise mehr Orientierung und Handlungssicherheit.

Die öffentliche Hand übernimmt eine größere Verantwortung durch die Schaffung eines staatlichen Rahmens für Sicherheitsvorfälle und Kontrollen. Ein neues Meldewesen für die physische Sicherheit wird das bestehende Meldesystem zur KRITIS-Cybersicherheit ergänzen. Der Staat wird die Betreiber auch weiterhin umfassend unterstützen, indem er Analysen, Leitfäden, Beratung, Übungen und Schulungen anbietet.

Dabei handelt es sich um Handlungsfelder, in denen die Freihoff Gruppe technologisch führend, kompetent und leistungsstark aufgestellt ist. Unsere sicherheitstechnischen Lösungen befinden sich bereits bei einer Vielzahl von KRITIS-Betreibern zuverlässig im Einsatz. Wir freuen uns, Ihnen diesen Praxisleitfaden von Dallmeier und deren Consulting-Tochter davidIT exklusiv zur Verfügung stellen zu können. Das Dokument richtet sich an Beteiligte am Entscheidungsprozess, an Fachleute aus den Bereichen „Physische Unternehmenssicherheit", „IT- und Informations-sicherheit" und „Datenschutz", an angrenzende Fachverantwortliche, beteiligte Ausschreibungsinstanzen, Planer und Facherrichter, an Aufsichts- und Zuständigkeitsbehörden und an die ausführende und gesetzgebende Politik.

Wir hoffen, Ihnen damit wertvolle Impulse geben zu können.
Ich wünsche Ihnen eine anregende und aufschlussreiche Lektüre!

Ihr Frank Pokropp
Geschäftsführender Gesellschafter der Freihoff Sicherheitsservice GmbH

PS: Für einen persönlichen Austausch, für Ihre Fragen und Ihr Feedback stehen wir jederzeit gern zur Verfügung.

Sie erreichen uns unter Telefon 02173 10638-0 oder per E-Mail an info@freihoff.de

FREIHOFF 24 GRUPPE

1 KRITIS: ANGRIFFSZIEL UND GEGENSTAND DER WELTWEITEN SICHERHEITSPOLITIK

Kritische Infrastrukturen sind seit Beginn des Jahres 2022 verstärkt Angriffsziel und Gegenstand der weltweiten Sicherheitspolitik.

So berichtete das deutsche Nachrichtenmagazin „Der Spiegel“ im März 2022 von einem Sonderlagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI). Demnach könne Deutschland im Zusammenhang mit der russischen Invasion in der Ukraine zum Ziel für politisch motivierte Cyberattacken werden. Konkret war von sogenannten „Hochwertzielen“ die Rede, also von Schlüsselsektoren der deutschen Industrie.

Spätestens seit den Sabotage-Angriffen auf die Nord-Stream-Pipelines und auf die Steuerungskabel der Deutschen Bahn im Herbst 2022 erlangte der KRITIS-Schutz eine gesteigerte Aufmerksamkeit: bei den KRITIS-Betreibern, in der Bevölkerung, aber auch in der Politik. In der Folge legte das Deutsche Bundeskabinett am 7. Dezember 2022 „Eckpunkte für das KRITIS-Dachgesetz“ vor und machte damit klar: Bei KRITIS handelt es sich um Industriezweige, die der Staat durch besondere Maßnahmen – klassisch „physisch“ als auch digital „cybertechnisch“ – verstärkt und ganzheitlich schützen und regulieren muss.

Auf internationaler Ebene vereinbarten die NATO und die EU im Januar 2023 eine engere Kooperation zum Schutz kritischer Infrastrukturen, speziell vor dem Hintergrund der Risiken durch „autoritäre Akteure“.

„Lex Huawei“ und geplantes KRITIS-Dachgesetz als Sinnbild eines erhöhten geopolitischen Sicherheitsbewusstseins
Seit dem Erlass des IT-Sicherheitsgesetzes 2.0 im Mai 2021, das als sogenanntes Artikelgesetz unter anderem das BSI-Gesetz änderte, gelten für KRITIS-Betreiber neue, strengere IT-Sicherheitsauflagen. Der neu hinzugekommene KRITIS-Sektor „Siedlungsabfallentsorgung“ und die Gruppe „Unternehmen von besonderem öffentlichem Interesse (UBI)“ sind davon ebenfalls betroffen. Auch der Kreis und die Anzahl der betroffenen und regulierten Unternehmen hat sich durch neue Definitionen und Schwellenwerte erhöht. Erstmalig nimmt der Paragraf § 9b BSI-Gesetz auch wahlweise Hersteller bzw. Vorlieferanten von kritischen Komponenten beim Einsatz in KRITIS in die rechtliche Pflicht, Stichwort „Prüfung auf Vertrauenswürdigkeit“ und „Garantieerklärung“. In der Öffentlichkeit ist dies besser bekannt als „Lex Huawei“ im Zusammenhang mit dem Aufbau des 5G-Mobilfunknetzes in Deutschland.

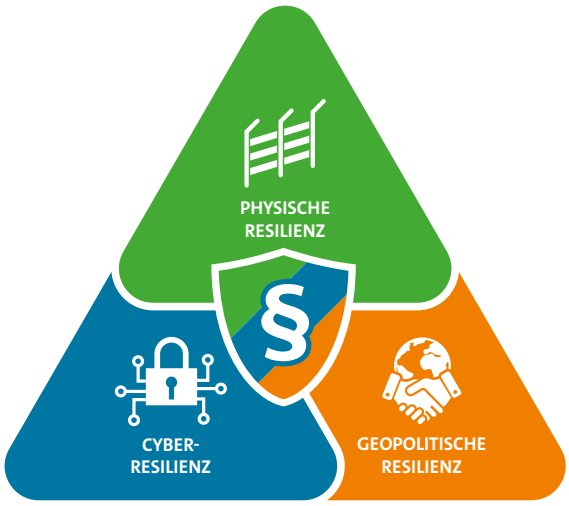
Der aktuelle KRITIS-Gesetzesrahmen ist im BSI-Gesetz kodifiziert, v. a. in den Paragrafen 8a ff. sowie in der KRITIS-Verordnung. Für das Jahr 2023 ist die Verabschiedung des KRITIS-Dachgesetzes angekündigt (siehe Kap. 3.4), welches erstmalig auch den physischen Schutz von KRITIS regulieren soll.

Es geht um die Souveränität Europas
Die schreckliche geopolitische Eskalation im Februar 2022 führt der Weltgemeinschaft offen vor Augen, dass Kritische Infrastrukturen, allen voran Energieversorgung, Informationstechnologie und Telekommunikation sowie Transport und Verkehr neben ihren eigentlichen funktional-technischen Aufgaben zudem geostrategische, geopolitische und sicherheitspolitische Bedeutung erlangen. Frieden und Rechtsstaatlichkeit sind plötzlich für die Industrie, v. a. die Kritische Infrastruktur, kein selbstverständlicher Rahmen mehr. Sie bedingen sich augenscheinlich gegenseitig. Die technische und geopolitische Integrität der Kritischen Infrastrukturen werden zu „Verhandlungsmasse" für Frieden und Rechtsstaatlichkeit in der Welt. Es geht also bei Kritischen Infrastrukturen nicht nur um die technologische und digitale, sondern auch um die ökonomische und politisch-völkerrechtliche Souveränität Europas.

> *„Probleme kann man niemals mit derselben Denkweise lösen, durch die sie entstanden sind."*
>
> **Albert Einstein,** Physiker

Die herausfordernde Aufgabenstellung für KRITIS-Betreiber, Technologiehersteller und Politik

1.1 DAS KRITIS-RESILIENZDREIECK



Das KRITIS-Resilienzdreieck (mit begleitender, staatlicher Regulatorik)

Ganz im Sinne von Einsteins Forderung wollen wir als Hersteller Dallmeier mit gutem Beispiel vorangehen und nachfolgend nicht vom KRITIS-Bedrohungsdreieck, sondern mit positiver Denkweise vom KRITIS Resilienzdreieck sprechen. Infolgedessen möchten wir mit diesem Praxisleitfaden und mit unseren Videolösungen zu mehr KRITIS-Sicherheit und Schutz und zur Problemlösung bzgl. aller Dimensionen des Resilienzdreiecks beitragen, ganz im Sinne von Einsteins mahnenden Worten. Und natürlich im Sinne aller KRITIS-Betreiber.

Nachfolgend beleuchten wir die Widerstandsfähigkeit gegen die einzelnen „Bedrohungen" und „Risiken".

1.1.1 KONVENTIONELLE UND PHYSISCHE BEDROHUNGEN

Die konventionellen Bedrohungen fallen dabei vorwiegend in den Bereich der sogenannten „Physischen Unternehmenssicherheit“. Beispiele hierzu sind Bedrohungen durch Einbruch, Diebstahl, Spionage, Sabotage und Vandalismus.

Hier trägt die Leistungsfähigkeit moderner Videotechnik immer erfolgreicher dazu bei, schwere Straftaten und Spionage- oder Sabotagevorfälle zu verhindern bzw. diesen vorzubeugen oder sie nachträglich aufzuklären. Die Fortschritte in der Bildqualität und die Möglichkeit der immer größeren Flächen- und Distanzabdeckung durch spezialisierte Videosysteme, wie z. B. die Multifocal-Sensortechnologie, steuern hierzu einen entscheidenden Beitrag bei, ebenso wie die KI-basierte Videoanalyse.

Reduzierung von Falschalarmen durch KI- und videobasierten Perimeterschutz im Rahmen einer „Safe KRITIS Strategie“.

1.1.2 CYBERBEDROHUNGEN

Dieser Praxisleitfaden behandelt die physische Sicherheit mit Schwerpunkt auf Videoüberwachung oder Videobeobachtung. Das Thema Cybersecurity wurde und wird zurecht in großem Umfang andernorts behandelt. Nichtsdestotrotz gibt es aber hier einen Zusammenhang mit der physischen Sicherheit: Als netzwerkbasierte Systeme sind alle Videosicherheitslösungen grundsätzlich vulnerabel gegenüber Cyberangriffen, so wie auch sonstige IT-Systeme. Deshalb lautet eine zentrale Frage, der sich KRITIS-Betreiber stellen müssen:

Sind IP-basierenden Video-Systeme selbst cybersicher und vertrauenswürdig bezogen auf oben genannte Resilienzkriterien?

- Insbesondere Cyberbedrohungen durch technische Vulnerabilities, absichtliche und unabsichtliche Backdoors, mangelnde technische Vorkehrungen zur Absicherung
- Einflussnahme durch Investoren und Hersteller aus Drittstaaten

CYBERSICHERHEITSTIPP — LIEFERKETTE

DAS SCHWÄCHSTE GLIED ENTSCHEIDET – AUCH UND INSBESONDERE IN DER LIEFERKETTE

Da Videosysteme Teil der IT-Gesamtinfrastruktur der KRITIS sind, gilt folgender allgemein bekannter Sicherheitstipp:

„Eine KRITIS-Sicherheitskette ist nur so stark wie ihr schwächstes Glied."

IT-SICHERHEITSGESETZ: VORLIEFERANTEN SIND EBENFALLS IN DER PFLICHT

Cybersecurity ist nach dem IT-Sicherheitsgesetz 2.0 nicht nur eine Pflicht-Anforderung für die KRITIS-Betreiber selbst, sondern in bestimmten Fällen auch für Hersteller/Vorlieferanten von Hardware und Software in der ganzen KRITIS-Lieferkette.

Seit 2022 müssen auch Hersteller von IT-Produkten als Vorlieferanten von KRITIS-Betreibern bei „Kritischen Komponenten" eine Garantieerklärung lt. § 9b Absatz (3) BSIG abgeben. In dieser muss dargelegt werden, wie das jeweilige IT-Produkt vor Cyberbedrohungen, Terrorismus, Spionage oder Sabotage geschützt ist.

DIE HERAUSFORDERUNG UND AUFGABENSTELLUNG FÜR KRITIS-BETREIBER

Netzwerkbasierte Videosicherheitsprodukte für die physische Sicherheit (z. B. für Perimeterschutz, Gebäudeschutz) dürfen NICHT die „andere", die komplementäre Sicherheit der KRITIS-Betreiber, nämlich die IT- und Cybersicherheit, gefährden.

Vorlieferanten von KRITIS müssen „Security und Privacy by Design"-Prinzipien einhalten.

„Made in Germany" wird wieder verstärkt als Gütesiegel für Qualität, Sicherheit und Vertrauen nachgefragt.

1.1.3 INVESTOREN UND HERSTELLER AUS DRITTSTAATEN

Bei der Bedrohung durch Investoren aus einem Drittstaat sei hier kurz der Fall der versuchten Übernahme des deutschen Stromnetzanbieters „50 Hertz“ durch einen chinesischen Staatskonzern im Jahre 2018 erwähnt. Die Übernahme wurde politisch und gesellschaftsrechtlich durch einen Ankauf von Anteilen an 50 Hertz durch die KfW verhindert.

Weitere Informationen: Investor Drittstaat - Fall 50 Hertz

Grundsätzlich gibt es neben dem Umweg über staatliche Anteilsaufkäufe auch Handlungsmöglichkeiten der Exekutive, direkte Auslandsinvestitionen von Investoren aus Drittstaaten im Einzelfall durch unmittelbare regulatorische Eingriffe zu prüfen und zu verhindern, wenn es um die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland geht.

Rechtsgrundlagen stellen hierbei das Außenwirtschaftsgesetz (AWG, speziell § 4 Abs. 1 Nr. 4 AWG) und die auf dessen Grundlage erlassene Außenwirtschaftsverordnung (AWV, speziell § 55 AWV) dar.

Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob das inländische Unternehmen Betreiber einer Kritischen Infrastruktur im Sinne des BSI-Gesetzes ist. (§ 55a AWV)

Zuerst Hersteller/Vorlieferant, dann Investor: Das Beispiel Gazprom
Ein Beispiel für eine politisch bzw. rechtlich nach AWG und AWV nicht verhinderte Direktinvestition in eine Kritische Infrastruktur (Energieversorgung) stellt der Fall Gazprom dar. Gazprom war über Jahre hinweg zuerst nur Hersteller/Vorlieferant von Gas, dann durch Kauf von deutschen Gasspeichern im Jahre 2015 auch zusätzlich Investor.

Die Abhängigkeiten und Folgen sind bekannt – von daher ist das BMWi eingeschritten und hat die Bundesnetzagentur als Treuhänderin bestellt. Diese Bestellung basiert auch auf dem oben genannten Außenwirtschaftsgesetz und der Außenwirtschaftsverordnung.

Weitere Informationen: Investor Drittstaat – Fall Gazprom

Hersteller aus Drittstaaten: Das Beispiel Huawei
In der jüngeren Vergangenheit erlangte 2020 in Deutschland der folgende Abwägungsfall öffentliche Aufmerksamkeit: „Darf der chinesische Hersteller Huawei einer der Netzausrüster sein und kritische Komponenten für das deutschlandweite 5G-Mobilfunknetz liefern?“

Es mussten die obigen KRITIS-Bedrohungen „Cyber“ und „Hersteller aus Drittstaaten“ gegen den Nutzen und technischen Vorteil der Huawei-Lösung sorgfältig gegeneinander abgewogen werden.

Beim 5G-Ausbau hat Deutschland kein explizites Huawei-Verbot erlassen, sondern mit dem IT-Sicherheitsgesetz 2.0, konkret mit § 9b Absatz (3) BSIG, eine Vertrauenswürdigkeitsprüfung (Garantieerklärung) eingeführt, die für alle Anbieter aus anderen Ländern gilt. Am Ende ließ die Politik Huawei & Co. also dennoch ein (gesetzliches Hinter-) Türchen offen. In anderen Ländern wie z. B. Kanada wurde beim Aufbau des 5G-Netzes die Technologie von Huawei verboten.

Kritische KRITIS-Anmerkungen zur Drittstaatenbedrohung
Ob dieses gesetzliche (Hinter-)Türchen „der einzelfallbezogenen Vertrauenswürdigkeitsprüfung (Garantieerklärung)“ von Herstellern nach dem Kriegsbeginn Russlands gegen die Ukraine und der Erkenntnis über einseitige Abhängigkeiten in Schlüsseltechnologien und Schlüsselenergien wie z. B. Gas von der handelnden Politik noch genauso gesehen wird, bleibt an dieser Stelle offen und spannend. Seit Mitte des Jahres 2022 gibt es bereits Tendenzen in der deutschen Regierung zu einem gesetzlich-nachträglichen Verbot der chinesischen Huawei-Technologie beim 5G-Netzausbau (nach § 9b Absatz (2) BSIG).

Diese Tendenz wird per Stand März 2023 (Redaktionsschluss Praxisleitfaden V1.0.0) durch aktuelle Berichte bekräftigt. Das Handelsblatt (online) schreibt am 07.03.2023: „5G-NETZ: Bundesregierung plant Huawei-Verbot“

Weitere Quellen zum geplanten Huawei-5G-Verbot: ZEIT ONLINE (03_2023) und heise online (03_2023).

Anmerkung Gesamtkontext:
Für die handelnde Politik gilt es natürlich, parallel zu gesetzlich-regulatorischen Einzelfallentscheidungen, die wirtschaftspolitische „Gesamtgemengelage“ mit bilateralen und multilateralen Geschäftsinteressen und Abhängigkeiten zu berücksichtigen. Die Frage nach der richtigen Kooperations- bzw. Wettbewerbsstrategie bzgl. (autoritären) Drittstaaten wird für die Politik und Wirtschaft aus unserer heutigen Sicht ein Balanceakt, der diese Dekade prägen wird.

Aus der Praxis: Verbot einiger Videotechnikhersteller
Die USA haben im Jahr 2019 im Kontext der zwei Bedrohungslagen Cyber und Geopolitik per NDAA (National Defense Authorization Act) den Einsatz von Videoüberwachungsgeräten zweier großer chinesischer Videotechnik-Hersteller bei Projekten verboten, die die öffentliche Sicherheit, die Sicherheit von Regierungseinrichtungen und die Sicherheit Kritischer Infrastrukturen betreffen.

In anderen Ländern wie Großbritannien, Australien, Dänemark, Norwegen, Italien und evtl. bald auch in Deutschland (siehe *) sind artähnliche, staatlich verordnete regulatorische Verbotstendenzen bezüglich chinesischer Herstellerprodukte zu beobachten. Begründet werden diese Verbote und Regulierungen mit Sicherheitsbedenken und Bedenken bzgl. einer potentiellen drittstaatlichen Durchgriffsmöglichkeit z. B. durch staatlich angeordnete Backdoors oder Drittstaaten-Trojaner. Darüber hinaus spielen ethische Gründe eine zunehmend beeinflussende Rolle. Im Kontext dieser geopolitischen Risiken, die von autoritären Akteuren ausgehen, haben die NATO und die EU im Januar 2023 eine engere Kooperation beim Schutz von KRITIS vereinbart.

(*) Prüfungs-und Verbotstendenzen in Deutschland bzgl. Videotechnik(hersteller) zum Zeitpunkt März 2023:

1) Spionagevorwürfe gegen China: Baden-Württemberg prüft Ausschluss chinesischer Produkte

2) Überwachung in Deutschland – made in China*: Einige Länder haben den Einsatz der Kameras aus Sicherheitsgründen bereits eingeschränkt, Deutschland hingegen noch nicht. Wie gefährlich ist das für die Kritische Infrastruktur?*

3) Datensicherheit: Das Risiko mit Überwachungskameras aus China

2 PERSONALMANGEL GEFÄHRDET SICHERHEIT UND BUSINESS CONTINUITY

Seit dem 1. Halbjahr 2022 haben KRITIS-Betreiber zusätzlich zu den klassischen Bedrohungen auch noch mit massivem Personalmangel als zusätzliches Problem bzgl. Sicherheit und Business Continuity zu tun.

Als eines von vielen Beispielen sei der massive Personalmangel im KRITIS-Sektor „Transport und Verkehr" – Subbranche Flughäfen – seit Mitte 2022 hier aufgeführt. Der Presseartikel „Luftverkehr: Kein Ende des Chaos an Flughäfen in Sicht" aus der ZEIT Online von Juni 2022 beschreibt die Situation und das Problem exemplarisch.

Aus der Sicht eines Praxisleitfadens stellt sich das Thema „Personalmangel und ein möglicher Lösungsansatz" in neutraler und schematischer Darstellung wie folgt dar:

Das Problem

- Sicherheit, Resilienz und Business Continuity in KRITIS gefährdet
- Personalmangel darf nicht auf Kosten der Sicherheit gehen

Die Forderung nach Ergänzung bzw. Substitution durch Technik (Zitat)
Beispiel Deutsche Lufthansa (Lufthansa-Vorstand Detlef Kayser, zuständig für Flotten und Infrastruktur, aus Frankfurter Allgemeine Zeitung – FAZ Online, 03.07.2022):

> *„Es gibt hochmoderne Scanner-Technik,*
>
> *die die Sicherheitskontrollen deutlich beschleunigen würde."*
>
> **Detlef Kayser,** Lufthansa-Vorstand

Videotechnik in vielen Fällen als Teillösung

- Videotechnik und KI-basierte Video- und Datenanalyse können in vielen Bereichen KRITIS-Prozesse vereinfachen oder automatisieren
- z. B. durch virtuelle Guards, Intrusion-Detection, Crowd-Detection, Objekt-Counting, Objekt-Klassifizierung, Heatmaps etc.

- Beispiel Virtueller Guard per Videotechnik:
  Alternative zum klassischen Wachdienst für Gewerbeobjekte, zudem noch wirtschaftlicher

- Zu diesem Lösungsmotto siehe zum Beispiel branchenbezogene Lösungen für Prozessautomatisierungen auf Basis von smarter Videoanalyse- und KI-Technologie.

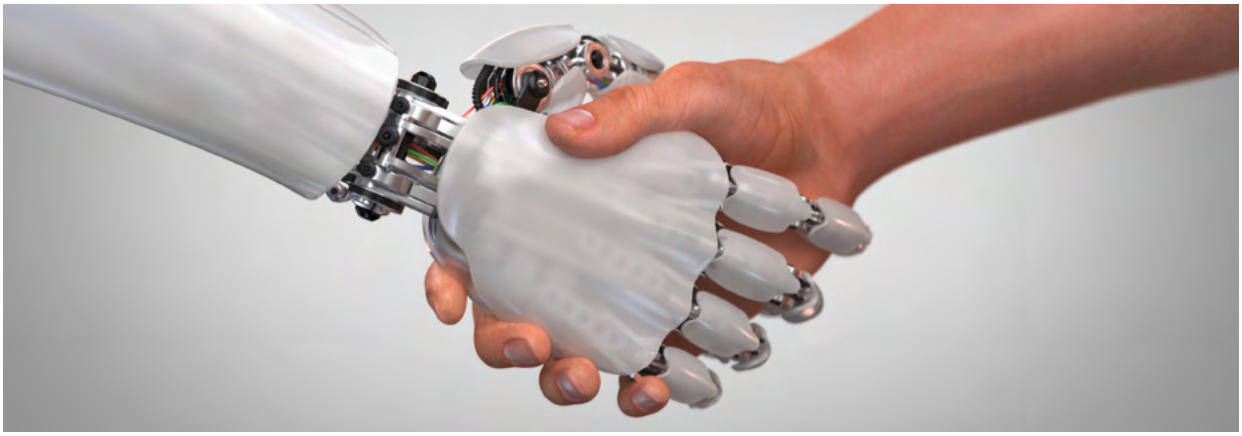
2.1 AUTOMATISIERUNG PER VIDEOTECHNIK ALS AUSWEG UND CHANCE

An dieser Stelle sei auf einen aus unserer Sicht treffenden Artikel zu Personalmangel und möglicher Auswege aus dem Dilemma im Handelsblatt, bereitgestellt über XING (Juli 2022), verwiesen. In der Überschrift wird wie folgt formuliert: „Flughafenchaos und Handwerker-Mangel: Letzter Ausweg Automatisierung“.

Im genannten Artikel werden 3 Auswege aus Personalmangel zur Diskussion gestellt:

- Längere Arbeitszeit
- Mehr Zuwanderung
- Mehr Automatisierung

Roboter oder Algorithmen, Künstliche Intelligenz (KI) und smarte Videotechnik können aus unserer fachlichen Sicht durchaus in einigen Bereichen die manuellen Tätigkeiten der fehlenden Arbeitskräfte automatisiert ausführen. Wenn auch keine Gesamtlösung, so bietet die Automatisierung von geeigneten KRITIS-Prozessen per Videotechnik einen Ausweg bzw. eine Verbesserung der Situation in Zeiten des Personalmangels.



Automatisierungspotenziale durch Videotechnik

Arbeitgeberpräsident Rainer Dulger prognostizierte im Juni 2022 im Kontext des Personalmangels folgendes „selbstsprechendes Bild“:

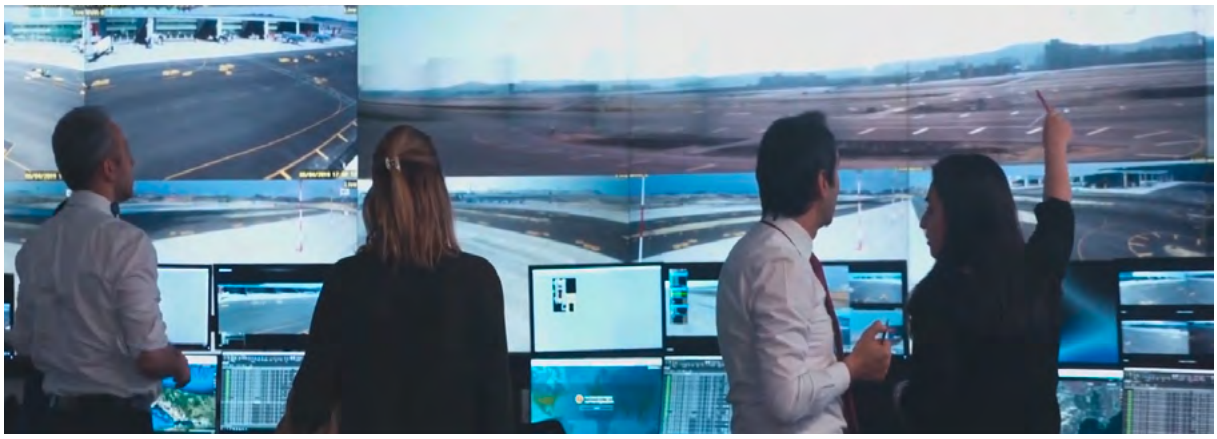
> *„Wir werden bald nicht über (Arbeits)losigkeit sprechen, sondern über (Arbeiter)losigkeit.“*
>
> **Rainer Dulger,** Arbeitgeberpräsident

Die Herausforderung und der Lösungsvorschlag

- Sicherheitsniveau und Business Continuity (hoch-) halten mit smarter Videosicherheitstechnologie
- Die durch Personalmangel hervorgerufenen Geschäftsprozessstörungen durch Videotechnik verkleinern, verhindern bzw. beheben: Überall dort, wo Videotechnik als Substitut in Frage kommt
- Dazu bietet sich eine Mehrfachnutzung der Kamerabilder an:
    - für Sicherheit
    - für Geschäftsprozessautomatisierung und Business Continuity (v. a. in kritischen KRITIS-Bereichen)
    - für zusätzliche Geschäftsdaten- und Informationsgenerierung
    - für eine fundierte, datenbasierte, faktenbasierte und zeitkritische Entscheidungsfindung

Drei Beispiele für intelligente Videotechnik zur Automatisierung von KRITIS-Geschäftsprozessen

- Sektor Transport und Verkehr – Luftfahrt – Airport Istanbul – Virtual Tower



ISTANBUL AIRPORT: Mit dem „Virtual Tower"-Konzept lassen sich Flugzeugbewegungen auf dem IGA aus der Ferne verfolgen. Durch den Einsatz von „Multifocal-Sensortechnologie" verbessert der IGA die Übersicht und ermöglicht es einer beliebigen Anzahl von „Stakeholdern" gleichzeitig auf Gesamt- und Detailansichten aller relevanten Airport-Bereiche zuzugreifen. Bildnachweis: Istanbul Airport

- Sektor Transport und Verkehr – Binnenschifffahrt/Seeschifffahrt – Hafen

Eine Lösung zur automatischen Schiffserkennung unterstützt unter anderem Hafenanlagenbetreiber und Raffinerien Auflagen zur Gefahrenabwehr gemäß ISPS-Code zu erfüllen. Neben der Gefahrenabwehr ist das Optimieren von Workflows in Hafengebieten ein weiterer Einsatzbereich einer aktuellen Videoanalyse-App. Bildnachweis: Dallmeier electronic

- Sektor Transport und Verkehr – Schienenverkehr – Dänische Staatsbahn

Die Videosicherheitslösung bei den Dänischen Staatsbahnen erlaubt es beliebig vielen Operatoren von der DSB-Hauptzentrale in Kopenhagen aus individuell auf die Videobilder sämtlicher Standorte zuzugreifen. Umfassende Darstellungs- und Vorfallsmanagement-Funktionen gewährleisten die effiziente Verfolgung, Intervention und Aufklärung eines Geschehnisses.

Der Return on Video-Investment für KRITIS

Mit einem smarten Video-Lösungspaket erreichen KRITIS-Betreiber folgende technischen und kaufmännischen Ziele:

Der Return on Video-Investment für KRITIS
(Teil)automatisierung per smarter, KI-gestützter Videotechnologie erhöht die objektive Sicherheit und steigert die Produktivität .

PRAXISKOMMENTAR — AUTOMATISIERUNG DURCH TECHNIK

GESAMTGESELLSCHAFTLICHER SINNENSWANDEL ZUR „AUTOMATISIERUNG DURCH TECHNIK“ NÖTIG

Zusätzlich zu den technischen Innovationen und dem technologischen Fortschritt wäre auch ein gesellschaftliches und unternehmerisches Umdenken nötig. Das herrschende Narrativ von der Arbeitsplatzvernichtung durch smarte Automatisierungstechnik mag durchaus für einige Jobs gelten, aber bei der mittel- und langfristig prognostizierten Personalnot sollte aus unserer Sicht nicht die Gefahr, sondern die große Chance zum Produktivitätsfortschritt, zur Schaffung neuer Arbeitsplätze in anderen KRITIS-Bereichen und zur Automatisierung durch (Video-)Technik gesehen werden.

3 KRITISCHE INFRASTRUKTUREN

3.1 EINTEILUNG KRITISCHER INFRASTRUKTUREN

Kritische Infrastrukturen sind laut Bundesamt für Sicherheit in der Informationstechnik (BSI) wie folgt definiert: Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Sektoren Kritischer Infrastrukturen:
Alle Organisationen aus diesen 10 Sektoren zählen **unabhängig von ihrer Größe** zu den Kritischen Infrastrukturen.

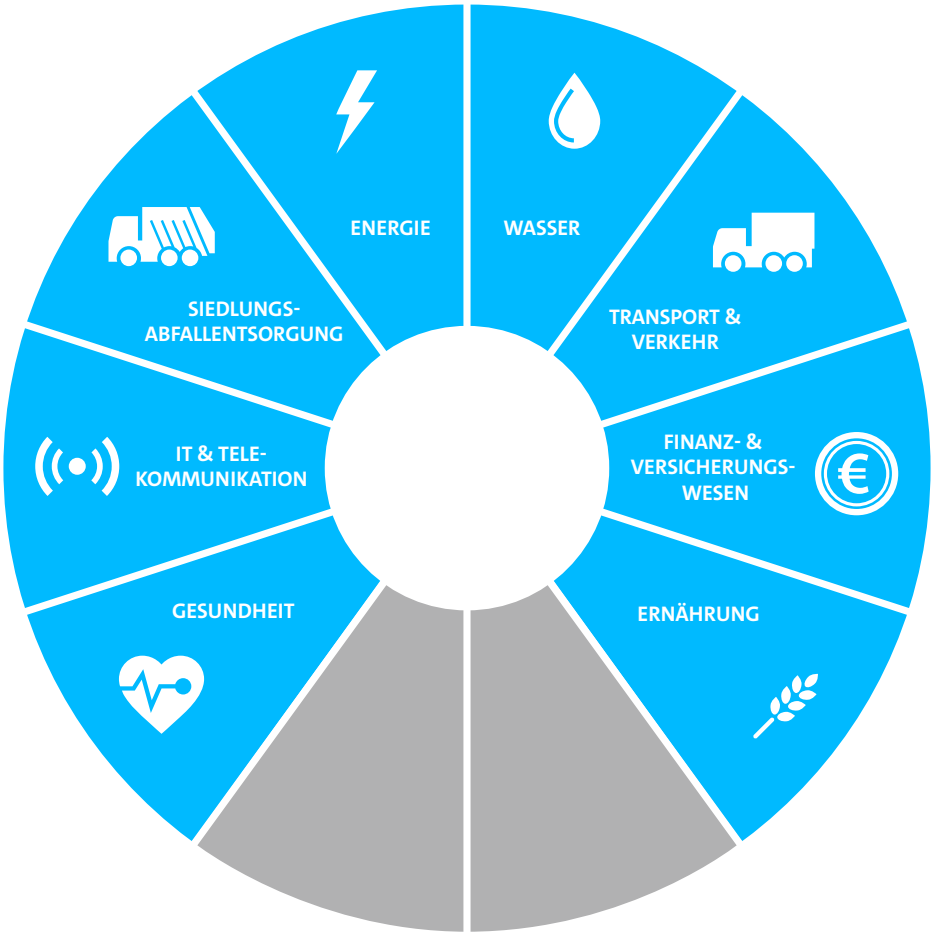
Die aktuellen 10 KRITIS-Sektoren

Das BSI-Gesetz (BSIG) reguliert nur 8 KRITIS-Sektoren

Gemäß § 2 Absatz 10 BSIG sind Kritische Infrastrukturen im Sinne des BSIG „Einrichtungen, Anlagen oder Teile davon, die den Sektoren...

Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören...

...und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“ (in kurzen Worten: kritische Dienstleistungen erbringen)



Die 8 durch das BSIG regulierten KRITIS-Sektoren

Fazit:
Die Sektoren „Staat und Verwaltung“ sowie „Medien und Kultur“ unterliegen nicht der Regulierung durch das BSIG.

Welche Organisationen und Unternehmen („Größenklassen“) fallen unter regulierte KRITIS?
Nach Verabschiedung des BSIG wurde vielerorts die Frage gestellt, welche Unternehmen konkret zu den Betreibern einer Kritischen Infrastruktur im Sinne des BSIG gehören.

Die letztlich regulierten Kritischen Infrastrukturen und die letztlich regulierten Organisationen und Unternehmen werden durch **Rechtsverordnung** nach § 10 Absatz 1 BSIG näher bestimmt.

Diese Rechtsverordnung heißt: BSI-Kritisverordnung
„Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“, kurz BSI-Kritisverordnung (BSI-KritisV).

Die BSI-Kritisverordnung definiert zu überschreitende Schwellenwerte (Art „Größenklassen“), Anlagen, Betreiber, Versorgungsgrad und die Frage „was sind kritische Dienstleistungen“.

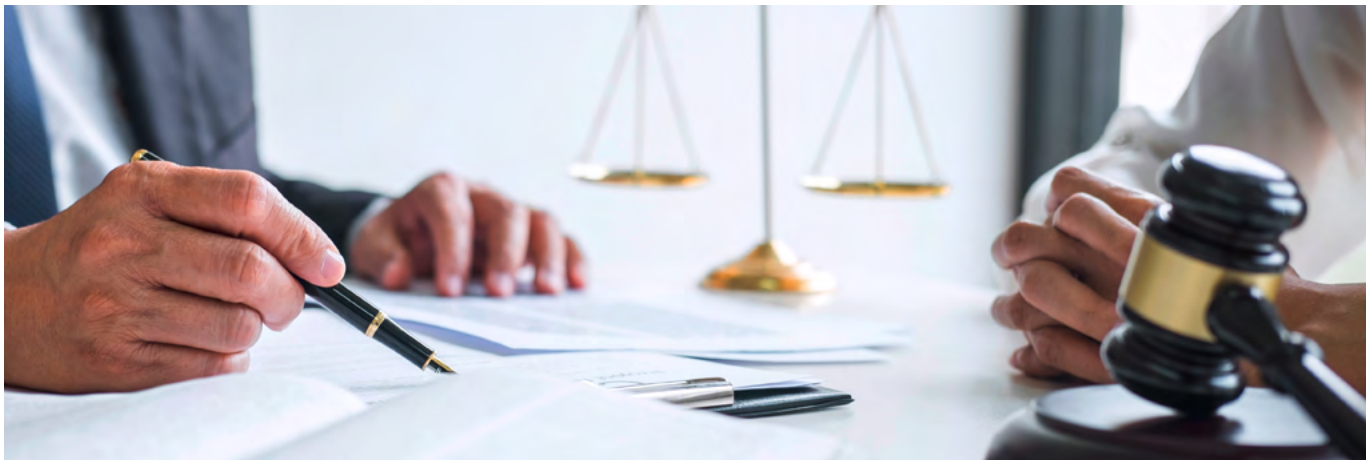
Werden die definierten Schwellenwerte und Kriterien erreicht oder überschritten, gelten für KRITIS-Betreiber die gesetzlichen Melde- und Nachweispflichten des BSIG.

Das BSI empfiehlt den Umsetzungsplan KRITIS („UP KRITIS“) als Kür
Auch wenn die Anlagen die Schwellenwerte der BSI-Kritisverordnung unterschreiten, empfiehlt das BSI die (freiwillige) Teilnahme am UP KRITIS. Der UP KRITIS (UP steht für Umsetzungsplan) ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen.

3.2 ZUSTÄNDIGE AUFSICHTSBEHÖRDE BSI, GESETZE UND VERORDNUNGEN IM DETAIL

Das Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Jahr 1991
- BSI lt. Website: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland.
- BSI lt §1 BSIG: Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene.
- Das BSI arbeitet auf Grundlage unterschiedlicher (spezial-)gesetzlicher Regelungen und Verordnungen auf nationaler und europäischer Ebene.
- Eine Auswahl dieser Regelungen wird auf diesen Seiten vorgestellt.



Das BSI-Gesetz (BSIG)

- Jahr 2009 (seitdem mehrmals novelliert, v. a. 2015/2021)
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI)
- BSIG regelte ursprünglich nur die Errichtung und Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik
- In der aktuellen Fassung regelt das BSIG auch, wer Adressat von besonderen Sicherheitspflichten ist
- Das BSIG ist das „maßgebliche KRITIS-Gesetz", d. h. es definiert v. a. in den Paragrafen 8a ff die Sicherheit in der Informationstechnik Kritischer Infrastrukturen
- Das BSIG definiert dabei die Sicherheitsanforderungen an die Betreiber der KRITIS und NEU seit 2022 auch die Sicherheitsanforderungen an Hersteller/ Vorlieferanten von kritischen Komponenten
- Das BSIG wird durch das IT-Sicherheitsgesetz geändert
- Gesetzestext im Wortlaut: BSI-Gesetz/BSIG

Das IT-Sicherheitsgesetz 1.0 (IT-SiG)

- Jahr 2015
- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- Das IT-SiG ändert als reines Änderungs- / Artikelgesetz neben dem BSI-Gesetz auch das Energiewirtschaftsgesetz, das Atomgesetz, das Telemediengesetz, das Telekommunikationsgesetz und weitere Gesetze
- Es definiert auch erweiterte Kompetenzen, Aufgaben und Befugnisse des BSI
- Mit verbindlichen Mindestanforderungen an die IT-Sicherheit verbessert es vor allem den Schutz der Kritischen Infrastrukturen
- Definiert Pflichtenkatalog für KRITIS-Betreiber:
  - Stand der Technik bzgl. IT-Sicherheit umsetzen
  - Kontaktstelle für das BSI benennen
  - Regelmäßige Nachweise zur IT-Sicherheit erbringen
  - IT-Störungen an das BSI melden
- Gesetzestext im Wortlaut: IT-Sicherheitsgesetz 1.0

Die NIS-Richtlinie der Europäischen Union

- Jahr 2016
- NIS = Netz- und Informationssicherheit
- Die NIS-Richtlinie ist das erste EU-weite Gesetz zur Cybersicherheit. Sie sieht rechtliche Maßnahmen vor, um das Gesamtniveau der Cybersicherheit in der EU zu verbessern.
- Im August 2016 trat die Gesetzesrichtlinie in Kraft, wobei die Umsetzung in nationales (z. B. deutsches Recht) bis Mai 2018 erfolgen musste.
- Der deutsche Gesetzgeber war mit dem IT-Sicherheitsgesetz 1.0 im Jahr 2015 also bereits in Vorleistung getreten, d. h. der EU-Richtlinie einen Schritt bzw. ein Jahr voraus.
- Als Vorreiter musste Deutschland sein IT-Sicherheitsgesetz nur minimal nachbessern zur Erfüllung der EU-NIS-Richtlinie.
- Gesetzestext im Wortlaut: NIS-Richtlinie
- Beispiel Österreich:
    - 2018 ist in Österreich das Netz- und Informationssicherheitssystemgesetz NISG in Kraft getreten, mit welchem die europäische NIS-Richtlinie in österreichisches Recht umgesetzt wurde.
    - Das NISG ist das österreichische Pendant zum deutschen IT-Sicherheitsgesetz (und BSI-Gesetz)

Die KRITIS-Verordnung 1.0

- Jahr 2016/2017
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
- BSI-Kritisverordnung – BSI-KritisV
- Nach Verabschiedung des IT-Sicherheitsgesetzes wurde vielerorts die Frage gestellt, welche Unternehmen konkret zu den Betreibern einer Kritischen Infrastruktur im Sinne des IT-Sicherheitsgesetzes gehören.
- Die BSI-Kritisverordnung 1.0 konkretisiert die Ausführungen vom IT-Sicherheitsgesetz 1.0 bzw. vom BSI-Gesetz und definiert Schwellenwerte, Anlagen und Vorgaben („Wer gehört zu Kritis?“).
- Gesetzestext im Wortlaut: BSI-KritisV

Das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)

- Jahr 2021, im Mai 2021 in Kraft getreten
- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- Mit dem IT-Sicherheitsgesetz 2.0 wurde der Auftrag des BSI 2021 erneut erweitert
- Zudem räumt das IT-SiG 2.0 dem BSI weitere Befugnisse gegenüber der Bundesverwaltung ein.

- Das IT-Sicherheitsgesetz ändert als sogenanntes Artikelgesetz neben dem BSIG das TKG, das TMG oder das Energiewirtschaftsgesetz
- Gesetzestext im Wortlaut: IT-Sicherheitsgesetz 2.0
- Siehe gesondertes Detail-Kapitel zum IT-Sicherheitsgesetz 2.0 (Kap. 3.3)

Die KRITIS-Verordnung 2.0

- Jahr 2021
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
- BSI-Kritisverordnung – BSI-KritisV
- Die BSI-Kritisverordnung 2.0 konkretisiert die Ausführungen von IT-Sicherheitsgesetz 2.0 bzw. BSI-Gesetz und definiert Schwellenwerte, Anlagen und Vorgaben („Wer gehört zu Kritis?").
- Gesetzestext im Wortlaut: BSI-KritisV (2.0)

Die CER-Richtlinie „Resilienz kritischer Infrastrukturen" der Europäischen Union

- November 2022: EU Parlament nimmt neue Regeln zum Schutz und Resilienz kritischer Infrastruktur in der EU an
- Offizielles Dokument RICHTLINIE (EU) 2022/2557 „Über die Resilienz kritischer Einrichtungen" (Sprachauswahlseite | Deutsche Fassung PDF)
- EU-Staaten müssen CER bis Oktober 2024 in nationales Recht überführen; in Deutschland womöglich mit dem KRITIS-Dachgesetz

Die NIS-2-Richtlinie der Europäischen Union

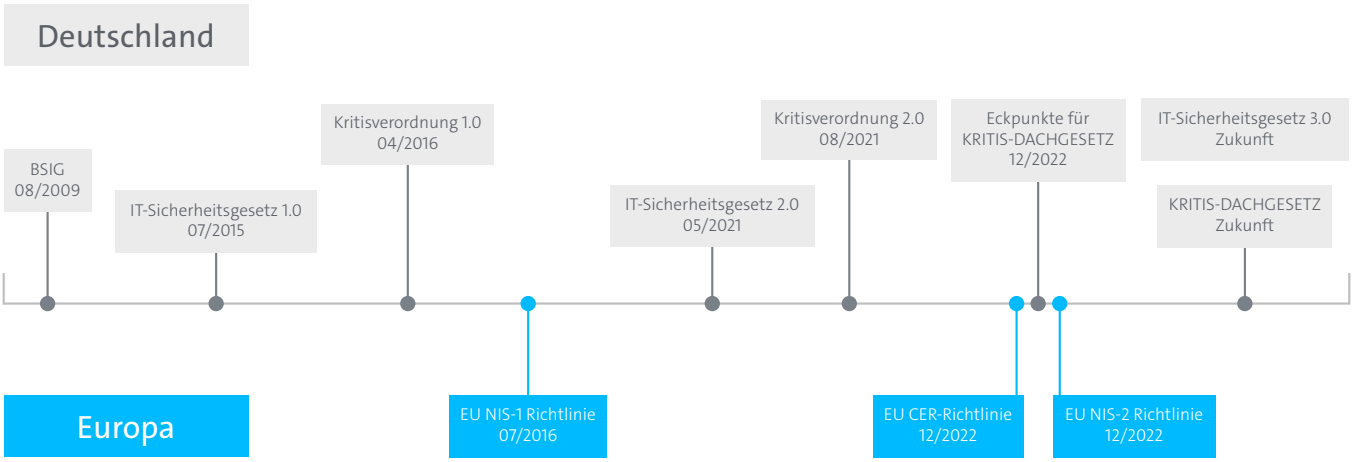
- Der neue NIS-2-Vorschlag der EU-Kommission zielt darauf ab, die Mängel der früheren NIS-Richtlinie zu beheben, sie an den aktuellen Bedarf anzupassen und zukunftssicher zu machen.
- November 2022: EU NIS-2-Richtlinie zur Cybersicherheit tritt in Kraft
  - EU Parlament online: Das EU-Parlament und der Rat haben im November 2022 dem NIS-2 Entwurf zugestimmt
  - Offizielles Dokument RICHTLINIE (EU) 2022/2555 „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union" (Sprachauswahlseite | Deutsche Fassung PDF)
  - EU-Staaten müssen NIS-2 bis Oktober 2024 in nationales Recht überführen; in Deutschland womöglich mit einem IT-Sicherheitsgesetz 3.0

KRITIS-Dachgesetz (geplant für das Jahr 2023)

- 07.12.2022: Bundesregierung verabschiedet die Eckpunkte des KRITIS-Dachgesetzes
- Webseite BMI: Eckpunkte für das KRITIS-Dachgesetz (Originalwortlaut/pdf)
- Weiterer geplanter Umsetzungsprozess: im Laufe des Jahres 2023

Tipp und Empfehlung:
Eine sehr gute unabhängige, neutrale und niederschwellige Informations-Plattform zu allen regulativen Fragen rund um KRITIS ist „OpenKRITIS".

Rechtsentwicklung KRITIS: Zeitschiene Europäische Union und Deutschland



Inhaltliche und zeitliche Roadmap KRITIS-Vorschriften EU und Deutschland

3.3 DER AKTUELLE „KRITIS-GESETZESRAHMEN 2.0“ IN DEUTSCHLAND

Nach dem Erlass des IT-Sicherheitsgesetzes 2.0 im Mai 2021 gelten für die Betreiber Kritischer Infrastrukturen – mit dem neu hinzugekommenen Sektor „Siedlungsabfallentsorgung“ und der Gruppe der „Unternehmen von besonderem öffentlichen Interesse (UBI)“ – neue, strengere Sicherheitsauflagen gegen die wachsende Bedrohung aus dem Cyberspace.

Auch der Kreis und die Anzahl der betroffenen und regulierten KRITIS-Unternehmen hat sich durch neue Definitionen und Schwellenwerte erhöht.

Der Kreis der Kritischen Infrastrukturen wurde um den Sektor Siedlungsabfallentsorgung erweitert. Daneben müssen künftig auch weitere Unternehmen im besonderen öffentlichen Interesse „UBI“ (zum Beispiel Rüstungshersteller oder Unternehmen mit besonders großer volkswirtschaftlicher Bedeutung) bestimmte IT-Sicherheitsmaßnahmen umsetzen und werden in den vertrauensvollen Informationsaustausch mit dem BSI einbezogen.

Erstmalig werden optional auch Hersteller bzw. Vorlieferanten von kritischen Komponenten beim Einsatz in KRITIS in die rechtliche Pflicht genommen (Stichwort Vertrauenswürdigkeitsprüfung / Garantieerklärung).

Das BSI erhält verstärkte Kompetenzen bei der Detektion von Sicherheitslücken und der Abwehr von Cyber-Angriffen. So kann das BSI als zentrales Kompetenzzentrum der Informationssicherheit die sichere Digitalisierung gestalten und unter anderem Mindeststandards für die Bundesbehörden verbindlich festlegen und effektiver kontrollieren.

IT-Sicherheitsgesetz 2.0 eine Art „DSGVO Déjà-vu“
Mancher KRITIS-Entscheider fühlt sich beim neuen IT-Sicherheitsgesetz 2.0 an das finale Inkrafttreten der DSGVO im Jahre 2018 erinnert. Obgleich die DSGVO seit 2016 bekannt war und es sogar eine zweijährige Übergangsfrist gab,

warteten viele Unternehmen bis zum letzten Drücker mit der Implementierung – beziehungsweise scheiterten fast daran.

Je nachdem, in welche Kategorie ein Unternehmen fällt, besteht schon jetzt für einige Akteure akuter Handlungsbedarf. Bei der neuen Gruppe der „Unternehmen von besonderem öffentlichen Interesse" ist es noch gar nicht eindeutig, wer hier überhaupt betroffen ist. Welche Unternehmen „nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für Deutschland sind", muss erst noch durch eine Rechtsverordnung definiert werden.

Der aktuelle KRITIS-Gesetzesrahmen ist im BSI-Gesetz bzw. in der KRITISVERORDNUNG 2.0. kodifiziert.

Richtlinien auf EU-Ebene
Mit dem IT-Sicherheitsgesetz 2.0 ist unserer Einschätzung nach Deutschland wie bereits bei der NIS-1-Richtlinie der NIS-2-Richtlinie als Vorreiter „inhaltlich und zeitlich teilweise zuvorgekommen". Das strenge IT-Sicherheitsgesetz 2.0 dürfte bereits Teile der neuen europäischen NIS-2-Richtlinie umgesetzt haben. Die fehlenden Teile würden dann möglicherweise in einem IT-Sicherheitsgesetz 3.0 respektive im geplanten KRITIS-Dachgesetz in nationales Recht umgesetzt werden. Dasselbe Umsetzungsszenario gilt auch als wahrscheinlich für die „EU RCE Directive on the resilience of critical entities", die CER-Richtlinie.

3.3.1 DAS IT-SICHERHEITSGESETZ 2.0 IM INHALTLICHEN SCHNELLÜBERBLICK

NEUERUNGEN IM IT-SICHERHEITSGESETZ 2.0	
Neue Pflichten KRITIS-Betreiber: ▪ Angriffserkennung ▪ Kritische Komponenten ▪ Neue Meldepflichten ▪ Unmittelbare Registrierung	**Mehr betroffene Unternehmen:** ▪ KRITIS-Sektor Entsorgung ▪ Unternehmen im besonderen öffentlichen Interesse ▪ Niedrigere Schwellenwerte ▪ Mehr Anlagen
Mehr Befugnisse für das BSI: ▪ Zentrale Meldestelle ▪ Tiefere Untersuchungen ▪ Schutz der Bundesnetze ▪ Mehr Personal	**Sanktionen und Verbraucherschutz:** ▪ Höhere Sanktionen für Betreiber ▪ Mehr mögliche Verstöße ▪ Neue Gütesiegel

MEHR CYBERSECURITY-PFLICHTEN

Angriffserkennung:

- Systeme zur Angriffserkennung (ab Mai 2023)
- Verpflichtender Einsatz von Systemen und Prozessen
- SOC, SIEM, Auswertungen

Meldepflichten:

- Zusätzliche Meldepflichten ans BSI
- Informationen bei erheblichen Störungen zur Bewältigung
- Auch personenbezogene Daten

Komponenten:

- Kritische Komponenten in KRITIS-Anlagen
- Nur mit Genehmigung durch das Innenministerium (§ 9b BSIG)
- Bis dato nur im TK-Sektor üblich und definiert

Registrierung:

- Unmittelbare Registrierung beim BSI als KRITIS-Betreiber
- Benennung Kontaktstelle
- BSI darf Betreiber selbst registrieren

NEU REGULIERT: ENTSORGUNG UND UBI

Entsorgung:

- Neuer KRITIS-Sektor Siedlungsabfallentsorgung
- Dienstleistung Entsorgung von Siedlungsabfällen:
  - Sammlung
  - Beseitigung
  - Verwertung
- Anlagen und Schwellenwerte noch offen (per Rechtsverordnung zu definieren)

UBI:

- Unternehmen im besonderen öffentlichen Interesse
- Schützenswert aber nicht KRITIS:
  - UBI Rüstung und Waffen (nach AWV)
  - UBI Volkswirtschaftliche Bedeutung
  - UBI Gefahrstoffe
- Eigene UBI Cybersecurity-Pflichten

MEHR KRITIS-ANLAGEN UND BETREIBER

Sinkende Schwellenwerte:

- Tiefere Schwellenwerte = mehr Betroffenheit bei KRITIS-Anlagen

Mehr KRITIS-Anlagen:

- Neue KRITIS-Anlagen in Sektoren = mehr Betroffenheit bei Betreibern

Mehr KRITIS-Betreiber:

- Die Regierung schätzt deutlich mehr KRITIS-Betreiber durch IT-SiG 2.0
- ca. +280 zu den ca. 1.600 bestehenden
- Vor allem bei Energie und Finanzen
- UBI, KRITIS-Entsorgung noch nicht berücksichtigt

HÖHERE SANKTIONEN	
Mehr Tatbestände ▪ Mehr Tatbestände im IT-SiG 2.0 definiert ▪ Vorsätzliche oder fahrlässige Verstöße gegen Vorgaben = Ordnungswidrigkeit ▪ Fehlende KRITIS-Nachweise, fehlende Registrierung, fehlende Maßnahmen...	**Höhere Bußgelder:** ▪ Deutlich erhöhte Bußgelder für die o. g. Ordnungswidrigkeiten ▪ Zwischen 100 Tsd. und 2 Mio. EUR ▪ Bis zu 20 Mio. für jur. Personen

TO-DO LISTE FÜR ALTE UND NEUE KRITIS-BETREIBER	
Bestehende KRITIS-Betreiber: ▪ Angriffserkennung SIEM SOC **(ab Mai 2023)** ▪ Neue KRITIS-Anlagen prüfen ▪ Tiefere Schwellenwerte prüfen ▪ Neue Meldepflichten ans BSI	**Neue Betreiber & Entsorger:** ▪ KRITIS-Anlagen identifizieren ▪ Als KRITIS beim BSI registrieren ▪ Cybersecurity umsetzen ▪ Meldepflichten ans BSI
Alle KRITIS-Betreiber: ▪ Kritische Komponenten identifizieren ▪ Kritische Komponenten melden & freigeben ▪ Auf EU-Regulierung (NIS-2- / CER-Richtlinie) vorbereiten (ab 2023) ▪ Auf KRITIS-Dachgesetz vorbereiten, v. a. bzgl. physischen Schutzmaßnahmen (ab 2023)	**UBI:** ▪ Als UBI beim BSI registrieren ▪ Cybersecurity umsetzen ▪ Meldepflichten ans BSI

Diese und weitere detailliertere Informationen zum IT-Sicherheitsgesetz 2.0 finden Sie auf OpenKritis.

3.3.2 DAS BSI-GESETZ IM GESETZLICHEN SCHNELLÜBERBLICK

RECHTSNORMEN: KRITIS-PARAGRAPHEN, DIE MAN KENNEN SOLLTE

§ 8a BSIG: Sicherheit in der Informationstechnik Kritischer Infrastrukturen

- Betreiber Kritischer Infrastrukturen müssen die Einhaltung von IT-Sicherheit nach dem Stand der Technik regelmäßig gegenüber dem BSI nachweisen. Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI im Einvernehmen mit den Aufsichtsbehörden deren Beseitigung anordnen.

- Betreiber Kritischer Infrastrukturen sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden.

- **Neu ab Mai 2023: Systeme zur Angriffserkennung**
  Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.

Schutzziele der Informationssicherheit

§ 8b BSIG: **Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen**

- Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

- Betreiber Kritischer Infrastrukturen haben Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden.

§ 8c BSIG: **Besondere Anforderungen an Anbieter digitaler Dienste**

- Anbieter digitaler Dienste haben geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen.

§ 8f BSIG: **Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse**

- Unternehmen im besonderen öffentlichen Interesse sind verpflichtet, eine Selbsterklärung zur IT-Sicherheit beim Bundesamt vorzulegen.

- Welche Unternehmen „nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für Deutschland sind“, muss erst noch durch eine Rechtsverordnung definiert werden.

§ 9b BSIG: **Untersagung des Einsatzes kritischer Komponenten**
[= Sicherheitsanforderungen an Hersteller/Vorlieferanten von kritischen Komponenten]

- Der Betreiber einer Kritischen Infrastruktur hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Absatz 13 dem Bundesministerium des Innern, für Bau und Heimat vor ihrem Einsatz anzuzeigen.

- Das Bundesministerium des Innern, für Bau und Heimat kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt.

- Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob

    - der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird
    - der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder auf deren Einrichtungen hatten, oder
    - der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.

TIPP:
siehe dazu Kap. 1.1.3: Resilienzdreieck KRITIS – Geopolitische Resilienz – Investoren und Hersteller aus Drittstaaten

§ 9b Absatz (3):
Hersteller/Vorlieferanten in der Pflicht und in der Vertrauenswürdigkeitsprüfung

- Kritische Komponenten gemäß § 2 Absatz 13 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der Kritischen Infrastruktur abgeben hat.

- Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.

- Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass

    - er gegen die in der Garantieerklärung eingegangenen Verpflichtungen verstoßen hat,
    - in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,
    - er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,
    - Schwachstellen oder Manipulationen nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber der Kritischen Infrastruktur meldet,
    - die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können oder
    - die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.

- Kritische Komponenten gemäß § 2 Absatz 13 BSIG:

    - (13) Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte,
        - die in Kritischen Infrastrukturen eingesetzt werden,
        - bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können und
        - die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift
          a) als kritische Komponente bestimmt werden oder
          b) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.

3.3.3 AKTUELLER KRITIS-GESETZESRAHMEN AUS HERSTELLERSICHT

Künftig müssen also optional auch Hersteller oder Vorlieferanten von IT-Produkten (z. B. Software- oder Hardwareprodukten), die als „Kritische Komponenten“ eingestuft werden, für KRITIS-Betreiber eine Vertrauenswürdigkeits- bzw. Garantieerklärung abgeben, in der sie darlegen, ob und wie sie versuchen das jeweilige IT-Produkt vor Terrorismus, Spionage oder Sabotage zu bewahren.

Lieferkette und Hersteller rücken in den Fokus
Diese Vertrauenswürdigkeits-Klausel ist aus unserer Sicht, auch vor dem Hintergrund der leidvollen Erfahrungen bzgl. kritischer (Liefer-) Abhängigkeiten, nicht nur in KRITIS, ein wichtiger und logischer Schritt hin zu mehr Autonomie und ökonomischer Souveränität. Es muss aber auch ein nachvollziehbarer Prüfmechanismus für die Prüfung der Vertrauenswürdigkeit der Hersteller und der Produkte etabliert werden. Dieser Prüfprozess darf aber nicht, wie bei der DSGVO gesehen (*), durch inflationäre und „Pseudo-Vertrauenswürdigkeitszertifikate oder Scheinzertifikate für KRITIS“ unterlaufen werden.

**DSGVO Zertifizierungen: Es gibt bis heute noch keinen freigegebenen Zertifizierungsprozess durch das European Data Protection Board (EDPB) gemäß Artikel 42 DSGVO für datenschutzspezifische Zertifizierungsverfahren sowie für Datenschutzsiegel und -prüfzeichen.*

Die Regelungen des neuen BSIG, insbesondere die Regelung des § 9b BSIG, werden sicherlich zur Reduzierung der Drittlandgefahr und damit zur Erhöhung der Gesamtsicherheit von KRITIS beitragen nach der oben beschriebenen Erkenntnis *„Die KRITIS-Sicherheitskette ist nur so stark wie ihr schwächstes Glied“*.

Die gesetzliche Zielrichtung auch positiv aus geopolitischer Sicht
In Anbetracht der Erkenntnisse in der Pandemie, Lieferabhängigkeiten und Lieferschwierigkeiten, und v.a. nach den „Kriegserkenntnissen“, Abhängigkeiten in Schlüsselenergien und Schlüsseltechnologien, sollten die verschärften rechtlichen Möglichkeiten und Optionen dazu beitragen, die Souveränität Europas und deren Kritischer Infrastrukturen wiederzuerlangen (siehe Entwicklung im Fall Huawei 5G).

Weitere Empfehlungen, Richtlinien und gesetzliche Vorgaben
Informieren Sie sich zudem auch bei den jeweils staatlich anerkannten Stellen in Ihrem Land über die neuesten gesetzlichen Vorgaben, Richtlinien und Empfehlungen für KRITIS.

3.4 AUSBLICK: DAS GEPLANTE KRITIS-DACHGESETZ IN DEUTSCHLAND

Die KRITIS-Regulierung in der EU und in Deutschland wird sich in den nächsten Jahren deutlich weiterentwickeln bzgl. mehr Anforderungen, mehr Betroffenheit (niedrigere Schwellenwerte) und generell mehr Regulierung mit dem Ziel einer ganzheitlichen Resilienz von Kritischen Infrastrukturen.

Spätestens seit den Sabotage-Angriffen auf die Nord-Stream-Pipelines und auf die Steuerungskabel der Deutschen Bahn im Herbst 2022 erlangte der KRITIS-Schutz eine gesteigerte Aufmerksamkeit: Bei den KRITIS-Betreibern, in der Bevölkerung, aber auch in der Politik. In der Folge legte das Deutsche Bundeskabinett am 7. Dezember 2022 „Eckpunkte für das KRITIS-Dachgesetz“ vor.

Die wichtigsten Eckpunkte für ein KRITIS-Dachgesetz:

- Physische Sicherheit soll erstmalig gesetzlich reguliert werden
  - Verpflichtende Umsetzung einheitlicher technischer Schutz-Mindeststandards
  - u. a. mit Detektionssystemen und Systemen zur Überwachung der Umgebung, z. B. durch Videoüberwachung
- Betroffene KRITIS definiert und erweitert
  - Öffentliche UND privatwirtschaftliche KRITIS-Betreiber
  - Ein neuer Sektor (Raumfahrt/Weltraum)
  - Klare, einheitliche „Wer gehört zu KRITIS“-Definitionen nach qualitativen und quantitativen Kriterien
- Hersteller-Vertrauenswürdigkeitsprüfung
  - Bei kritischen IT-Komponenten: BSI-Gesetz (§ 9b Abs. 3 BSIG) fordert Garantieerklärungen über Vertrauenswürdigkeit des Herstellers
  - Bei anderen kritischen NICHT-IT-Komponenten: Für einen umfassenden Schutz werden Regelungen geprüft, um KRITIS insgesamt vor Einflüssen und Abhängigkeiten von bedenklichen Herstellern aus dem Ausland zu schützen

- Ganzheitliche Resilienz als Ziel
    - Physische Sicherheit und Cybersicherheit gemeinsam und übergreifend „denken“, monitoren und prüfen
    - Steigerung der „geopolitischen“ Resilienz durch obigen optionalen Punkt „Prüfung bedenklicher Hersteller aus dem Ausland“
    - Kohärenz beim Cyberschutz und beim physischen Schutz auch durch enge Zusammenarbeit zweier Aufsichtsbehörden:
        - IT- und Cyberschutz: Bundesamt für Sicherheit in der Informationstechnik (BSI)
        - Physischer Schutz (neu): Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
- Einbettung in EU Rechtsrahmen
    - Umsetzung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience / CER-Richtlinie)
    - Umsetzung der EU NIS-2-Richtlinie (Netz-und Informationssicherheit)
    - Weitere Info zu NIS-2- und CER-Richtlinie
- Gesetz und gesetzlicher Umsetzungsprozess
    - 07.12.2022: Bundesregierung verabschiedet die Eckpunkte des KRITIS-Dachgesetzes
    - Webseite BMI: Eckpunkte für das KRITIS-Dachgesetz (Originalwortlaut/pdf)
    - Weiterer geplanter Umsetzungsprozess: im Laufe des Jahres 2023

Unsere Einschätzung: „Physische Resilienz“ – Der noch fehlende gesetzliche Baustein für ganzheitliche KRITIS-Resilienz

Unserer Einschätzung nach steckt hinter dem geplanten KRITIS-Dachgesetz die politische Erkenntnis, dass man für den Schutz und die Resilienz von KRITIS keinen „fragmentiert-regulierten“, nicht aufeinander abgestimmten, sondern einen ganzheitlichen und hybriden Ansatz verfolgen muss. Nur eine Art „ganzheitliches Schutzdach“ für KRITIS wäre zielführend.

Es gibt ja aktuell in Gestalt des IT-Sicherheitsgesetzes bzw. BSI-Gesetzes bereits einzelregulatorische Vorschriften für KRITIS-Betreiber bezüglich der Cybersicherheit, aber eben nur für Cybersicherheit.

Es gibt zwar aktuell auch fragmentierte, sektorspezifische, branchenspezifische Regelungen für physische Sicherheit, z. B. im Luftsicherheits-Gesetz mit z. B. den Artikeln 8 und 9, aber generelle, sektor- und gefahrenübergreifende bundesweite „Dach-Vorschriften“ bzw. „Dach-Sicherheitsstandards“ für die physische Sicherheit und Absicherung von KRITIS gibt es bis dato noch nicht.

Zudem stellt die Definition in der Kritisverordnung „Wer gehört zu KRITIS“ („Größenklassen“, Schwellenwerte) nur auf den Aspekt der Informations- und Cybersicherheit ab.

Die geplanten Vorschriften und dieser Schritt hin zu mehr physischer Sicherheit mittels eines KRITIS-Dachgesetzes sind aus unserer Sicht in geopolitischer und sicherheitspolitischer Sicht zu begrüßen, auch im Hinblick auf die versorgungstechnische Souveränität, Unabhängigkeit und Continuity der KRITIS.

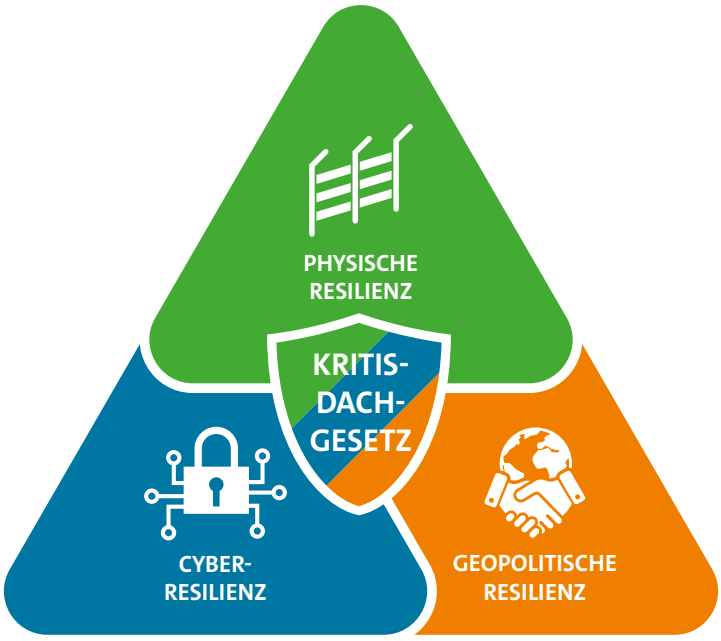
Daneben wäre ein solches Dachgesetz auch schon alleine aus einfachen Gründen wie gesetzlich klaren, verbindlichen Definitionen von KRITIS-Einrichtungen, von Verantwortlichkeiten und Zuständigkeiten und sektorübergreifenden und bundesweit einheitlichen Schutzstandards wünschenswert.

Die Herausforderung bei der Umsetzung des KRITIS-Dachgesetzes wird aus unserer Sicht sein, jenseits von „leichter durchsetzbaren Fällen“ wie im Falle von KRITIS-Einrichtungen in Staatseigentum (z. B. Deutsche Bahn), gesetzlich angeordnete Investitionen in den physischen Schutz von privatwirtschaftlichen KRITIS-Betreibern (ist die Mehrzahl) zu verargumentieren im Hinblick auf die Kostenbelastung und Finanzierung dieser Maßnahmen. Das Problem der Finanzierung zeigte sich auch bei der Verabschiedung der Eckpunkte, welche den Zusatz „unter generellem Finanzierungsvorbehalt“ enthielten.

Videotechnik Made in Germany versus „bedenkliche Hersteller“
Wir stellen in letzter Zeit fest, dass „Made in Europe, Made in Germany“ wieder verstärkt als Gütesiegel für Qualität, Sicherheit und Vertrauen wahrgenommen, wertgeschätzt und nachgefragt wird.

Wenn dann noch neben der „freiwilligen“ Made in Europe / Made in Germany-Tendenz zudem eine im BSI-Gesetz oder in einem kommenden KRITIS-Dachgesetz kodifizierte gesetzliche Regelung für mehr physische Sicherheit, für mehr vertrauenswürdige Hersteller und vertrauenswürdige Produkte und Komponenten hinzukommt, kann das nur positiv im Sinne der KRITIS-Sicherheit sein.

Ganzheitliche KRITIS-Resilienz



Das KRITIS Resilienzdreieck: mit KRITIS-Dachgesetz und Dallmeier Videolösungen zur ganzheitlichen KRITIS-Resilienz.

4 WELCHE „STOLPERSTEINE“ SIND BEI EINEM KRITIS-VIDEOPROJEKT ZU ERWARTEN?

Manchmal handelt es sich bei Projekten im Bereich Kritischer Infrastrukturen um ein Erstprojekt, bei dem die Verantwortlichen nur auf wenige oder gar keine Erfahrungswerte zurückgreifen können. So stehen die Verantwortlichen vor vielen politischen, technischen, infrastrukturellen, datenschutzrechtlichen, cybersicherheits-relevanten und schlussendlich entscheidungsrelevanten Prozessen und Fragestellungen, die es zu lösen gilt.

Die Checkliste verringert die Fehlerquote
Für KRITIS-Projektverantwortliche ist es immer hilfreich, den Herausforderungen und Stolpersteinen positiv und proaktiv zu begegnen. Es empfiehlt sich deshalb, die wesentlichen Erfolgsfaktoren, aber auch die möglichen Stolpersteine und Hindernisse zu kennen und sich entsprechend darauf vorzubereiten. Aus mehr als 38 Jahren Projekterfahrung mit Videoüberwachung für Kritische Infrastrukturen weiß der Autor dieses Dokuments, welche Schwierigkeiten zu erwarten sind, und wie man am besten darauf reagiert. Am Ende des Dokuments haben wir auch noch mal die wichtigsten Fragen als Checkliste zusammengestellt.

4.1 KOSTEN: BEGRÜNDEN UND ARGUMENTIEREN

Technische Lösungen kosten Geld, das ist keine Neuigkeit. Und diese Kosten gilt es zu begründen und zu legitimieren, und zwar oft gegenüber mehreren unterschiedlichen Gruppen, die an der Entscheidung beteiligt sind – und die vielleicht jeweils eine ganz eigene und vor allem unterschiedliche „Agenda“ verfolgen. Insbesondere im öffentlich-rechtlichen KRITIS-Rahmen ist diese Herausforderung möglicherweise größer als einem lieb ist, denn politische und unternehmerische Gremien und Finanzausschüsse müssen der Investition im Zweifelsfall mehrheitlich zustimmen und diese genehmigen.

Objektive Sicherheitslage und subjektives Sicherheitsgefühl
Somit sind die Kosten eines Projektes zwar häufig der letzte Schritt, der im Entscheidungsprozess relevant wird. Aber bereits während der Planung einer Videobeobachtung (jemand schaut live auf das Bild) oder Videoüberwachung (jemand sieht sich nur bei einem Vorfall die Aufzeichnungen an) für KRITIS werden diverse Budgetierungen und Grobkonzepte abgestimmt. Diese sollten stets technisch und planerisch einwandfrei und begründbar sein. Denken Sie an die unterschiedlichen Interessenlagen und zeigen Sie das Verbesserungs- und Lösungspotenzial für die objektive Sicherheitslage und das subjektive Sicherheitsbedürfnis der Betreiber, Mitarbeiter, Partner, Kunden oder anderer betroffener Stakeholder auf.

Ihr wichtigstes Argument: Was ist der Wert von Sicherheit?
Für die Verbesserung der subjektiven und objektiven Sicherheit der Kritischen Infrastrukturen kann man den „Return on Investment“ gar nicht hoch genug ansetzen. Sicherheit gehört zu den Grundbedürfnissen des Menschen.

Keine Erfindung von KRITIS-Betreibern, Politik oder Sicherheitswirtschaft: Sicherheit gehört zu den originären Grundbedürfnissen des Menschen, zu sehen an der Maslowschen Bedürfnispyramide.

PRAXISTIPP — ARGUMENTATION „PRO VIDEO“

DIE RICHTIGE ARGUMENTATIONSKETTE & ANSCHAULICHE BEISPIELE

Hilfreich bei der Argumentation in der eigenen Organisation ist die richtige „Struktur“. Es geht im Normalfall bei moderner Videotechnik immer um den Dreiklang aus Prävention, Reaktion in möglichen „Live- bzw. Beobachtungssituationen“ und der Aufklärung. Eine Recherche im Internet führt heute zu zahlreichen seriösen Fundstellen, aus denen die teilweise spektakulären Erfolge moderner Videoüberwachung und Videobeobachtung hervorgehen. Diese zu sammeln und zusammenzustellen hilft bei der Argumentation, z. B. gegenüber Betriebsrat oder Datenschutz.

4.2 INFRASTRUKTUR: PLÄNE UND INFORMATIONEN SAMMELN

Die Infrastruktur – bestehend aus Masten, Kupferverkabelung, Glasfaser, Richtfunkstrecke, Hoch- und Tiefbauarbeiten usw. – stellt in der Regel eine komplexe Aufgabenstellung im Gesamtprojekt dar. In diesem Kontext ergeben sich u. a. folgende Fragen bei der Planung:

- Gibt es Pläne des zu überwachenden Bereiches / der Fläche?
- Gibt es Leitungs- und Trassenpläne von vorhandenen Infrastrukturen, wie z. B. Gas, Fernwärme,Telekommunikation?
- Sind Infrastrukturen wie Verkabelung von Strom und Netzwerk bekannt/vorhanden?
- Wie erfolgt die Netzwerkanbindung für die Kameras?
- Gibt es eventuell vorhandene Netzwerk-ressourcen, die man nutzen kann wie z. B. von Verkehrsbetrieben, anderen KRITIS-Anlagen oder verbundenen Unternehmen? Diese verfügen häufig bereits über entsprechende Leitungen, z. B. an modernen Lichtmasten
- Wie kommt Strom zur geplanten Kameraposition?
- Können vorhandene Masten bzw. Lichtmasten genutzt werden?
- Müssen neue Masten errichtet werden?
- Welche Einwilligungen müssen eingeholt werden, wenn man Kameras an Gebäuden oder Wänden platzieren möchte?

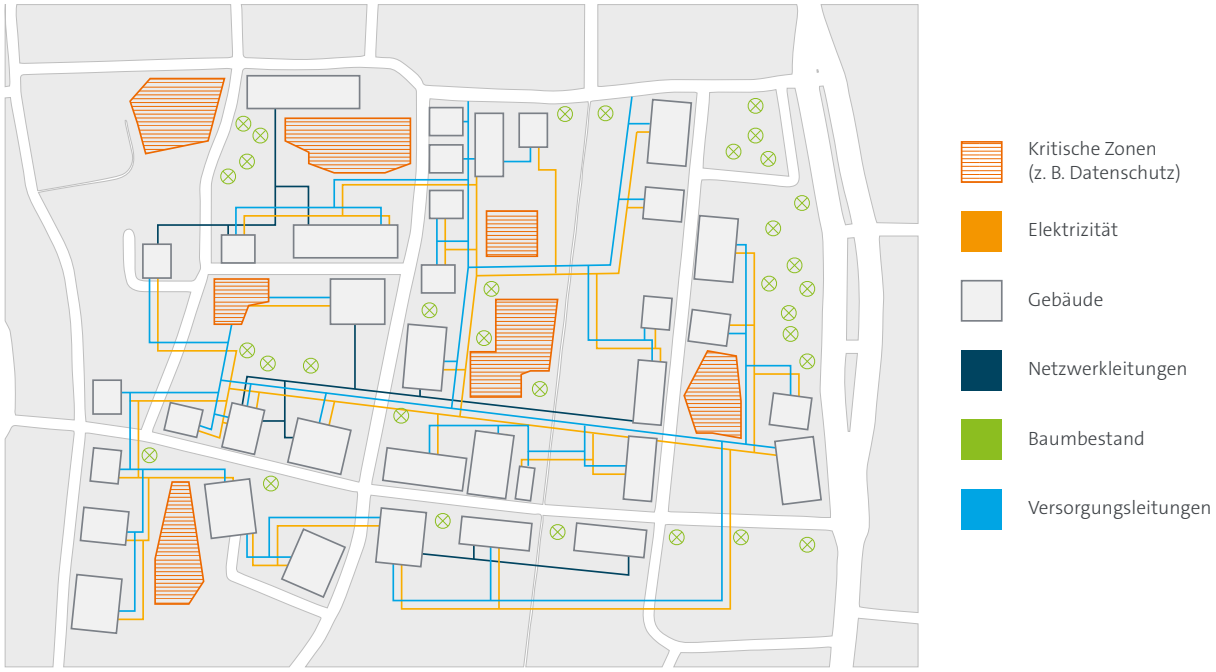
Gute Vorbereitung ist die Basis für gute Planung.

PRAXISTIPP INFRASTRUKTURSYNERGIEN

WELCHE INFRASTRUKTUR IST BEREITS VORHANDEN?

Wie so häufig: Miteinander reden hilft. Oft gibt es nützliche Synergieeffekte, z. B. indem man natürlich die eigene IT-Abteilung, aber evtl. auch „angrenzende“ Infrastruktur- oder IT-Stakeholder aktiv einbezieht oder man eventuell bereits vorhandene Netzwerkinfrastrukturen nutzen kann. Oder es lassen sich Infrastrukturelemente anderer „benachbarter oder gesellschaftsrechtlich-verbundener“ KRITIS-Betriebe verwenden.

Ein frühzeitiges Einbeziehen und eine „Fragen kostet nichts“-Mentalität sind unter Umständen bares Geld wert.



Bezieht man bestehende KRITIS-Infrastruktur frühzeitig in die Planungen mit ein, lassen sich u. U. viel Geld und Zeit einsparen.

4.3 UMWELTSCHUTZ UND LANDSCHAFTSBILD: SENSIBILITÄTEN RESPEKTIEREN UND AUF DIE PASSENDE TECHNIK ACHTEN

Masten, sonstige Befestigungen sowie aufwendige und vor allem neue Infrastruktur verändern das Landschafts- bzw. KRITIS-Bild. Es empfiehlt sich, die entsprechenden Institutionen und verantwortlichen Einzelpersonen, wie etwa im Bereich Denkmalschutz und KRITIS-Planung, frühzeitig einzubinden und Meinungen aufrichtig und konstruktiv aufzunehmen.

Wichtig ist auch die Technik selbst: Ein Konzept, das mit möglichst wenigen Kameras und Montageorten möglichst große Flächen abdeckt, hat den geringsten Einfluss auf das KRITIS-Erscheinungsbild. Zudem kommt es mit minimalem Infrastrukturaufwand aus, was wiederum als Nebeneffekt eine hohe Wirtschaftlichkeit sicherstellt. Es gibt hier große Unterschiede bei den Technologien, die weiter hinten noch erläutert werden.

Die Wahl der Technologie wirkt sich unter Umständen gravierend auf das KRITIS-Erscheinungsbild aus.

4.4 Mitglieder im Team und Projektbeteiligte

Je mehr Personen und Institutionen an einem Projekt beteiligt sind, desto aufwendiger, langwieriger und komplexer (insbesondere in der Kommunikation) wird es. Hier müssen die Entscheider zahlreiche Schnittstellen abstimmen und beauftragen, die in der Praxis häufig Probleme aufweisen. Wir empfehlen, sich zu Beginn einen Überblick über alle potenziellen Beteiligten zu verschaffen. Zudem hilft es, das Gesamtprojekt in mehrere einzelne Projektschritte aufzuteilen, die die beteiligten Personen für sich jeweils schnell und effizient abschließen können.

Je nach Organisations- und Gesellschaftsform der KRITIS (öffentlich-rechtlich / privatrechtlich), unterscheiden sich die Teammitglieder und Projektbeteiligten doch erheblich. Nachfolgende Mindmap stellt demnach nur eine Sammlung möglicher Akteure und Stakeholder dar.

Ich
Projektverantwortlicher

TECHNIK
- Verantwortlicher Sicherheit (Chief Security Officer (CSO))
- Verantwortlicher Corporate Security / Physische Sicherheit / Objektschutz
- Planer / Planungsbüro
- Facherrichter
- Gesellschaftsrechtlich-verbundene Betriebe (wegen optional gemeinsamer Nutzung Infrastruktur)
- Videoaffine Fachabteilung (Prozessautomatisierung)
- Sonstige Technische Projektbeteiligte

IT
- IT-Abteilung
- CIO
- Chief Information Security Officer (CISO)
- IT-Systemhaus (extern)

FINANZEN
- Investor / Geldgeber / Gesamtentscheider
- Budgetverantwortlicher
- Einkauf / Procurement

ÖFFENTLICHE BEHÖRDEN
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Bauaufsichtsbehörde
- Ordnungsbehörde

DATENSCHUTZ
- Datenschutzaufsicht
- Datenschutzbeauftragter / Betriebsrat
- Datenschutzinitiativen

COMPLIANCE UND RECHT
- Compliance- und Legal-Verantwortlicher
- Risiko- und Krisenmanager
- Optional ab 2023 nach Lieferketten-sorgfaltspflichtengesetz (LkSG):
  - Verantwortlicher für Ethik, Menschenrechte und Nachhaltigkeit in der Supply Chain

PRESSE
- International
- National
- Lokal

POLITIK
- International
- National
- Lokal

PRAXISTIPP

ALLE BETEILIGTEN FRÜHZEITIG UND PROAKTIV EINBEZIEHEN

PROAKTIVES HANDELN UND OFFENE KOMMUNIKATION ANSTATT WIDERSTÄNDE ABWARTEN

Gehen Sie aktiv und frühzeitig auf alle Beteiligten zu. Holen Sie alle Interessenvertreter und Anspruchsgruppen (Stakeholder) frühzeitig und auf Augenhöhe „ins Boot“. Dazu gehören Geschäftsleitung genauso wie Betriebsrat und Datenschützer.

Durch aktives „TUN“: Ansprechen, Informieren, Zeigen und Vorführen (Technik, 3D-Planungen, Zahlen, etc.) und Argumente Pro & Contra Austauschen (technisch, kaufmännisch, rechtlich) – Reden hilft immer! Nehmen Sie die Argumente oder berechtigte und unberechtigte Einwände ernst. Zeigen Sie den technischen und kaufmännischen Nutzen (z. B. anhand eine digitalen Zwillings bzw. einer TCO-Betrachtung) der jeweiligen Lösung auf. Holen Sie evtl. zusätzlichen Rat von Experten ein.

5 KEINE ANGST VOR DATENSCHUTZ – HÖCHSTE PRIORITÄT CYBERSECURITY

Datenschutz und Datensicherheit bzw. Cybersecurity mögen manchem Entscheider im Zuge einer geplanten Videoüberwachungslösung besonders große Magenschmerzen bereiten – schließlich kommt dem Schutz der Privatsphäre und der Mitarbeiter- und Bürgerrechte insbesondere in „sensiblen, kritischen Bereichen“ höchste Bedeutung zu. Zudem gilt die wechselseitige Abhängigkeit: Ohne Datensicherheit auch kein Datenschutz. Die Magenschmerzen müssen aber nicht sein, wenn man einige Grundregeln beachtet.

5.1 ANFANGS- ODER ANFÄNGERFEHLER: DER DATENSCHUTZ ALS „FEIND“

Der oder die betriebliche Datenschutzbeauftragte oder die externe Datenschutzaufsicht – sowohl kommunal als auch auf Landes- oder Bundesebene – erfüllt in unserer demokratischen Gesellschaft eine wichtige Funktion. Bei KRITIS-Überwachungsprojekten erlebt man immer wieder, dass die Datenschützer als „Gegner“ wahrgenommen und aus Angst vor etwaigem Widerstand (zu) lange aus dem Entscheidungsprozess herausgehalten werden. Je früher eine Einbindung in das Projekt und die Planung erfolgt, desto höher ist fast immer die Akzeptanz der geplanten Maßnahmen und umso wahrscheinlicher ist ein konflikt- und verzögerungsfreier Projektverlauf.

PRAXISTIPP — **DATENSCHUTZBEAUFTRAGTE UND DATENSCHUTZAUFSICHT**

AUF AUGENHÖHE DURCH „PARTIZIPATION UND INTEGRATION“

Involvieren Sie interne sowie externe Datenschutzanspruchsgruppen bereits, sobald ein erstes Konzept entworfen ist. Nehmen Sie deren Interessen ernst, lassen Sie sich beraten und klären Sie Ihrerseits auf.

PRAXISTIPP 2

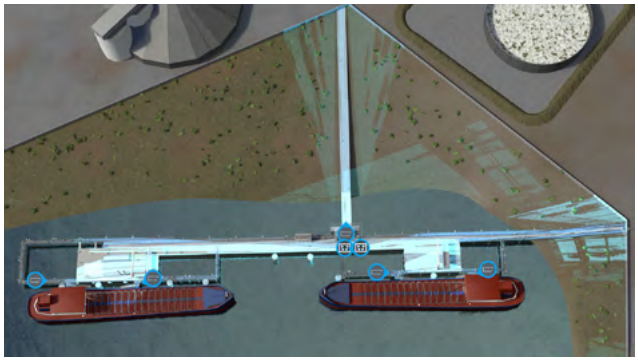
DATENSCHUTZBEDENKEN AUSRÄUMEN: 3D-PLANUNG IST ERFOLGSSCHLÜSSEL

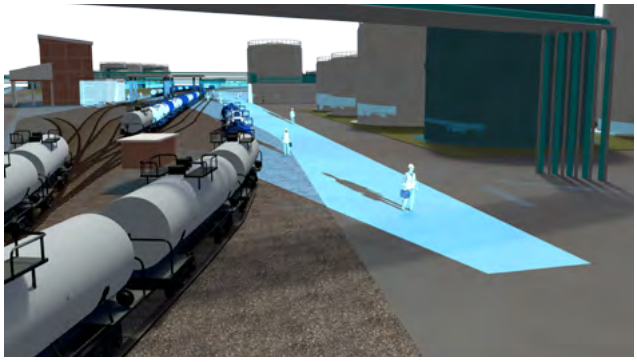
DEN DATENSCHUTZSTAKEHOLDERN ZEIGEN, WAS GEPLANT IST („SEE MORE BEFORE“)

Häufig steht hinter einer kategorischen Ablehnung schlicht und ergreifend Unsicherheit oder mangelndes Wissen. VOR Projektstart hilft oftmals die Präsentation der 3D-Planung des zukünftigen Systems vor allen DATENSCHUTZSTAKEHOLDERN (wie z. B. Datenschutzbeauftragte, Betriebsrat, Mitarbeiter, Datenschutz-Aufsichtsbehörde), um berechtigte und unberechtigte Datenschutzbedenken erfolgreich auszuräumen.

DER ERFOLGSSCHLÜSSEL: EINE 3D-PLANUNG

Zu Beginn eines Projekts erstellt ein 3D-Planungsteam einen „digitalen Zwilling“ Ihrer Umgebung. Dabei werden alle Planungen und Veränderungen durchgeführt, bis das Lösungskonzept technisch und datenschutzrechtlich „wasserdicht“ ist. Dies gewährleistet eine optimale, kosteneffiziente Planung und Umsetzung und garantiert die Zielerreichung unter Berücksichtigung von Budget, Zeit, Datenschutz und Datensicherheit.





KRITIS-Sektor „Transport und Verkehr – Binnenschifffahrt und Schienenverkehr“
Das 3D-Planungsteam erstellt eine detailgetreue Simulation der Lösungsumgebung, hier Beispiel Hafenumgebung. In diesem „digitalem Zwilling“ lassen sich Standorte und Sichtfelder der Überwachungskameras exakt simulieren. Die Anzahl der benötigten Systeme wird so minimiert.

VOR PROJEKTSTART DIE DATENSCHUTZSTAKEHOLDER ÜBERZEUGEN

- Rechtzeitige Einbindung aller Stakeholder VOR Projektstart
- Reden wir über dasselbe?
- Abklärung mit Datenschützer: Was sieht welche Kamera? Mit welcher Bildqualität? Welche Bildwinkel? Welche Szene? Sind Mitarbeitern betroffen? Entstehen personenbezogene Daten?
- Visualisierung der Datenschutz-Funktionen im digitalen Zwilling (z. B. Private Zonen, Verpixelung)

Mehr zum Thema und zu den Vorteilen einer 3D-Planung finden Sie in Kap. 7.6.

5.2 VIDEOÜBERWACHUNG NACH DSGVO UND DAS OBLIGATORISCHE HINWEISSCHILD

Videoüberwachung nach DSGVO

Mit einer Videokamera dürfen personenbezogene Daten nur verarbeitet werden, wenn eine gesetzliche Grundlage dies erlaubt. Das Problem bei der Einführung der DSGVO im Jahre 2018 war und ist heute noch die Tatsache, dass die DSGVO keine explizite und spezifische Regelung zur Videoüberwachung durch nicht-öffentliche Stellen (Privatpersonen und Unternehmen) beinhaltet.

Welche Regelung der DSGVO ist für die Videoüberwachung nun einschlägig?

Für die Prüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch nicht öffentliche Stellen ist zunächst auf die „Generalklausel" in Art. 6 DSGVO abzustellen. D.h. man muss mangels eines eigenen „Videoüberwachungsparagraphen" in der DSGVO auf diese Grundsatzklausel zur Rechtmäßigkeit einer Datenverarbeitung zurückgreifen. Der Großteil der Videoüberwachungsprojekte wird mit der „Rechtmäßigkeits-bedingung Interessenabwägung" des Buchstaben (f) des Art. 6 Abs. 1 S. 1 lit. f DSGVO legitimiert und ist im nachfolgenden Hinweisschild in der Zeile „Zwecke und Rechtsgrundlage der Datenverarbeitung" einzutragen. Grundsätzlich kann sich die Rechtmäßigkeit einer Videoüberwachung aber auch aus allen anderen Rechtmäßigkeitstatbeständen des Art. 6 Absatz 1 Satz 1 DSGVO ergeben.

Der wichtigste Artikel der DSGVO für Videoüberwachung im Wortlaut:
Art. 6 Abs. 1 S. 1 lit. f DSGVO: Rechtmäßigkeit der Verarbeitung

> *„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:*
>
> *f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt."*

Videoüberwachung und Datenschutz nach dieser Generalklausel ist immer folgende Abwägung

- Berechtigtes (Sicherheits-) Interesse des Verantwortlichen oder eines Dritten

  versus

- Interessen, Persönlichkeitsrechte und Grundrecht auf „informationelle Selbstbestimmung" der betroffenen Person

- Allgemeine Abwägung: Zweckmäßigkeit, Erforderlichkeit und Interessen

Weitere Fragen zur DSGVO und der Begründung der Videoüberwachung finden sich auch in der DSK Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen und im DSK Kurzpapier Nr. 15 (jeweils mit Fokus auf nicht-öffentliche Stellen).

Für öffentliche Stellen gelten Landesdatenschutzgesetze, beispielhaft nachfolgende Links für Baden-Württemberg / Bayern.

Das obligatorische Hinweisschild

In der DSGVO wird die Hinweispflicht bei Videoüberwachung auch nicht videospezifisch geregelt, sondern richtet sich nach der generellen Klausel „Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person“ des Artikel 13 DSGVO.

Nachfolgend ein Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung:

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung

Weitere Informationen erhalten Sie:
- an unserer Rezeption im Erdgeschoss
- im Internet unter www.muster.de/video

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Muster GmbH
Geschäftsführer Herr Mustermann
Musterstraße 1, 00000 Musterstadt
E-Mail: info@muster.de
Tel.: 0123/456789

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Herr Beispiel, E-Mail: dsb@muster.de, Tel.: 0123/456789-01

Zwecke und Rechtsgrundlage der Datenverarbeitung:

Zwecke: Prävention und Aufklärung von Einbruch, Diebstahl, Spionage, Sabotage
Rechtsgrundlage: Art. 6 Abs. 1 S.1 lit. f DSGVO

berechtigte Interessen, die verfolgt werden:

Schutz des Eigentums des Verantwortlichen.

Speicherdauer oder Kriterien für die Festlegung der Dauer:

Die gespeicherten Aufzeichnungen werden regelmäßig überschrieben, eine Löschung findet spätestens nach 7 Tagen statt, insofern zur Beweissicherung keine weitere Speicherung nötig wird.

Weitere Info: Transparenzanforderungen und Hinweisbeschilderung bei einer Videoüberwachung nach der DSGVO

5.3 JE BESSER DIE BILDQUALITÄT, DESTO BESSER DIE ZWECKERFÜLLUNG

In der Videotechnik gibt es augenscheinlich viele Lösungen, die erfolgversprechend sind. Allerdings sagt die Rechtsprechung auch, dass Videoüberwachung und Videobeobachtung nur zulässig sind, wenn sie ihren Zweck erfüllen. Tun sie das nicht, z. B. weil die Bildqualität nicht in allen Bereichen des überwachten Raums ausreicht, um z. B. Personen identifizieren zu können (= Zweck der Überwachung), gibt es unter Umständen Einspruch von Seiten des Datenschutzes.

Das hört sich widersprüchlich an? Ist es aber nicht…
Wenn Sie sich kurz noch mal das Hinweisschild für Videoüberwachung in Kap. 5.2 anschauen, da gibt es eine Zeile wie folgt: „Zwecke und Rechtsgrundlage der Datenverarbeitung".

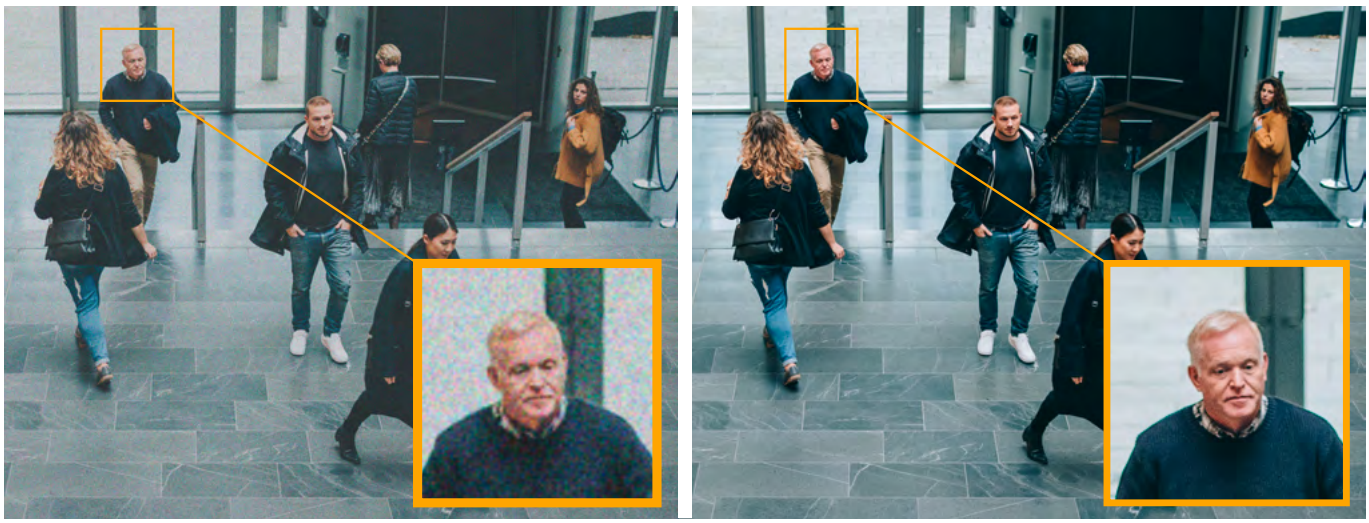
Wenn Sie als Zweck z. B. Diebstahlprävention und Diebstahlaufklärung angeben und nach einem Jahr der Datenschützer feststellt, dass kein Diebstahl aufgeklärt werden konnte aufgrund der schlechten Bildqualität, dann hat die Videoüberwachung ihren Zweck nicht erfüllt und ist aus Datenschutzsicht nicht mehr erlaubt.

Noch verständlicher wird der Sachverhalt, wenn man sich die entsprechende Grundsatz-Regelung jeglicher Datenverarbeitung in der DSGVO kurz anschaut, den Artikel 5 (1) b DSGVO:

> *„Personenbezogene Daten müssen…*
> *…für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden… („Zweckbindung")"*

Fazit (was es herzuleiten galt):

- JE BESSER DIE BILDQUALITÄT, DESTO BESSER DIE ZWECKERFÜLLUNG
- …UND FOLGLICH DESTO BESSER DER DATENSCHUTZ NACH DSGVO



Ohne ausreichende und flächendeckend konstante Bildqualität keine Zweckerfüllung nach DSGVO.

PRAXISTIPP

ZWECKBINDUNG DER (VIDEO-) DATENVERARBEITUNG

ZWECKBINDUNG UND ZWECKERFÜLLUNG DES VIDEOSICHERHEITSSYSTEMS FESTLEGEN UND DOKUMENTIEREN

Die initiale Zweckbestimmung (z. B. Objektüberwachung) wird nach DIN 62676-4 in den Kapiteln über „Betriebsanforderungen“ (Kap. 5ff) festgelegt. Weiterhin muss die Zweckbindung und Zweckerfüllung des Videosicherheitssystems nach der DSGVO dokumentiert und im Zeitablauf überprüft werden. Personenbezogene Daten dürfen nur für den definierten Zweck in der Videoüberwachungsanlage verarbeitet werden. Wird der Zweck nicht erfüllt oder ändert sich der Zweck, entfällt der Grund für die Verarbeitung der Daten. Die Anlage muss entsprechend zurück- oder umgebaut werden.

5.4 AUFKLÄREN HILFT GEGEN WIDERSTÄNDE

Wir stellten und stellen in sehr vielen Projekten zudem ein hohes Maß an Aufklärungs- und Schulungsbedarf fest, was die technischen Realitäten moderner Überwachungstechnik betrifft.

Hier ist es oftmals hilfreich, die Beteiligten, z. B. unter Einbeziehung eines oder mehrerer Hersteller, schon frühzeitig zu informieren und so Widerstände, die aus mangelnder Informiertheit resultieren, abzubauen.

Die geplante Videoanlage vorzuführen, ist eine bewährte, aber viel zu selten genutzte Methode, um Vorurteile und Widerstände abzubauen und sachlich aufzuklären.

PRAXISTIPP

„TOUCH A VIDEO SYSTEM“

VORFÜHREN, WAS GEPLANT IST

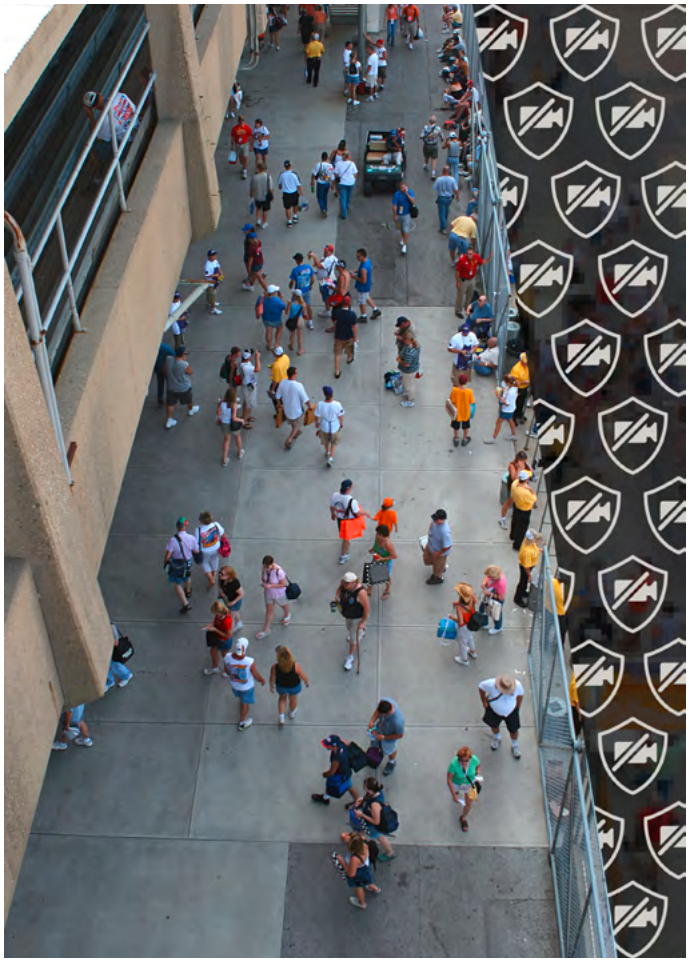
Häufig steht hinter einer kategorischen Ablehnung schlicht und ergreifend Unsicherheit und mangelndes Wissen. Vielleicht hilft die Live-Vorführung einer Test-Installation des zukünftigen Systems – z. B. im „internen KRITIS-Entscheider-Zirkel“ oder bei einer betriebsinternen oder politischen Informationsveranstaltung? Alternativ oder begleitend helfen oftmals auch branchengleiche oder artähnliche (Video-) Case Studies von erfolgreich durchgeführten Projekten.

5.5 PRIVACY & SECURITY BY DESIGN

Und natürlich muss die eingesetzte Technik maximalen Datenschutz und Datensicherheit gewährleisten: Der Hersteller sollte nachweisen können, dass er die in der DSGVO festgelegten Prinzipien „Security by Design“ (Art. 32) und „Privacy by Design“ (Art. 25) befolgt und sämtliche heute verfügbaren Techniken in seinen Produkten zur Verfügung stellt (aktuelle Tendenz: „Zero Trust“-Ansatz).

Diese reichen von einem technisch erzwingbaren „Vier-Augen-Prinzip“ für das Ansehen von Aufzeichnungen bis hin zu „Privaten Zonen“ für Bereiche, die nicht erfasst werden dürfen. Und natürlich möchte niemand, dass die eingesetzten Systeme verwendet werden, um in die dahinterliegenden IT-Systeme einzudringen. Die eingesetzten Videosysteme dürfen also nicht das „Einfallstor“ in die IT- und/oder gar in die OT-Netzwerke sein.

Dementsprechend müssen alle dem Stand der Technik entsprechenden und geeigneten technischen und organisatorischen Maßnahmen zur Cybersicherheit gemäß Vorgabe DSGVO umgesetzt sein. Die regulierten KRITIS-Betreiber und optional auch beteiligte Hersteller und Vorlieferanten müssen zusätzlich die geltenden KRITIS-Gesetze bzgl. IT- und Cybersicherheit beachten.



Einhaltung von Datenschutz durch technische Funktionen wie z.B. „Private Zonen“ (Bildbereich „schwärzen“).

PRAXISTIPP — **KRITIS-GESETZE ZU IT- UND CYBERSICHERHEIT**

GELTENDE GESETZE ZU IT- UND CYBERSICHERHEIT PRÜFEN UND EINHALTEN

Für KRITIS-Betreiber nach der KRITIS-Verordnung und deren Vorlieferanten gilt es zu prüfen, ob diese mit den international (z. B. EU-NIS-Richtlinien und Art 32 DSGVO) und national geltenden, einschlägigen KRITIS- und Cybersecurityvorschriften, wie in Deutschland dem IT-Sicherheitsgesetz 2.0 / BSIG konform gehen. Beachten Sie dazu die Informationen, die Paragraphen und Tipps in Kap. 3. Weitere Aspekte nachfolgend in Kap. 5.6.

5.6 PRIORITÄT CYBERSECURITY: SCHWÄCHSTES GLIED IN DER LIEFERKETTE ENTSCHEIDET

KRITIS sind seit ihrer Digitalisierung und unabhängig von der jeweiligen geopolitischen Lage digital-cybertechnisch angriffsaffine Ziele. Daher liegt beim Thema Cybersecurity und Resilienz eine sehr hohe Priorität, sowohl beim zuständigen Gesetzgeber, als auch beim KRITIS-Betreiber selbst und bei den seit dem IT-Sicherheitsgesetz 2.0 neu regulierten Herstellern und Vorlieferanten von kritischen Komponenten.

KRITIS sind verstärkt angriffsaffine Ziele seit 2022

Die Digitalisierung in den Kritischen Infrastrukturen ist seit Jahren voll im Gange, etwas zeitversetzt schreitet die Digitalisierung auch in der physischen Sicherheitsbranche voran. Digitale Geschäftsprozesse, Vernetzung von IT-und OT-Systemen und cloudbasierte Lösungen bieten aber auch mehr Angriffsfläche für Cyberkriminalität. Die digitale Angriffsfläche wächst stetig.

So dokumentieren Lageberichte des BSI zur IT-Sicherheit in Deutschland einen rasanten Anstieg bei cyber-krimineller Erpressung durch Ransomware und DDoS-Angriffe sowie immer mehr Schadprogramm-Varianten und BOT-Infektionen.

Jährliche Studien des Digitalverbands Bitkom berichten von immensen Schadenssummen für die deutsche Wirtschaft (200 Mrd. in 2022). Lt. der Studie werden fast 9 von 10 Unternehmen Opfer von Datendiebstahl, Spionage oder Sabotage.

Im Zuge des Krieges in der Ukraine erlangte die Awareness für IT- und Cybersicherheit eine noch größere Beachtung. Es geht nicht mehr einzig und alleine darum, „privatwirtschaftlich-organisierte“ Kriminelle abzuwehren. Cyber-Angriffe durch staatliche Akteure werden/wurden vermehrt zu einer realen Gefahr, z. B. durch staatlich angeordnete Backdoors oder Drittstaaten-Trojaner. Zudem versuchen politisch motivierte Hacker schon seit Jahren, die freiheitlich-demokratischen Systeme zu diskreditieren.

Beispiel:
BSI-Warnung im Jahre 2022 vor Verwendung der russischen Sicherheitssoftware von Kaspersky aufgrund der potentiellen Möglichkeit eines „staatlichen Durchgriffs“ bzw. staatlich verordneten, geopolitisch motivierten Missbrauchs.

Supply Chain Attacks – Sicherheitsrisiken aus der Lieferkette

Aber nicht erst seit dem von Russland initiierten Krieg und der BSI-Warnung vor dem Einsatz der AV-Lösungen von Kaspersky stellen viele Unternehmen und KRITIS-Betreiber Gedanken über Sicherheitsrisiken an, die von zugekauften Produkten ausgehen könnten. Medial bekanntgewordene Supply Chain Attacks wie z.B der Fall Solarwinds haben zudem bei vielen Unternehmen das Bewusstsein geschärft für diese Sicherheitsbedrohung „aus der Lieferkette“. Ein Angriff auf die Lieferkette zielt auf das schwächste Glied in einer Vertrauenskette ab. Wenn ein KRITIS-Unternehmen selber über eine hohe Cybersicherheit verfügt, aber einen unsicheren Vorlieferanten mit unsicheren kritischen Komponenten und Produkten hat, werden die Angreifer diesen Lieferanten/Hersteller ins Visier nehmen.

Burg und Burggraben-Ansatz reicht nicht mehr – Möglicher Ausweg „Zero Trust“

Die Herausforderung und die Zielstellung von KRITIS-Betreibern ist die Vermeidung IT-bedingter Verwundbarkeit.

Das Komplexe an der Zielstellung ist, dass mittels den jahrelang etablierten IT-Sicherheitsprozessen und Sicherheitskonzepten die Fremdverwundbarkeit durch vernetzte oder cloudbasierte Fremdsysteme nicht mehr so einfach abgefangen werden kann. Bislang galt der „Castle and Moat"-Ansatz (Burg und Burggraben-Ansatz), auch bekannt als Cyberperimetersicherheit, als wirksamste Methode gegen Cyber-Bedrohungen. Unternehmen aus KRITIS schützten ihre Netzwerke vor allem durch Firewalls, Proxy-Server und weitere Intrusion-Prevention-Tools. Das Prinzip der Cyberperimetersicherheit basiert darauf, die Eingangs- und Ausgangspunkte des Netzwerks zu überprüfen. Doch durch den Einsatz von Cloud Anwendungen und der Möglichkeit des Zugriffs durch Mitarbeiter von einer Vielzahl von Geräten und Standorten aus, hat sich das Bedrohungsszenario verändert. Ein weiterer Schritt hin zur mehr Sicherheit und Vertrauen könnte künftig ein sogenannter „Zero Trust"-Ansatz sein.

Eine nötige Grundvoraussetzung für eine ganzheitliche Sicherheitskette ist zudem, dass die Fremdsysteme und Subsysteme selber eigene, dem Stand der Technik entsprechende IT-Sicherheitsfunktionen implementiert haben, nach der DSGVO-Artikel 32-Forderung „Security by Design".

Schon gehört?
Durch den EU Cybersecurity Act (CSA) aus dem Jahre 2019 und den EU Cyber Resilience Act (CRA) aus dem Jahre 2022 sollen auf Produktebene ebenfalls „Security by Design" und „Security by Default" als Regelungsprinzipien für sicherheitsrelevante Produkte in ganz Europa verbindlich festgeschrieben werden. Eine ähnliche Regulierungstendenz auf Software-Produktebene ist in den USA mit dem sog. SBOM („Software Bill of Materials" – Software-Stückliste) neu zu beobachten – ein noch recht junges Konzept zur Erhöhung der Transparenz und der Sicherheit der Bestandteile von Software.

Cybersecurity und Künstliche Intelligenz
Eine weitere Problematik sei hier kurz angerissen, der immer noch viel zu wenig Aufmerksamkeit gewidmet wird: Der Cybersecurity-Resilienz beim Einsatz von Anwendungen mit Künstlicher Intelligenz und Videoanalyse.

Wenn ein paar kaum sichtbare Klebestreifen ein Stoppschild für die Fahrzeugkamera in ein 80 km/h-Schild verwandeln können, müssen Lösungen dafür gefunden werden. Was aber, wenn tatsächliche Cyberattacken auf KI-Systeme mit entsprechender, vielleicht gar nicht erkennbarer Manipulation des KI-Systems selbst, stattfinden?

Es dürfen ausschließlich KI-Technologien zum Einsatz kommen, die ein Höchstmaß an Datenschutz und Daten-/Cybersicherheit aufweisen. Zudem muss die KI ethisch vertretbar sein.

Auf EU-Ebene werden derzeit entsprechende Richtlinien erarbeitet für eine „vertrauenswürdige KI". Nach diesem risikobasierten EU-Ansatz soll KRITIS in die Risikoklasse B „Hohes Risiko" eingruppiert werden. In dieser Risikoklasse sollen KI-Anwendungen erlaubt werden mit speziellen Anforderungen an Cybersicherheit, Verantwortlichkeit, Transparenz, Datenschutz, Ethik und an eine hohe Datenqualität. Siehe mehr dazu in Kap. 7.7.

Wir als Hersteller würden eine solche EU-weite KI-Verordnung begrüßen und empfehlen auch jedem KRITIS-Betreiber im Eigeninteresse, seine KI-Anwendungen und Anbieter nach solchen vertrauenswürdigen KI-Kriterien zu bewerten.

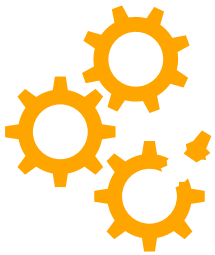
Cybersecurity hat Priorität 1
In den vorangegangenen Kapiteln hat dieser Praxisleitfaden bereits ausführlich die Gesetze, Aktualität, Priorität und die Maßnahmen zur Cybersicherheit in KRITIS beleuchtet.

Nachfolgend hier nur noch einmal der Dringlichkeit geschuldet als Wiederholung die wichtigsten Sicherheitspraxistipps für eine ganzheitliche KRITIS-Sicherheitsstrategie:

CYBER-SICHERHEITSTIPP

SCHWÄCHSTES GLIED IST ENTSCHEIDEND

SCHWÄCHSTES GLIED IN DER LIEFERKETTE ENTSCHEIDEND FÜR DIE GESAMTE KRITIS-CYBERSECURITY



Da die Videodevices ja Teil der IT-Gesamtinfrastruktur der KRITIS sind, bitte folgenden Sicherheitstipp beachten:

„Eine KRITIS Sicherheits- und Lieferkette ist nur so stark wie ihr schwächstes Glied."

„SCHWÄCHSTER" HERSTELLER/VORLIEFERANT BEI KRITISCHEN KOMPONENTEN MITENTSCHEIDEND

Bei der Garantieerklärung lt. § 9b Absatz (3) BSIG bitte Augenmerk auf die unternehmerische und IT-technische Vertrauenswürdigkeit der Hersteller und Vorlieferanten und ihrer Produkte legen.

Machen Sie den Herstellercheck gemäß Kap. 9.5 und berücksichtigen diesen Aspekt bei den Technologieentscheidungen in den Kap. 7ff.

PRAXISTIPP

BEST PRACTICES EINHOLEN UND ABFORDERN

KRITIS-BETREIBER, PLANER UND ERRICHTER SCHÄTZEN BESONDERS ZWEI DINGE

Zum einen die Unterstützung durch den Hersteller mit „Best Practice"-Materialien zu Cybersecurity und Datenschutz, zum anderen „Security by Default": Das Aktivieren der wichtigsten Security-Funktionen ab Werk, was die Fehlerquote bei der Konfiguration deutlich verringert.

INFOS ZU CYBERSICHERHEIT UND DATENSCHUTZ BEI VIDEOSYSTEMEN

Genauere Informationen zu Datenschutz und Datensicherheit bei Videosystemen finden Sie hier – von Dokumenten der EU und DSK (Datenschutzkonferenz) bis zu herstellerspezifischen Techniken wie etwa die Broschüre „Videosicherheit, Datenschutz und Datensicherheit" oder den „Best Practice Guide Cybersecurity"

5.7 WAS HAT HERSTELLER-ETHIK MIT DATENSCHUTZ UND DATENSICHERHEIT ZU TUN?

Gerade in so sensiblen Bereichen wie der Sicherheitstechnik geht es nicht allein um die technische Lösung. Kunden – und bei der KRITIS-Überwachung manchmal bzw. insbesondere auch die Öffentlichkeit – möchten wissen, „mit wem sie es zu tun haben". Videosicherheitssysteme müssen die jeweils landesspezifischen und weitere überregionale Regelungen zum Datenschutz, wie etwa die europäische Datenschutz-Grundverordnung (DSGVO), einhalten. Neben dem Vertrauen, dass personenbezogene Daten nach den Vorgaben der DSGVO und der geltenden Gesetze behandelt und verarbeitet werden, spielen auch zunehmend Aspekte der Ethik und der Menschenrechte eine Rolle.

Entscheider sind gut beraten, zu recherchieren, ob mit der favorisierten Lösung – auch wenn sie unter Umständen auf den ersten Blick die billigste ist – nicht anderswo gravierend Menschenrechte verletzt werden. Auch das Thema Nachhaltigkeit (Ökologie, Soziales, Ökonomie) spielt bei der Kaufentscheidung zunehmend eine wichtige Rolle.

Auf dem Markt für Videosicherheitstechnik werden Themen wie ethische Verantwortung, Nachhaltigkeit und vertrauenswürdige KI-Anwendungen immer wichtiger im Rahmen der eigenen „Corporate Social Responsibility".

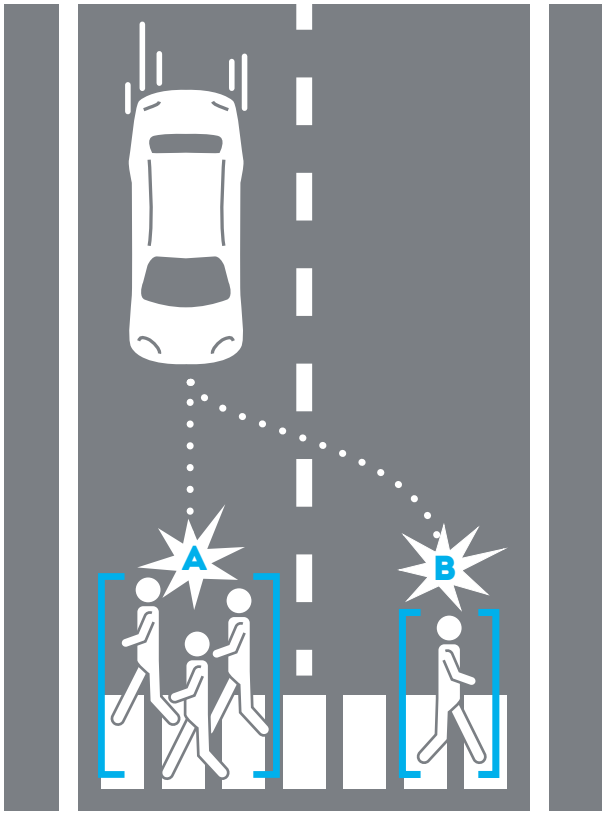
Ethische Verantwortung – ein reales Beispiel aus der Videobranche
So installierte im Oktober 2020 das EU-Parlament Kameras eines chinesischen Herstellers in Staatseigentum, dessen Systeme auch im Rahmen der Uiguren-Internierungen in Xinjiang zum Einsatz kommen. Aufgrund des öffentlichen Drucks und unter Zustimmung von fast 90 % der Abgeordneten wurden diese im April 2021 wieder entfernt. Dies ist nur ein Beispiel, um die Thematik zu illustrieren: Der öffentliche Druck zum ethischen Handeln wächst. Hier kann sich eine Investition in die falschen Produkte schnell als wirtschaftliche Sackgasse und öffentlichkeitswirksam negativer Bumerang erweisen.

Ethische Verantwortung in der Lieferkette: Lieferkettensorgfaltspflichtengesetz
Der Aspekt der Ethik und der Beachtung von Menschenrechten entlang der ganzen Lieferkette wird weltweit zusehends gesetzlich reguliert, z. B. in Deutschland durch das neue „Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten", kurz Lieferkettensorgfaltspflichtengesetz / Lieferkettengesetz (LkSG).

Gültig ist das LkSG (hier im Gesetzestextwortlaut) ab dem Jahr 2023 für Unternehmen ab 3.000 Mitarbeitenden, ab dem Jahr 2024 ab 1.000 Mitarbeitenden.

Künftig müssen also große Unternehmen dokumentieren und nachweisen, wie sie entlang ihrer ganzen Lieferkette die Einhaltung von Menschenrechten und ethischen Standards gewährleisten. Die Bundesregierung erwartet von Unternehmen die Einführung eines Prozesses zur Beachtung von menschenrechtlichen und umweltbezogenen Sorgfaltspflichten. Diese Sorgfaltspflichten beziehen sich auf den eigenen Geschäftsbereich und unmittelbare Zulieferer. Für mittelbare Zulieferer gilt eine anlassbezogene Sorgfaltspflicht, d. h. Unternehmen müssen allein bei substantiierten Hinweisen auf mögliche Rechtsverletzungen in der Lieferkette tätig werden.

Das ist aus unserer Hersteller-Sicht ein wichtiger Schritt in die richtige Richtung. Es muss aber auch ein nachvollziehbarer Prüfmechanismus für die Prüfung der Vertrauenswürdigkeit der Hersteller und Lieferanten und der Lieferprozesse etabliert werden. Dieser Prüfprozess darf aber nicht, wie bei der DSGVO gesehen, durch inflationäre oder „Pseudo-Ethik-Zertifikate“ oder „Scheinzertifikate für menschenrechtsverletzungslose Lieferketten“ unterlaufen werden.



Ethische Verantwortung bei KI-Anwendungen
Der Aspekt der Ethik ist bzw. wird künftig noch mehr als jetzt schon entscheidend sein bei der Entwicklung von KI-Anwendungen. Ein mit Künstlicher Intelligenz arbeitendes System soll demnach nicht nur in normativer Hinsicht absolut unbedenklich sein. Es soll auch ethischen Grundsätzen genügen – und darf nicht nur keinen technischen, sondern auch keinen sozialen Schaden z. B. durch intransparente Entscheidungsprozesse oder diskriminierende KI-Ergebnisse („Bias-Problem“) anrichten. Auf EU-Ebene werden derzeit entsprechende Richtlinien erarbeitet für eine „sichere, vertrauenswürdige und ethisch vertretbare KI“. Die Einhaltung ethischer Standards ist bei KI ein Muss und kein freiwilliges Beiwerk.

Die Frage nach den ethisch-moralischen Folgen von KI: Das immer noch ungeklärte Dilemma beim Unfallverhalten eines autonom fahrenden Autos ist da ein fast schon klassisches Beispiel.

PRAXISTIPP **„ANBIETER-CHECK MACHEN“**

ANBIETER AUF KRITERIEN DATENSCHUTZ & DATENSICHERHEIT UND ETHIK PRÜFEN

„Prüf- und Fragen-Checklisten“ als Entscheidungshilfe finden Sie am Ende dieses Dokuments im Kap. 9.5.

6 ÖFFENTLICHKEIT & PRESSE: EIN KOMMUNIKATIONSKONZEPT HILFT

Nicht selten scheuen am Entscheidungsprozess Beteiligte die Presse und damit die Öffentlichkeit, da diese v.a. bei öffentlich-rechtlichen KRITIS-Projekten oftmals als Gegenspieler und damit als „Verhinderer“ bzw. „Bremser“ im Prozess gesehen werden. Diese Beteiligten von Anfang an als „Sparringspartner“ ernst zu nehmen und – wenn möglich – mit „ins Boot zu holen“ wird den Gesamtprozess in den allermeisten Fällen verkürzen, vereinfachen und beschleunigen.

Auch wenn dies am Anfang vielleicht mehr Zeit in Anspruch nimmt: Mit einem klar strukturierten und begleitendem internen und externen Kommunikationskonzept können Sie die Erfolgswahrscheinlichkeit und Akzeptanz positiv beeinflussen.

Auf Pressevertreter proaktiv zuzugehen und beispielsweise eine Pressekonferenz einzuberufen, kann helfen, Vorurteile und Hürden gleichermaßen abzubauen.

6.1 KNOW-HOW-LÜCKEN SCHLIESSEN UND ÖFFENTLICHKEIT EINBINDEN

Die Presse hat ihren berechtigten Aufklärungs- und Informationsauftrag und sie will, muss und wird diesem nachkommen – sei es mit Ihnen oder ohne Sie. Die Erfahrung zeigt, dass häufig nur fehlendes Wissen über Entscheidungsprozesse, die Rechtslage, Erfolgsnachweise, die eingesetzten Technologien usw. der Grund für Widerstand gegen geplante Maßnahmen ist. Eine entsprechende Aufklärung erhöht oftmals bereits lange im Vorfeld der geplanten Maßnahmen das Verständnis und die Akzeptanz wesentlich.

6.2 STATT „KALTER SCHULTER“: LIEBER VERSTÄNDNIS ZEIGEN

Ein Kommunikationskonzept hilft, Informationsdefizite zu schließen. Hersteller und Facherrichterunternehmen unterstützen gerne mit entsprechenden Experten. Dasselbe trifft übrigens auch auf die möglicherweise als am meisten störend wahrgenommenen Beteiligten: Bürgerinitiativen und vergleichbare Protagonisten. Auch hier ist es empfehlenswert, das Gespräch zu suchen und aufzuklären. Ganz häufig sind auch diese Gruppen gar nicht negativ gegenüber der Videotechnologie an sich eingestellt, sondern wünschen sich schlichtweg Transparenz und ein Verständnis sowie Diskussionsbereitschaft für ihre als berechtigt empfundenen Bedenken.

PRAXISTIPP — **AUFEINANDER ZUGEHEN**

TRANSPARENZ UND DISKUSSIONSBEREITSCHAFT

Ganz am Anfang des Entscheidungsprozesses sind Aufklärungsveranstaltungen für die Presse sinnvoll, in denen die spezifischen Herausforderungen (Gefahrensituation und Risikograd, Ereignisse und Historie, Anforderungen und Schutzziele, Standort und Planung, Datenschutz und Datensicherheit usw.) dargelegt werden. Es ist fast immer besser, die Presse aktiv zu informieren, anstatt auf Anfragen erst zu reagieren, wenn sie schon gestellt wurden. Ein proaktives statt reaktives Vorgehen zeigt, dass Sie die Presse als Institution und Partner auf Augenhöhe ernst nehmen. Gleiches kann auch für entsprechende Initiativen und dergleichen gelten.

7 TECHNOLOGIE- UND FINANZENTSCHEIDUNGEN

Die technische Entwicklung befindet sich (wieder einmal) in einem höchst dynamischen Wandel. Dies gilt insbesondere im Bereich „KRITIS“: Konventionelle Videosicherheitstechnik entwickelt sich durch Analytik, KI und moderne Softwarelösungen unaufhaltsam zu einem Mehrzweck-Tool, das Anwender künftig auch verstärkt für andere „SMART KRITIS“-Projekte wie etwa die Verkehrsflusssteuerung (Transport & Verkehr) und viele andere Anwendungen einsetzen. Die vielen unterschiedlichen Kameratechnologien und Softwareplattformen bieten Vor- und Nachteile, deren detaillierte Betrachtung hier jedoch zu weit greifen würde.

Stattdessen soll auf die allgemeine Fragestellung eingegangen werden, mit der sich KRITIS-Verantwortliche informiert an die richtige Hardware-, Software- und KI-Technologie „heranarbeiten“ können und die Sie vielleicht auch dem Hersteller oder Errichter-Partner bei der Auswahl stellen können.

Eine Zusammenfassung aller wichtigen Detailfragen bzw. einen Fragenkatalog zur Technologieentscheidung finden Sie im Kap. 9.4.

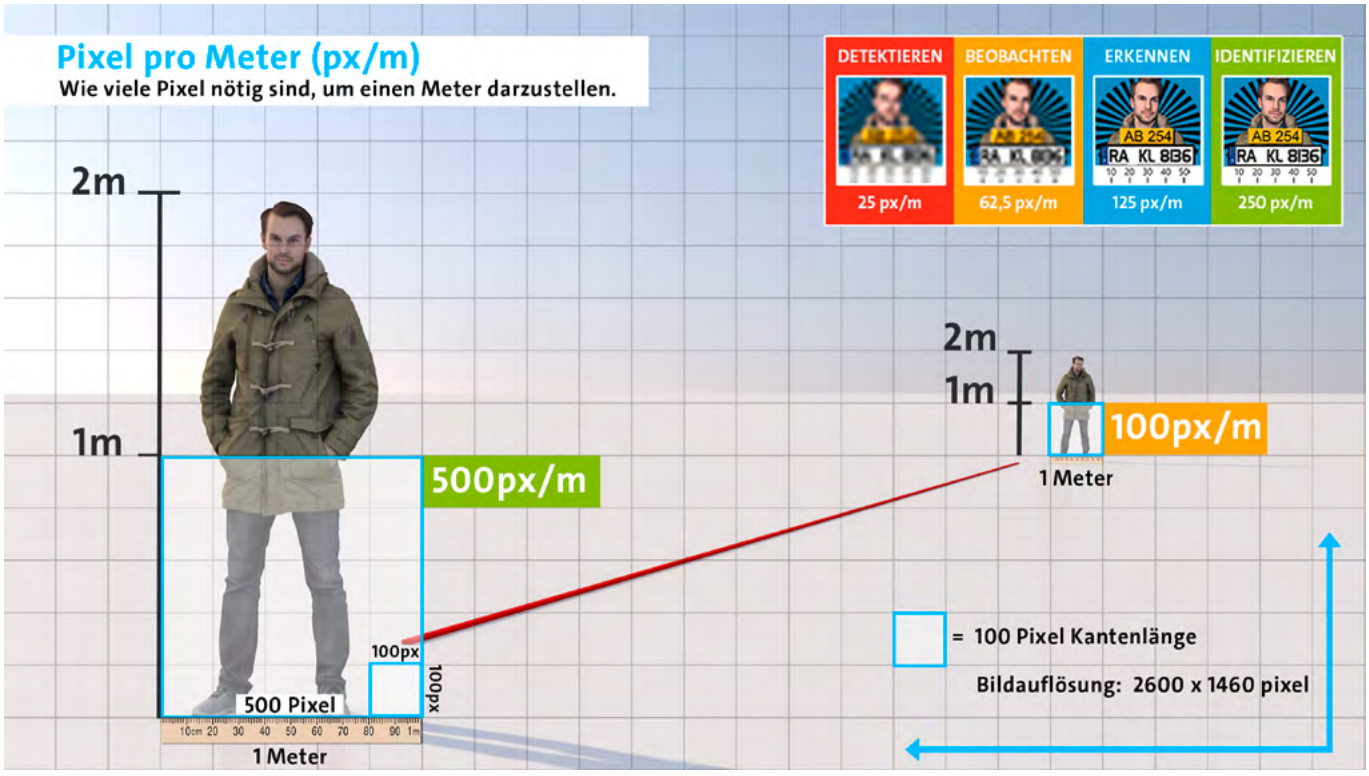
7.1 WIE VIELE KAMERAS FÜR WELCHE FLÄCHE?

Bei der KRITIS-Überwachung geht es meist darum, große Flächen und/oder lange Distanzen zu erfassen. Dabei spielt naheliegenderweise die Bildqualität eine wesentliche Rolle – sowohl für die Verwertbarkeit vor Gericht als auch für die genaue Erkennbarkeit von Detailzusammenhängen. Nur so lassen sich Täter identifizieren und Vorgänge rekonstruieren.

Wie aber definiert sich eigentlich die Bildqualität zur Überwachung großer Flächen? Entscheidend für die Qualität ist die nötige Auflösung. Da diese auf der gesamten Fläche zum Tragen kommen soll und einen bestimmten Mindestwert nicht unterschreiten darf, spricht man von „Auflösungsdichte“ bzw. „Pixeldichte“. Diese ist in der Norm DIN EN 62676-4 definiert (siehe Kap. 7.2). Hat man diese Auflösungsdichte über den gesamten zu überwachenden Bereich ermittelt, kann man daraus mit dem Hersteller zusammen durch eine Vorplanung den Kamerabedarf ableiten (allerdings bieten nicht alle Hersteller diese Möglichkeit).

Das A und O bei Videoüberwachung:
So wenige Kameras wie möglich, so viel Auflösung wie nötig
Moderne Kameratechnik – richtig ausgewählt, geplant (*) und implementiert – kann heute mit wenigen Systemen große Flächen und lange Distanzen abdecken.

(*) Apropos „richtig geplant“: Mehr zum Thema „3D-Planung mit exakter Angabe der Pixeldichte im digitalen Zwilling“ - siehe Kap. 7.6

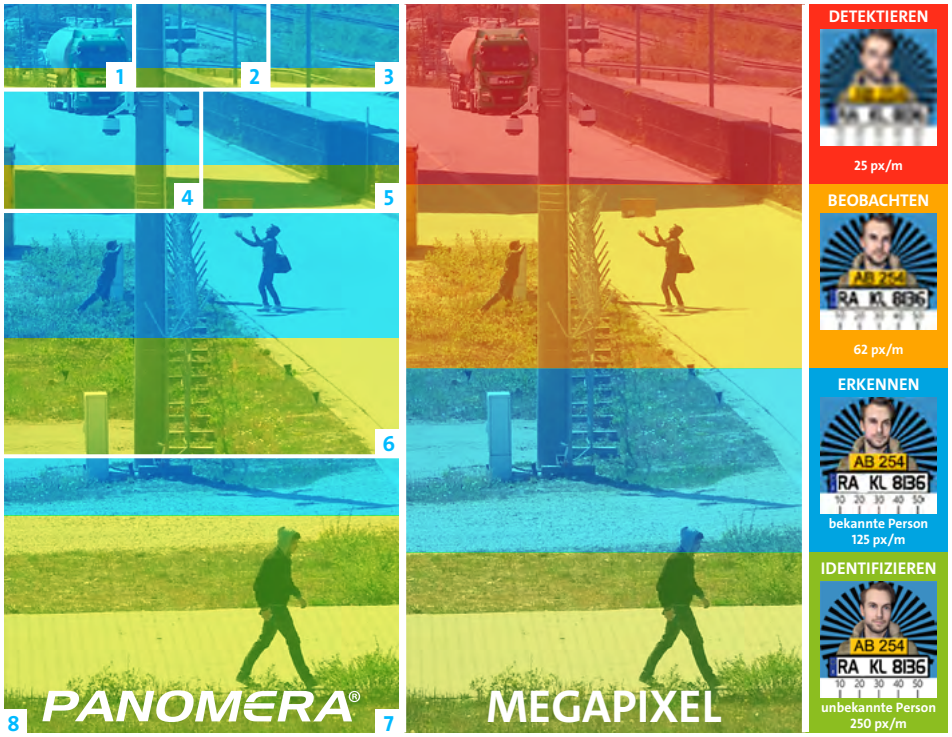


Pixel pro Meter – der globale Standard für die Bildqualität von Videosicherheitssystemen (DIN EN 62676-4).

7.2 WAS IST EIGENTLICH „MINDESTAUFLÖSUNG“ UND WIE VIEL BENÖTIGE ICH?

Die beiden Größen „Mindestauflösung in Pixel pro Meter (px/m)“ und „Quadratmeter pro Kamera“ stehen in engem Zusammenhang. In vielen Fällen sind 250 px/m („Identifizieren“) nach DIN EN 62676-4 oder mehr für eine zuverlässige Gerichtsverwertbarkeit der Bilder erforderlich. Dabei handelt es sich sehr vereinfacht gesagt um den Wert, bei dem ein Richter mit hoher Wahrscheinlichkeit sagen wird, dass er die vor ihm sitzende Person und die Person auf dem Videobild für identisch hält oder eben nicht. Dabei muss dies auch bei schlechten Lichtverhältnissen möglich sein.

Für andere Anwendungszwecke z. B. mit der Anforderung „Erkennen“ sind nach der DIN EN 62676-4 mindestens 125 px/m nötig.



Die in der DIN EN 62676-4 festgelegten Werte für die Mindestauflösung sind die Grundlage für jede Planung. Je nach Technologie verändert sich diese mit zunehmender Entfernung.

PRAXISTIPP | **DIN EN 62676-4**

DIN EN 62676-4 UND FLÄCHE

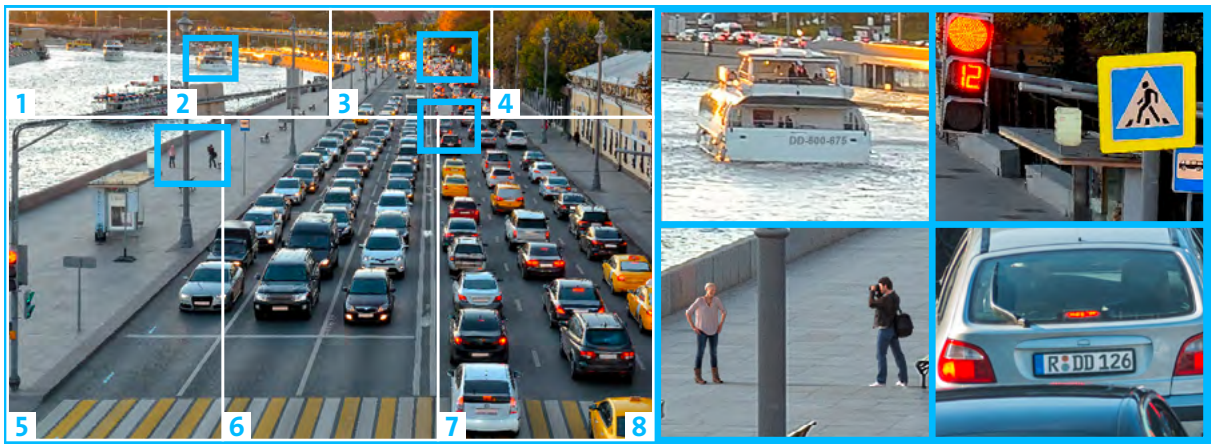
Die beiden Größen „Mindestauflösung in Pixel pro Meter (px/m)“ und „Quadratmeter pro Kamera“ stehen in engem Zusammenhang. Meist sind 125 px/m („Erkennen“) oder 250 px/m („Identifizieren“) nach DIN 62676-4 im Projekteinsatz gefordert.

7.3 DIE KAMERA-HERAUSFORDERUNG: GROSSE FLÄCHEN, LANGE DISTANZEN

Hochwertige, besonders für die KRITIS-Überwachung geeignete Kameras schaffen es, diese Auflösungsdichte für 1.000 Quadratmeter oder für eine Strecke von 160 Metern pro Kamera zu erreichen. Dies funktioniert allerdings nicht mit einfachen Kamerasystemen. Besonders gut geeignet sind sogenannte Multifocal-Sensorsysteme, die die Bilder von bis zu sieben Detail- und einem Übersichtssensor in einer optischen Einheit kombinieren. Die Einzelbilder werden per Software zu einem Gesamtbild zusammengefügt und können so sehr großräumige Zusammenhänge abbilden. Die Bediener können dann in diesem Übersichtsbild theoretisch unbegrenzt viele Zoombereiche öffnen und hochauflösend beliebige Details betrachten.

Diese Technik ist in vielen Kritischen Infrastrukturen weltweit im Einsatz und bietet mehrere Vorteile:

- Die Bediener müssen deutlich weniger Kamerabilder und Bildschirme als bei konventionellen Lösungen im Auge behalten.
- Beliebig viele „virtuelle“ PTZs: Per Mausklick lassen sich beliebig viele hochauflösende Detailzooms im Gesamtbild öffnen. Besonders bei komplexen Lagen ein unschätzbarer Vorteil.
- Alle Bereiche werden ständig hochauflösend aufgezeichnet – ganz im Gegensatz zu den weit verbreiteten PTZ-Kameras.
- Im KRITIS-Einsatz reicht eine Kamera für mindestens 1.000 Quadratmeter (meist sogar noch mehr). Damit ist die Multifocal-Sensortechnologie die einzige Technologie, die immer den gesamten Objektraum hochauflösend abdeckt.
- Durch die geringe Menge an benötigten Kameras sinken Infrastruktur- und Betriebskosten deutlich.



Szene: KRITIS-Sektor „Transport und Verkehr“ - Binnenschifffahrt und Straßenverkehr

Die Multifocal-Sensortechnologie ist besonders gut für die KRITIS-Überwachung geeignet: Selbst in komplexen Lagen steht immer ein hochauflösender Gesamtüberblick zur Verfügung, auch in der Aufzeichnung. Gleichzeitig können Bediener parallel eine theoretisch unbegrenzte Zahl an Detail-Zooms öffnen („virtuelle PTZs“).

Technische Besonderheiten der Multifocal-Sensortechnologie sind unter anderem:

MULTIFOCAL- SENSORTECHNOLOGIE

- Einsatz von Objektiven unterschiedlicher Brennweiten
- „Staffelung“ der Szene
- Hoher Dynamikumfang (Bildbereiche unterschiedlicher Helligkeit werden gut erfasst)
- Durchgängige Tiefenschärfe
- Optimale Brennweite für jeden Bereich
- Gleichbleibendes Auflösungsraster über den gesamten Objektraum

PRAXISTIPP

KAMERA-TECHNOLOGIEVERGLEICH

UNTERSCHIEDLICHE KAMERATECHNOLOGIEN FÜR UNTERSCHIEDLICHE EINSATZBEREICHE

Eine Analyse der verschiedenen Technologien und ihrer Vor- und Nachteile – wie PTZ (Pan-Tilt-Zoom, also Schwenken, Neigen, Zoomen), Megapixel (Single-Sensor), Multisensor oder Multifocal-Sensor – bietet der Fachartikel „Welche Kameratechnologie für welchen Zweck?“ (erschienen in: PROTECTOR 9/2020).

Zum Selbstausprobieren (Desktop empfohlen):
Der interaktive Kamerasimulator – am Beispiel KRITIS-Perimeterüberwachung

PRAXISTIPP **ANBIETERCHECK**

LÄSTIG SEIN UND GENAU NACHFRAGEN

Fragen Sie Ihren Anbieter ganz genau, wie viele Quadratmeter pro Kamerasystem in der benötigten Pixeldichte abgedeckt werden können. Fragen Sie zudem nach den Kosten und wie viele Bildschirmarbeitsplätze / Monitore für Personal vorgehalten werden müssen. Achten Sie darauf, dass die Werte genau definiert werden und nachvollziehbar sind. Am besten durch eine entsprechende 3D-Vorplanung.

7.4 DIE SOFTWARE-HERAUSFORDERUNG: GROSSE AUSWAHL, VIELE FUNKTIONEN

Offene, flexible Softwareplattform

Herausforderung softwareseitiges Sicherheits- und Videomanagement:
Vor lauter Bäumen den Wald nicht sehen.

Am Markt für Videomanagementsoftware gibt es eine Vielzahl an guten Einzelanwendungen von diversen Sicherheitssoftwareherstellern für die unterschiedlichsten Anforderungen und Einsatzbereiche in KRITIS.

Von der klassischen Video- und Alarm-Managementsoftware VMS, über Vorfalls- und „Situational Awareness“-Management, über KI-basierte Videoanalyse bis hin zum Daten- und Integrationsmanagement innerhalb einer Gebäude- und Gefahrenmanagementlösung (PSIM).

Die hohe Kunst für KRITIS-Betreiber besteht nun darin, dass alle funktional nötigen Einzelsoftwareanwendungen zueinander kompatibel sind und der ganze Video-, Daten- und Informationsfluss und die Kommunikation aus einem Guss und medienbruchfrei funktionieren.

Zudem muss die Kompatibilität und Integrationsfähigkeit zu diversen Hardwareprodukten wie v. a. zu IP-Kameras oder Aufzeichnungshardware gewährleistet ein. Nicht zu vergessen ist eine durchgängige Sicherheit bzgl. Datenschutz und Datensicherheit.

Für diese herausfordernde Aufgabenstellung hat sich in der Sicherheitsbranche ein sogenannter offener Plattform-Ansatz bewährt, der auf der einen Seite die ganzheitliche Durchgängigkeit und Sicherheit gewährleistet, auf der anderen Seite aber auch die benötigte Offenheit und Flexibilität für benötigte Integrationen und Schnittstellen nach dem Best-of-Breed Ansatz offen lässt.

Flexibles Lösungsdesign dank Plattformansatz
Ein offener Plattformansatz hat sich in zahlreichen KRITIS-Projekten erfolgreich bewährt und bietet mehrere Vorteile für die KRITIS-Anwender:

- Kunden können aus einer Art „Baukasten“ aus:
    - Video- und Alarmmanagement
    - KI-basiertes Analyse- und Datenmanagement
    - digitales Vorfalls- und „Situational Awareness“-Management
    - Map-Management zur Verortung von Events und Alarmen
    - und Frontend-Applikationen
- genau die für ihre Anwendung nötigen Module auswählen und individuell zusammensetzen.
- Security-Operatoren oder Prozessverantwortliche können damit fundierte Entscheidungen treffen.
- Es resultieren Software-Bundles, die dem Kunden die benötigte Funktionalität und zudem Wahlmöglichkeiten und Flexibilität offen lassen.

Wie sich diese Software-Bundles zusammen mit Kamera- und Aufzeichnungssystemen zu einer KRITIS-Gesamtsicherheitslösung zusammenstellen lassen und welche zwei Strategien es dabei gibt, erfahren Sie im folgenden Kap. 7.5.

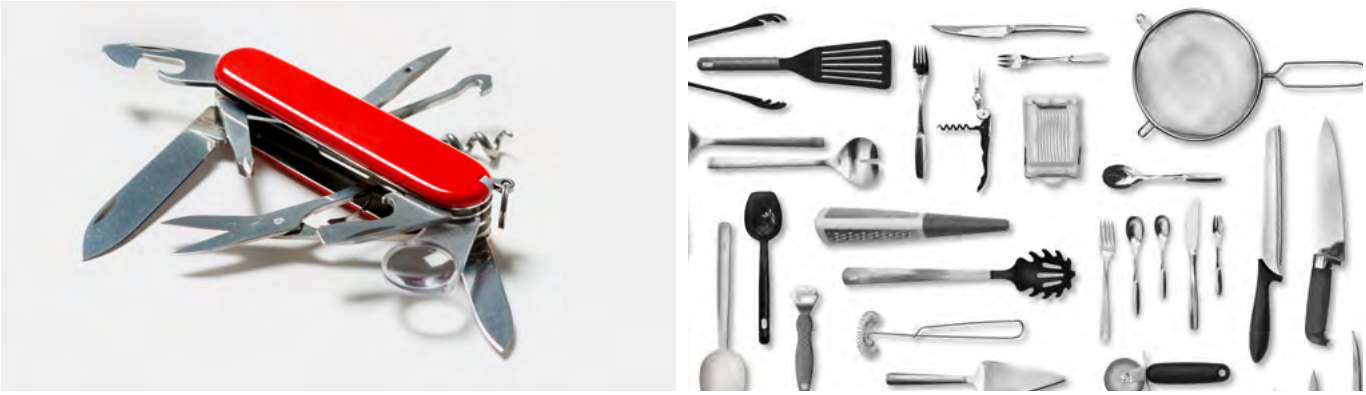
7.5 BEST-OF-BREED ODER ALLES AUS EINER HAND ODER BEIDES?

Bei der Zusammenstellung Ihrer KRITIS-Gesamtsicherheitslösung aus Software-Bundles, Kameras und Aufzeichnungssystemen stehen Ihnen grundsätzlich zwei bekannte und bewährte Handlungsoptionen zur Auswahl.

Best-of-Breed oder Alles aus einer Hand – oder beides
Schon seit längerer Zeit konkurrieren zwei verschiedene Ansätze miteinander: „Best-of-Breed“ oder „Alles aus einer Hand“.

Vereinfacht gesagt müssen Sie sich entscheiden, ob Sie entweder das für die jeweilige individuelle Einzelanforderung vermeintlich „beste“ Produkt von unterschiedlichen Anbietern auswählen und so Ihre vermeintlich beste Gesamtlösung „zusammenkombinieren“ oder aber, ob die Antwort eher in der „Alles aus einer Hand-Komplettlösung“ eines einzigen Anbieters zu finden ist.

Bei beiden Optionen ist immer das Ziel und die Aufgabenstellung, all Ihre Sicherheits- oder Prozessanforderungen vollständig und durchgängig abzudecken.



Alles aus einer Hand Ansatz und Best-of-Breed Ansatz.

Welche Vor- und Nachteile gibt es jeweils?
Beide Ansätze haben natürlich ihre Daseinsberechtigung und bringen jeweils Vor- und Nachteile mit sich – doch welche empfiehlt sich für Sie am ehesten, im Hinblick auf Funktionsumfang, Skalierbarkeit, Integrationsfähigkeit und Benutzerfreundlichkeit?

Es würde in diesem Praxisleitfaden zu weit führen, die allgemeinen Argumente für das Für und Wider des jeweiligen Ansatzes hier zu erläutern. Hierzu gibt es zahlreiche Fundstellen im Internet.

Praxiserfahrung zeigt: Es kommt immer auf den Einzelfall an
Die Wahl zwischen einer Komplettlösung aus einer Hand und modularen Einzellösungen ist nicht immer leicht. Wie Sie sich vielleicht vorstellen können, lässt sich diese Frage nicht pauschal beantworten. Mit welcher Strategie Sie am

besten fahren, hängt von verschiedenen Faktoren ab. Es kommt vor allem auf Ihre Anforderungen und die individuellen Gegebenheiten im Unternehmen an.

Auch entscheidend: Welches Equipment und welche Infrastruktur sind bereits vorhanden?

Bei Neuprojekten „auf der grünen Wiese" können Sie natürlich zwischen beiden Optionen leichter entscheiden als bei der häufig anzutreffenden Situation, dass in bestimmten Teilbereichen bereits Lösungen und Produkte vorhanden und „gesetzt" sind, d. h. bestehen bleiben sollen.

In letzterem Fall kommt häufig der Best-of-Breed Ansatz schon allein deshalb nur in Frage, weil der beim Kunden gesetzte aktuelle Anbieter gar nicht die Produkte im Portfolio hat, welche für die Erweiterung oder Neuanforderung nötig wären.

Das spricht für die Best-of-Breed Strategie
Best-of-Breed Lösungen sind in ihrem jeweiligen Fachgebiet bzw. beim Ausführen einer Spezialanforderung / Spezialaufgabe überlegen und punkten vor allem mit Speziallösungen.

Ein Beispiel für eine Spezialanforderung im Videobereich ist das Überwachen von großen Flächen oder langen Distanzen mit möglichst wenigen Kameras und möglichst wenigen Installationspunkten, aber immer unter Einhaltung der geforderten Mindestauflösung („Bildqualität am Zielpunkt") für z. B. „Erkennen" oder „Identifizieren" nach DIN 62676-6 (siehe dazu Kap. 7.2).

Machen Sie sich Gedanken zu folgenden Punkten:

- Wie ist Ihre Systemlandschaft bisher aufgebaut?
- Was ist bereits von welcher Marke vorhanden, was wird neu benötigt?
- Welcher Hersteller ist lieferfähig?
- Welche Probleme und Anforderungen müssen Sie aktuell und künftig bewältigen?
- Welche Themen haben Priorität?
- Wie komplex sind die abzubildenden Prozesse?

Eine Kombination beider Modelle?
Wie im echten Leben ist bei Projekten nicht immer alles schwarz oder weiß. Warum also sich nur für eine Option entscheiden? In der Praxis verwenden viele Unternehmen eine Mischung beider Ansätze, da sich die beiden Modelle auch gut miteinander kombinieren lassen.

ONVIF als „Best-of-Breed enabler" und Bindeglied
Für den Best-of-Breed Ansatz in der Sicherheitstechnik haben die marktführenden Hersteller einen Industriestandard und ein gemeinsames Kommunikationsprotokoll namens „ONVIF" entwickelt.

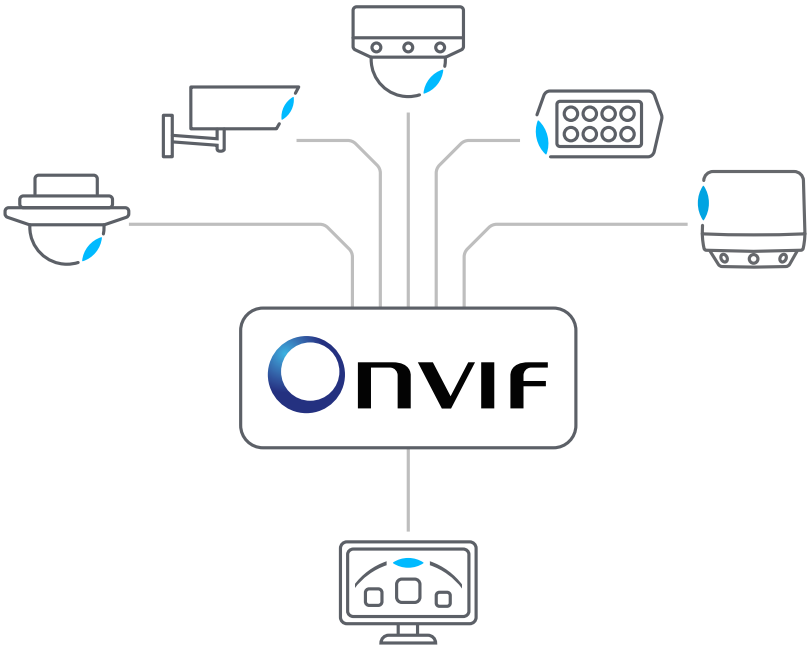
ONVIF ist eine Abkürzung für „Open Network Video Interface Forum". Es steht sowohl für ein globales Forum als auch ein globales Protokoll, das die nahtlose Zusammenarbeit und Integration verschiedener IP-basierter Überwachungs- und Sicherheitsgeräte von unterschiedlichen Herstellern ermöglicht.

PRAXISTIPP

BEST-OF-BREED AUS KAMERATECHNOLOGIE UND VIDEOMANAGEMENTSYSTEM

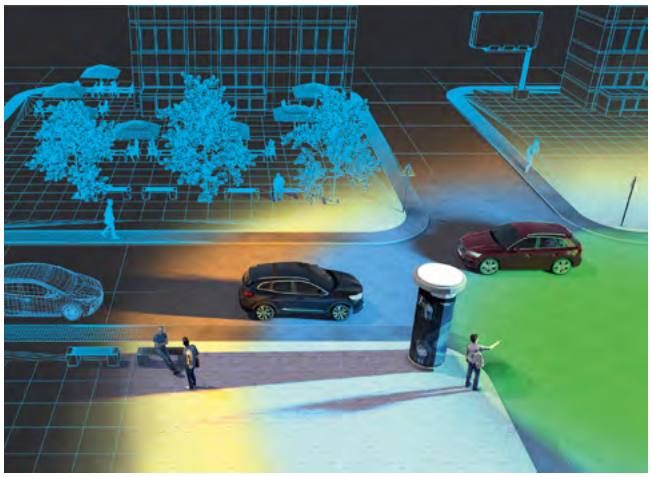
SCHON GEWUSST? MULTIFOCAL-SENSORTECHNOLOGIE FUNKTIONIERT MIT FÜHRENDEN VIDEOMANAGEMENTSYSTEMEN

Durch die Integration der Multifocal-Sensortechnologie in marktführende Videomanagementsysteme steht diese Kameratechnologie auch den Anwendern und Verfechtern des Best-of-Breed Ansatzes zur Verfügung und eröffnet so völlig neue Möglichkeiten bei der Beobachtung und Überwachung weitläufiger Flächen und großer räumlicher Zusammenhänge.



Das Protokoll ONVIF ermöglicht Anwendern die Integration sämtlicher ONVIF-Kameras (Single-Sensor-Kameras sowie Multifocal-Sensor-Kameras) in ihr bevorzugtes Video Management System.

7.6 PLANUNG IST GUT – PLANUNG IN 3D IST (NOCH) BESSER



Gute Planung ist alles

Zu Beginn eines Projekts ist ein „digitaler Zwilling" der Umgebung mittels einer 3D-Planung von großem Vorteil. Dabei werden alle Planungen und Veränderungen von 3D-Spezialisten solange durchgeführt, bis das Lösungskonzept technisch und datenschutzrechtlich „wasserdicht" ist. Dies gewährleistet eine optimale, kosteneffiziente Planung und Umsetzung und garantiert die eigene Zielsetzung zur Vermeidung planungsbedingter Verwundbarkeit Kritischer Infrastrukturen. Und all das unter Berücksichtigung von Budget, Zeit, Datenschutz und Datensicherheit.

Für KRITIS-Betreiber, KRITIS-Datenschutz-Stakeholder und für Architekten, Planer und Facherrichter ergeben sich folgende Vorteile:

Mehrwert durch 3D-Planung

- Vermeidung planungsbedingter Verwundbarkeit Kritischer Infrastrukturen
- Planungs- und Kostensicherheit
- Persönliches Vorab-„Erleben" der Lösung
- 100%ige Flexibilität in der Planungsphase
- Keine bösen nachträglichen Überraschungen durch Planungsansatz „What we plan is what you get"
- Erstellung eines detailgetreuen „digitalen Zwillings" der Umgebung
- Erkennen und Umgehen von Sichtfeldverdeckungen
- Exakte Simulation und Festlegung der Auflösungsdichten innerhalb der gesamten Umgebung
- Festlegen und Erreichen objektiver Leistungskriterien (z. B. Bildqualität gem. DIN EN 62676-4)
- Diagnose und Planung der IT-Infrastruktur (z. B. Netzwerk und Speicherplatzbedarf)
- Parallele optionale Nutzung von BIM-Modellen (Building Information Modeling), Sicherheitsprodukte als „digitale Datenblätter"
- Generieren von „Cam-Cards" – Dokumente mit genauen Installations- und Konfigurationsanweisungen, Abbildung von Sichtfeld, Gerätedaten usw. für jede Kamera

Datenschutzrechtliche Vorteile

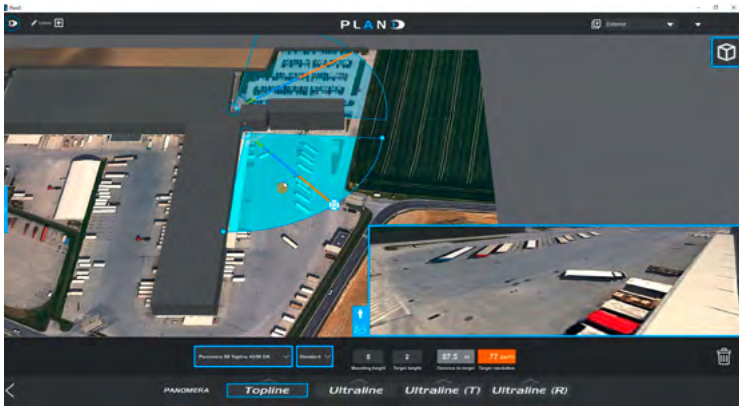
- Anfängliche Datenschutzbedenken per 3D-Planung ausräumen (siehe Praxistipp im Datenschutz-Kap. 5.1)
- Einbindung aller Stakeholder, wie z. B. Datenschutzbeauftragter, Betriebsrat, Datenschutz-Aufsichtsbehörde
- Abklärung VOR Projektstart mit dem Datenschutz und dem Betriebsrat: Was sieht welche Kamera? Mit welcher Bildqualität? Welche Bildwinkel? Welche Szene? Sind Persönlichkeitsrechte von Dritten oder Mitarbeitern betroffen? Entstehen personenbezogene Daten?
- Visualisierung der Datenschutz-Funktionen im digitalen Zwilling (z. B. Private Zonen, Verpixelung)

PRAXISTIPP — DAS RICHTIGE PLANUNGSTOOL

3D-PLANUNG MIT EXAKTER ANGABE DER PIXELDICHTE – DIGITALER ZWILLING

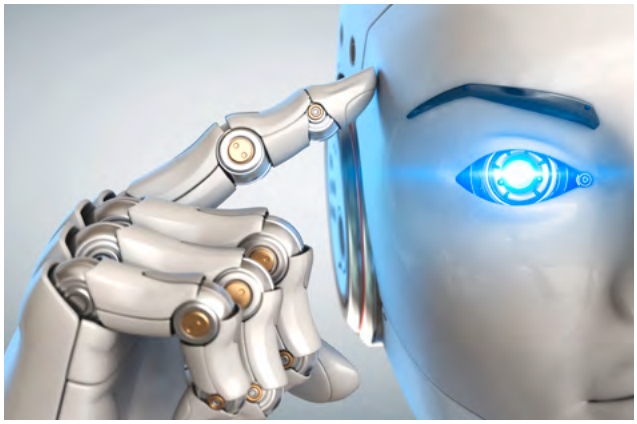
Die meisten Hersteller bieten heute eine mehr oder weniger umfangreiche Planung in 3D an. Diese ist aber nur wirklich hilfreich, wenn sie die gesamte Umgebung als „digitaler Zwilling“ möglichst exakt simulieren und so die genaue Pixeldichte-Abdeckung sowie die Kameraansichten für sämtliche Bereiche anzeigen kann. So ist eine Planung möglich, die sowohl die Zweckerfüllung und den effizienten Betrieb als auch die maximale Kosteneffizienz sicherstellt.

Einen Eindruck einer modernen und professionellen 3D-Planung am Beispiel KRITIS-Sektor „Transport und Verkehr – Hafen“ erhalten Sie hier.



Beispiel 3D-Planungstool zur eigenen Nutzung: Professionelle 3D-Planungen intuitiv und einfach selber erstellen.

7.7 KÜNSTLICHE INTELLIGENZ: ZWISCHEN HYPE UND SMARTEM ASSISTENZSYSTEM



KI – ZWISCHEN HYPE UND ASSISTENZSYSTEM
Ähnlich wie beim autonomen Fahren finden sich hohe Erwartungen und manche Versprechungen bezüglich der Künstlichen Intelligenz (KI) auch im Bereich der Videosicherheitstechnik: Hier reichen die Vorstellungen vom Erkennen auffälliger Verhaltensweisen wie etwa von Angriffen auf Personen („unusual behaviour"-Erkennung) über das Identifizieren einzelner Gesichter in Menschenmassen bis zum Wunsch nach dem automatischen Detektieren des berühmten „Bombenkoffers" in Kritischen Infrastrukturen.

KI kann dem Menschen assistieren
In der Realität sieht es heute so aus, dass immer mehr Analysetechniken auf den Markt kommen, die sich durchaus als „Assistenzsysteme" eignen und dem Sicherheitspersonal wie auch den Ermittlern viel Arbeit abnehmen können. Dazu gehören beispielsweise Systeme zur Personenzählung, zur Suche nach auffälligen Merkmalen wie bestimmten Kleidungsstücken, zum Erkennen und Klassifizieren von Objekten etwa in KRITIS-Bereichen, die nicht betreten oder befahren werden dürfen, und einiges mehr.

KI-basierte Videotechnik für KRITIS
Die Videotechnik und v. a. die KI-basierte Videoanalyse entwickeln sich rasant weiter: Neben der optischen Beweissicherung bieten sich Anwendern immer mehr Möglichkeiten zur automatischen oder teilautomatisierten Analyse von Bilddaten mittels Videoanalyse und KI. Hier den Überblick zu behalten, ist nicht immer einfach, zumal in hoher Frequenz neue Lösungen auf den Markt drängen und viele Systeme sich noch im Forschungs- und Experimentierstadium befinden.

In der Videoüberwachung werden Videoanalysen immer wichtiger. Dies kann live oder auch im Nachhinein sein. Klassischerweise wurde dies früher bzw. heute noch von Menschen vorgenommen (einem Mitarbeiter in einer Überwachungszentrale). Wenn ein Mensch ein Video analysiert, dann kann er das nur mit normaler Geschwindigkeit machen (nicht z. B. im Schnellvorlauf). Auch mehrere Videos parallel zu analysieren erscheint sehr schwierig. Soll nun eine Videoüberwachung mit dutzenden, hunderten oder tausenden Überwachungskameras analysiert werden, so ist man auf die Hilfe von Videoanalyse-Software angewiesen. In der Videoanalyse gibt es heute Software, die auf Videos die unterschiedlichsten Ereignisse erkennen kann. Und dabei wird zusehends mehr Künstliche Intelligenz eingesetzt.

Kameras sind prinzipiell als „optische Sensoren" hervorragend zur Erfassung von Analysedaten geeignet: Es gibt kaum bessere Wege, mit relativ geringem Aufwand verschiedenste Arten von Daten aus komplexen Zusammenhängen zu extrahieren, als ein Videobild sie eröffnet.

Die Möglichkeiten der Videoanalyse mit KI-Unterstützung sind vielfältig: „Crowd-Analysen" zum Zählen von Personen oder Objekten, „Ship Detection" für Häfen und Raffinerien mit Tankschiffhafen, „Smart Search" zum Auffinden von Personen oder Objekten basierend auf bestimmten Merkmalen und diverse „Intrusion Detection"-Systeme etwa zur Absicherung von „Sterile Areas" in Kritischen Infrastrukturen oder am Perimeter von Kritischen Infrastrukturen uvm.

Praxisbeispiel: Reale, funktionierende KI-basierte Videoanalyse für KRITIS-Perimeterschutz

KRITIS-Sektor „Transport und Verkehr – Straßen-und Schienenverkehr – Binnenschifffahrt – Logistik“

Für weitere Informationen sehen Sie sich unsere Video-Casestudy „Container Terminal Herne: Gefährliche Situationen nachvollziehen & Diebstahlschutz gewährleisten“ an.

Perimeterschutz mit KI-basierter Objekterkennung branchenneutral und allgemein erklärt: Hier im Video.

KI bedeutet mehr als Technik

Bei vielen Innovationen wird aber oft außer Acht gelassen, dass neue Techniken fast immer auch eine gesellschaftliche Diskussion und Änderungen von ganz konkreten Rahmenbedingungen erfordern, bevor sie flächendeckend zum Einsatz kommen können. Das immer noch ungeklärte Dilemma beim Unfallverhalten eines autonom fahrenden Autos ist da ein fast schon klassisches Beispiel. Beim Einsatz von KI in der Videosicherheitstechnik gibt es ähnlich ungeklärte Fragen:

- Wie viel an Entscheidungsfreiheit erhält ein System?
- Welche Qualitätskriterien werden z. B. bei der Objekterkennung angesetzt?
- Wer ist zur Verantwortung zu ziehen, wenn KI – gerade im Bereich der öffentlichen Sicherheit – die in sie gesetzten Erwartungen bei einem Vorfall nicht erfüllt?
- Welche Reaktionszeiten werden definiert? Bis wann müssen Einsatzkräfte bei einem „KI-Alarm“ vor Ort sein?
- Stehen genügend Kräfte für die potenziellen neuen Einsatz- und Rechercheoptionen zur Verfügung?
- Entsprechen die Überlegungen zum Einsatz von KI den Einsatzabläufen bzw. können diese beispielsweise bei der Klassifizierung von Objekten angepasst werden?
- Wurden Aspekte des „Austricksens“ von KI durch Täter, wie etwa bei der Objekterkennung, ausreichend in Betracht gezogen?
- Wie ist das Zusammenspiel aus Bild- und damit Datenqualität und Analyse?

- Wie erfolgt der Umgang und die öffentliche Diskussion bei „False Positives“, also der „automatischen Verdächtigung“ Unschuldiger?
- Treten die eigentlichen Überwachungsziele durch eventuell zu große Technikbegeisterung in den Hintergrund?
- Sind Lösungen, die in der Öffentlichkeit/ Presse vorgestellt und diskutiert werden, echte Lösungen, die es bereits gibt? Oder handelt es sich um Forschungsvorhaben mit ungewissem Ausgang?
- Wer definiert oder kontrolliert ethische Standards von KI-Anwendungen?

Jeder Anwendungsfall ist anders
Gerade deshalb sind allgemeingültige Aussagen zum Thema KI & Videotechnik schwierig zu treffen. Generell sollten Entscheider jeden Anwendungsfall genau prüfen. Eine gute Suchfunktion in der Videomanagementsoftware (VMS) mit Vorschaubildern und der Möglichkeit des Vor- und Zurückspulens mag unter Umständen nützlicher sein als eine KI-basierte Personenerkennung. Letztere hilft wenig, wenn das verknüpfte VMS die Suche nach den relevanten Sequenzen und deren Handhabung äußerst umständlich macht. Eine Kombination beider kann – je nach Anwendungsszenario – den Systembedienern dagegen große Vorteile bringen.

Ausblick KI-Verordnung der EU: „Vertrauenswürdige Künstliche Intelligenz“
Im Zusammenhang mit neuen Technologien wie KI gilt zumeist folgende Feststellung:
Nicht alles, was durch Technik technisch machbar ist, hier in diesem Fall durch Videoanalytik und Künstliche Intelligenz, ist bis dato weder datenschutz- und datensicherheitsrechtlich noch normativ rechtlich hinreichend und einheitlich definiert und geregelt, ganz zu schweigen von der ethischen Vertretbarkeit.

Das Problem:
Bei KI in der Videosicherheitstechnik fehlen bis dato noch verbindliche Industriestandards, rechtliche Normen und auch ethische Standards.

Weltweit erster Rechtsrahmen für KI vorgelegt
Den ersten Schritt, dieses Dilemma der fehlenden technischen und rechtlichen Normierung von KI in der Europäischen Union zu beheben, hat die EU-Kommission im Jahre 2021 mit ihrem Vorschlag für eine „vertrauenswürdige Künstliche Intelligenz“ („EU-KI-VERORDNUNGSENTWURF“ / AI ACT) gemacht.

Unserer Einschätzung nach wird es analog dem Beispiel „DSGVO – Datenschutzgrundverordnung – Verordnung für den Bereich Datenschutz“ in näherer Zukunft auch eine Art „KIGVO – KI-Grundverordnung – Verordnung für den Bereich Künstliche Intelligenz“ auf europäischer Ebene geben.

Regulierung von KI und Regulierung von KI in KRITIS
Der aktuelle EU-Kommissionsvorschlag für eine „vertrauenswürdige Künstliche Intelligenz“ enthält auch explizite und kodifizierte Regelungen für KI in Kritischen Infrastrukturen.

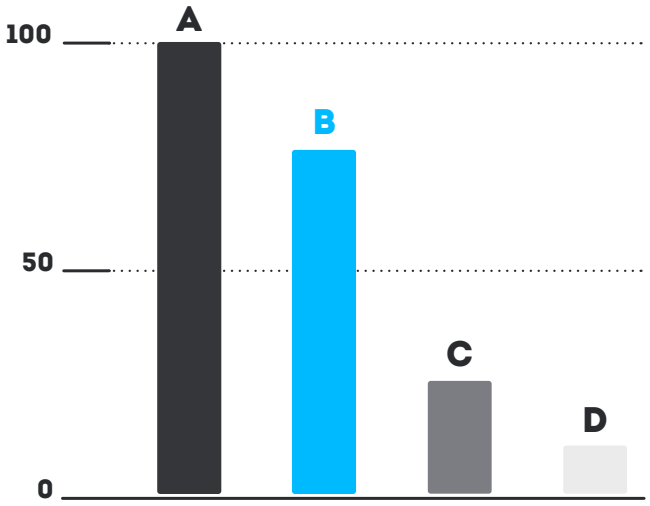
KI-Systeme, die die Sicherheit, die Lebensgrundlagen und die Rechte der Menschen bedrohen, werden verboten. Für KI-Systeme mit hohem Risiko sollen strenge Vorgaben gelten, die erfüllt sein müssen, bevor sie auf den Markt gebracht werden.

Risikobasiertes KI-Konzept mit 4 Risikoklassen

Die EU will KI-Anwendungen in vier verschiedene Risikoklassen einteilen und entsprechend reglementieren. Nach dem Motto: „Je höher das Risiko einer spezifischen Nutzungsart der KI, desto strenger die Regeln." Die neuen Vorschriften werden auf einer zukunftssicheren Definition der KI beruhen und in allen Mitgliedstaaten direkt und in gleicher Weise Anwendung finden. Sie folgen einem risikobasierten Ansatz:

- **Risikoklasse A (Unannehmbares Risiko): KI verboten**
  Unannehmbares Risiko: KI-Systeme, die als klare Bedrohung für die Sicherheit, die Lebensgrundlagen und die Rechte der Menschen gelten, werden verboten.

  Dazu gehören KI-Systeme oder -Anwendungen, die menschliches Verhalten manipulieren, um den freien Willen der Nutzer zu umgehen (z. B. Spielzeug mit Sprachassistent, das Minderjährige zu gefährlichem Verhalten ermuntert), sowie Systeme, die den Behörden eine Bewertung des sozialen Verhaltens (Social Scoring) ermöglichen.



Die vier Risikoklassen für vertrauenswürdige KI – die KRITIS-Risikoklasse in blau.

- **Risikoklasse C (Geringes Risiko): KI erlaubt, mit besonderen Transparenzverpflichtungen**
  Geringes Risiko, d. h. KI-Systeme, für die besondere Transparenzverpflichtungen gelten: Beim Umgang mit KI-Systemen wie Chatbots sollte den Nutzern bewusst sein, dass sie es mit einer Maschine zu tun haben, damit sie in voller Kenntnis der Sachlage entscheiden können, ob sie die Anwendung weiter nutzen wollen oder nicht.

- **Risikoklasse D (Minimales Risiko): KI erlaubt, freie Nutzung**
  Minimales Risiko: Der Vorschlag soll die freie Nutzung von Anwendungen wie KI-gestützten Videospielen oder Spamfiltern ermöglichen. Die große Mehrheit der KI-Systeme fällt in diese Kategorie. Der Verordnungsentwurf soll hier nicht eingreifen, denn diese KI-Systeme stellen nur ein minimales oder kein Risiko für die Bürgerrechte oder die Sicherheit dar.

- **Risikoklasse B (Hohes Risiko): KI erlaubt, unter strengen Vorgaben**

  Die „KRITIS-Risikoklasse"
  Hohes Risiko:
  KI-Systeme, bei denen ein hohes Risiko besteht, wenn KI-Technik in folgenden Bereichen eingesetzt wird:

  - Kritische Infrastrukturen (z. B. im Transport & Verkehr), in denen das Leben und die Gesundheit der Bürger gefährdet werden könnten
  - Sicherheitskomponenten von Produkten (z. B. eine KI-Anwendung für die roboterassistierte Chirurgie, Gesundheitswesen)
  - Strafverfolgung, die in die Grundrechte der Menschen eingreifen könnte (Staat & Verwaltung, z. B. Bewertung der Verlässlichkeit von Beweismitteln)

- Migration, Asyl und Grenzkontrolle (Staat & Verwaltung, z. B. Überprüfung der Echtheit von Reisedokumenten)

Für KI-Systeme mit hohem Risiko werden strenge Vorgaben gelten, die erfüllt sein müssen, bevor sie auf den Markt gebracht werden dürfen:

Vorgaben für KRITIS-KI-Anwendungen:

- Angemessene Risikobewertungs- und Risikominderungssysteme
- Protokollierung der Vorgänge, um die Rückverfolgbarkeit von Ergebnissen zu ermöglichen
- ausführliche Dokumentation mit allen erforderlichen Informationen über das System und seinen Zweck, damit die Behörden seine Konformität beurteilen können
- klare und angemessene Informationen für die Nutzer
- angemessene menschliche Aufsicht zur Minimierung der Risiken
- Hohes Maß an Robustheit, IT- und Cybersicherheit und Genauigkeit
- Hohe Qualität der Datensätze, die in das System eingespeist werden, um Risiken und diskriminierende Ergebnisse so gering wie möglich zu halten

Anmerkung zu:
Hohes Maß an Robustheit, IT- und Cybersicherheit und Genauigkeit.
Wenn ein paar kaum sichtbare Klebestreifen ein Stoppschild für die Fahrzeugkamera in ein 80 km/h-Schild verwandeln können, müssen Lösungen dafür gefunden werden. Noch mehr gilt dies für den Fall von tatsächlichen Cyberattacken auf KI-Systeme mit entsprechender, vielleicht gar nicht erkennbarer Manipulation des KI-Systems selbst. Wir als Hersteller unterstützen die Forderung nach IT- und Cybersecurity-Resilienz (siehe auch Kap. 5.6) und empfehlen jedem KRITIS-Betreiber, unabhängig jeglicher regulatorischen Pflicht, im Eigeninteresse seine KI-Anbieter nach solchen Kriterien zu bewerten.

Praxistipp:
Eine hohe Qualität der Datensätze, die in das System eingespeist werden, hält Risiken und diskriminierende Ergebnisse so gering wie möglich.

PRAXISTIPP

QUALITÄT VON BILD- UND TRAININGSDATEN FÜR KI

„QUALITY IN, QUALITY OUT" – FÜR DIE ZUKUNFT GERÜSTET SEIN

QUALITY IN 1: BILDQUALITÄT

Die Analysetechnik entwickelt sich schnell. Die Lebens- bzw. Abschreibungsdauer bei Videotechnikkomponenten – allen voran Kameras, die ja häufig aufwendig befestigt werden – liegt aber bei mehreren Jahren. Es empfiehlt sich daher, bei der Auswahl der Kamerasysteme auf eine möglichst hohe, durchgehende Bildqualität über den gesamten Objektraum hinweg zu achten. Denn die Qualität der Analyseergebnisse kann immer nur so gut sein, wie die Qualität der Eingangsdaten (hier: die Bildqualität).

Synthetische Daten als Trainingsdaten.

QUALITY IN 2: TRAININGSDATENQUALITÄT

Bei der KI-Analyse ist neben der Bildqualität zudem auch die Qualität und Quantität (repräsentativer Querschnitt der Grundgesamtheit) der KI-Trainingsdaten entscheidend. Nachfolgend zu sehen: Computergenerierte 3D-Figuren, mit denen Videoanalyse-Systeme angelernt werden können.

Diese vier Fälle determinieren die Qualität der KI-Ergebnisse (Output).

QUALITY OUT: KI-ERGEBNISSE

Black Box-Problematik: Die Systeme können einerseits durch Verzerrungen (biases) in Trainingsdaten oder in ihren Modellen bestehende gesellschaftliche Diskriminierungsmuster übernehmen oder verstärken, können aber andererseits auch darüber hinaus – also selbst wenn der Einfluss dieser Verzerrungen in Daten und Modell minimiert werden könnte – ungerechtfertigte Ungleichbehandlungen hervorrufen und verfestigen.

Nur die Kombination aus hochwertigen KI-Trainingsdaten und hochauflösenden Videobildern liefert Analyseergebnisse, die vertrauenswürdig und frei von Diskriminierung sind.

„Formel“ für eine vertrauenswürdige KI

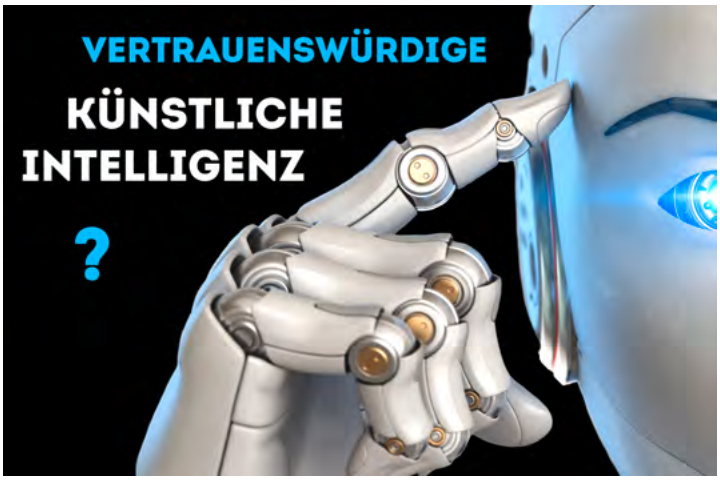
1) Hoher Datenschutz nach DSGVO

2) Hohe Datensicherheit/Cybersicherheit

3) Hohe Datenqualität zur Vermeidung von diskriminierenden KI-Ergebnissen
   a) Trainingsdaten
   b) Echtdaten (Bild/Videodaten)

4) Einhaltung Werte, Grundrechte, ethische Standards der EU

5) Einhaltung angrenzender EU-Gesetze (u. a. Haftungsrecht, Strafrecht, Urheberrecht)



PRAXISTIPP — NÜTZLICHE UNTERLAGEN ZU KI & CO

WEITERE INFORMATIONEN ZUM THEMA

- Positionspapier der DSK zur biometrischen Analyse
- Datenschutzrechtliche Anforderungen an Künstliche Intelligenz (Hambacher Erklärung KI)
- Praxisleitfaden: „Videoanalyse: Wie gut ist eine Künstliche Intelligenz?“
- Expertentipp: „Videotechnik und KI“
- EU Kommissionsvorschlag für eine Vertrauenswürdige Künstliche Intelligenz

7.8 WIRTSCHAFTLICHKEIT: „WAS KOSTET BEI IHNEN DENN SO EINE KAMERA?“

Hersteller oder Errichter sehen sich in Beratungsgesprächen oder Ausschreibungen leider immer noch sehr häufig mit der Frage nach den „Kosten pro Kamera“ konfrontiert. Bei modernen Videosicherheitsanlagen handelt es sich aber immer um Lösungen aus verschiedenen Komponenten (Kameras, Software, Aufzeichnungssysteme, Dienstleistungen usw.), mit teilweise sehr gravierenden Unterschieden bei Bedienereffizienz, Infrastrukturkosten oder auch Aufwand bei der Bereitstellung und Installation. Zudem sind die Unterschiede zwischen den verfügbaren Technologien häufig wesentlich größer als man glauben möchte.

7.9 NICHT DAS BILLIGSTE, SONDERN DAS WIRTSCHAFTLICHSTE ANGEBOT

Es empfiehlt sich daher immer, eine genaue Betrachtung der Gesamtkosten („Total Cost of Ownership“) durchzuführen, die alle Kostenaspekte einer Lösung berücksichtigt, und zwar von der Planung bis hin zum laufenden Betrieb. Schließlich gilt sowohl bei öffentlichen Ausschreibungen als auch bei privatwirtschaftlichen „Ausschreibungen“ das Prinzip des wirtschaftlichsten Angebots.

PRAXISTIPP | **VERGABEVERFAHREN**

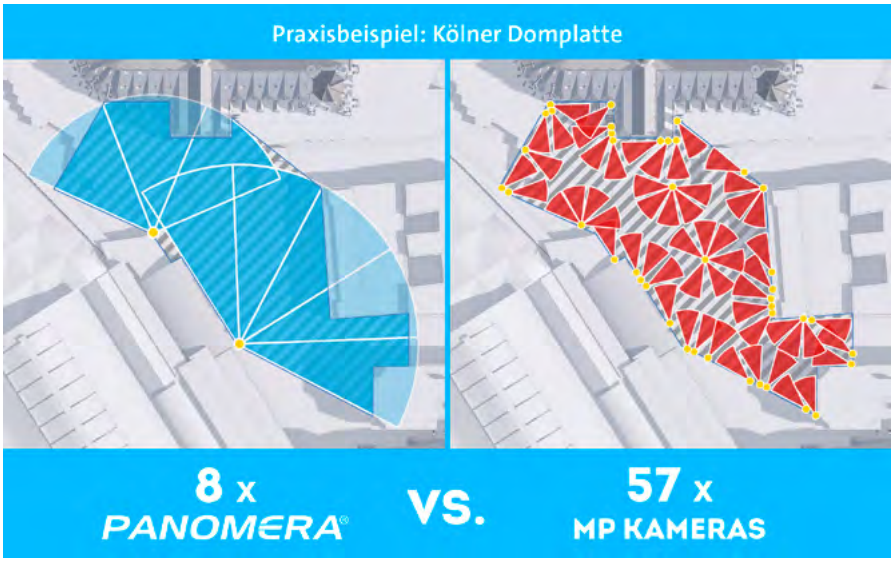
DAS WIRTSCHAFTLICHSTE ANGEBOT

Die Publikation „Das wirtschaftlichste Angebot – Hinweise zur richtigen Gestaltung und Wertung im Vergabeverfahren“ des Bayerischen Staatsministeriums für Wirtschaft, Landesentwicklung und Energie gibt beispielhaft gute Informationen und Hinweise.

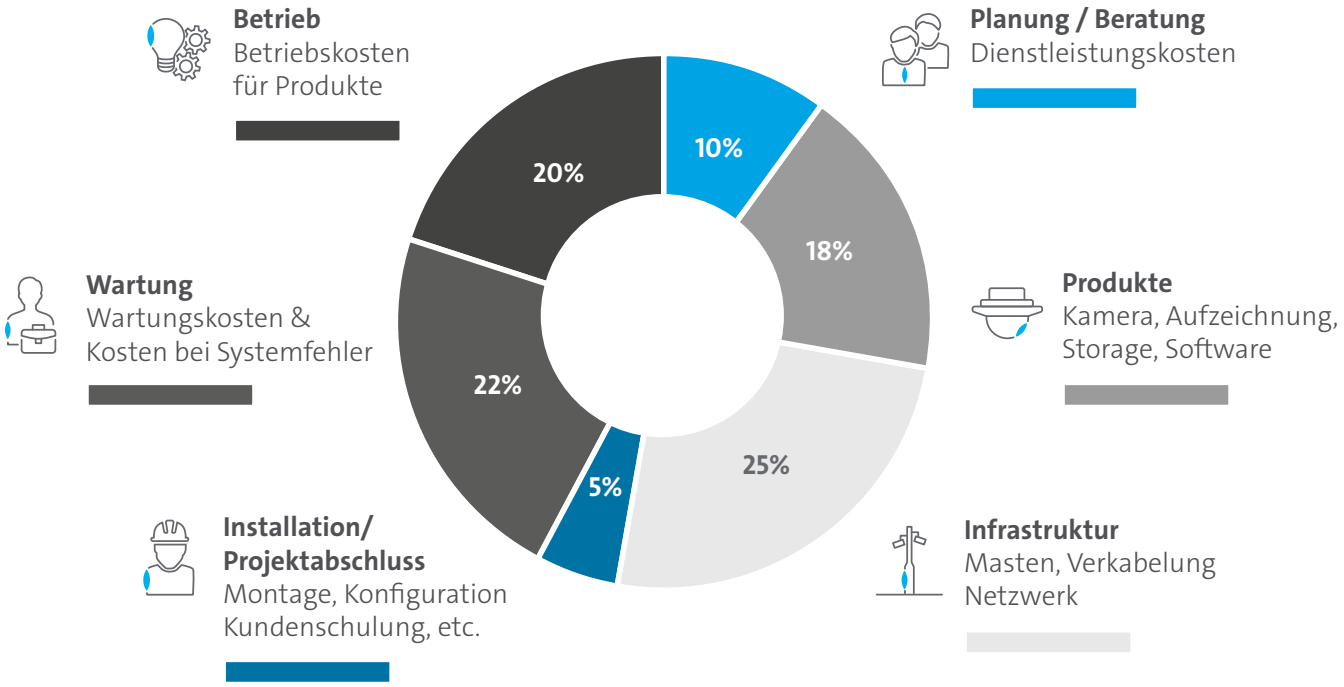
Im Einzelnen werden die Gesamtkosten beeinflusst durch:

- Die Beratung: Wie zeitaufwendig? Kostenlos oder bereits mit Kosten verbunden?
- Die genauen Anforderungen: Wie hoch soll die Auflösungsdichte und Bildqualität sein?
- Die Anzahl der Kameras: Wie viele Systeme welcher Art werden für wie viele Quadratmeter Fläche benötigt?
- Die Planung: Wie zeitaufwendig ist die Planung, welche digitalen Systeme kommen dabei zum Einsatz? Dies hat direkte Auswirkungen auf die Geschwindigkeit der Umsetzung und auch auf die Flexibilität.
- Die Kosten für Infrastruktur, inklusive Arbeitskosten: Werden Masten, Tiefbau, Kabel, Netzwerktechnik benötigt?
- Die Kosten für die Installation: Hier spielt die Anzahl der insgesamt benötigten Kameras naturgemäß eine Schlüsselrolle.
- Die Montagesysteme: Gibt es Systeme, die die Installation besonders teuer oder besonders günstig machen?
- Die Konfigurationsunterlagen: Inwiefern können Daten aus der Planung direkt bei der Installation vor Ort genutzt werden? Manche Hersteller können direkt aus der Planung heraus Installationsunterlagen generieren.

- Die Kosten für die technischen Komponenten selbst: Wie viel kosten Kameras, Aufzeichnungssysteme oder Software-Komponenten?
- Die Kosten für die laufende Wartung: Wie sieht es mit Gewährleistung, Garantie oder „all-inclusive“-Supportverträgen aus?
- Die Kosten für den Betrieb: Wie hoch sind die Lohnkosten für die Bediener? Wie viele Bediener werden bei welcher Lösung benötigt?
- Die Kosten für „unproduktives Handling“: Wie bedienerfreundlich sind die Lösungen? Wie viele Kamerabilder muss jeder Bediener im Auge behalten (meist sind max. 6-8 Bilder pro Operator zumutbar)? Im Umkehrschluss: Wie viele Personenstunden erfordert die jeweilige Lösung bei der aktiven Videobeobachtung?



Je nach eingesetzter Technik kann die Anzahl der benötigen Kamerasysteme stark variieren – mit großen Auswirkungen auf Infrastruktur-, Betriebs- und Wartungskosten. (Beispiel: Kölner Domplatte)



Beim Einsatz von Videotechnologie gibt es weitaus mehr Kostenfaktoren als die reinen Kosten für die technischen Videokomponenten Kameras, Aufzeichnung und Software.

7.10 AUSSCHREIBUNGEN: GETRENNTE LOSE GEMEINSAM BETRACHTEN

In vielen Ausschreibungen werden die Lose für die Videoanlage und die Lose für die dafür nötigen Bau- und Infrastrukturmaßnahmen getrennt ausgeschrieben. Dies kann unter Umständen zu einer deutlichen Verzerrung der Gesamtkosten führen, z. B. wenn Kameras in der Anschaffung günstiger, aber die dafür benötigten Infrastruktur- und Installationskosten aber wesentlich höher als bei einem Vergleichsangebot sind.

Weitere hilfreiche Praxis- und Beratungstipps für den Kontext von „Öffentliche Ausschreibungen“:

- Thema „Leistungsbestimmungsrecht“, Publikation „Das wirtschaftlichste Angebot“, Seite 4-5:

  „Bei der Bestimmung des Beschaffungsbedarfs hat der öffentliche Auftraggeber grundsätzlich ein Leistungsbestimmungsrecht“ nach § 7 VOB/A.

- Thema „Lose“: Publikation „Das wirtschaftlichste Angebot“, Seite 5:

  „Eine Gesamtvergabe ist hingegen (nur) dann zulässig, wenn wirtschaftliche oder technische Gründe dies erfordern“.

- Thema „Arten der Vergabe“:

  - VOB/A (Deutsches Vergaberecht): Bitte prüfen Sie bei Ihrem KRITIS-Projekt die einschlägigen Paragrafen § 3, § 3a, insbesondere § 3a Absatz 3.
  - VOB/A - EU (EU-Vergaberecht): Bitte prüfen Sie bei Ihrem KRITIS-Projekt die einschlägigen Paragrafen § 3, § 3a, insbesondere § 3a Absatz (3) Nr. 3b und 3c.
  - Analoge Paragrafen bei der Vergabe von Dienst- und Lieferaufträgen (VOL/VgV).

8 DER RICHTIGE PARTNER

Neben der Entscheidung für den richtigen „Technologie-Mix“ ist die Wahl des richtigen Installationspartners (im Videotechnik-Jargon meist „Facherrichter“) ebenso wichtig. Viele KRITIS-Betreiber entscheiden sich bei größeren Projekten für einen Partner, der als Generalunternehmer fungiert und sich von der Beratung über die Planung und Umsetzung auch um den laufenden Betrieb und die Wartung der Systeme kümmert.

Bei der Auswahl des richtigen KRITIS-Partners können folgende Überlegungen helfen:

- Wie erfahren sind die Projektleiter und Mitarbeiter des Unternehmens im Bereich Sicherheit von KRITIS?
- Liegen Erfahrungen mit Projekten unterschiedlicher Größen vor und sind diese nachweisbar?
- Liegen Referenzschreiben von KRITIS-Entscheidern vor? Fragen Sie gegebenenfalls nach.
- Ist der Anbieter flexibel, was das Anbieten bzw. Auslagern von Dienstleistungen betrifft?
- Bekommt der Anbieter optional auch Unterstützung durch Hersteller-Experten?
- Liegen Lücken im Portfolio des Errichters vor, die mit anderen Dienstleistern gefüllt werden müssen? Oder gibt es auf Wunsch „alles aus einer Hand“?
- Wie erfolgt die Planung? 2D, 3D, Pixeldichte-Simulation und BIM usw.?
- Gibt es Erfahrungen in puncto Videotechnik und Datenschutz?
- Gibt es Erfahrungen beim Umgang mit beteiligten Behörden und Institutionen?
- Wie läuft die Koordination der Gewerke (Tiefbau usw.) ab? Ist dies über den Errichter möglich?
- Kann der Facherrichter alle gewünschten Betreiber- und Wartungsaufgaben übernehmen?

9 FRAGENKATALOG ZUR EIGENEN VORBEREITUNG

Im letzten Kapitel haben wir die wichtigsten Punkte aus diesem Dokument für Sie zu einem Fragenkatalog zusammengefasst.

Sind Sie ... (?)

- KRITIS-Projektverantwortlicher
- Investor / Geldgeber / Gesamtentscheider
- Einkäufer / Procurement
- Verantwortlicher Sicherheit oder Corporate Sicherheit
- IT-Stakeholder (Inhouse-IT, CIO, externes Systemhaus)
- Datenschutz-Stakeholder (Datenschutzbeauftragter, Datenschutzaufsicht, Datenschutzinitiative)
- Datensicherheits-Stakeholder (wie z. B. CISO)
- Compliance- und Legal-Verantwortlicher
- Ethik-Verantwortlicher
- Nachhaltigkeits-Verantwortlicher
- Risiko- und Krisenmanager
- Compliance-, Ethik-, oder Nachhaltigkeits-Stakeholder
- Vertreter Aufsichtsbehörde
- Planer / Planungsbüro
- Fach- und Sicherheitserrichter
- Politischer Entscheidungsträger
- Interessierter Vertreter der Medien / Presse
- sonst am Entscheidungs- oder Umsetzungsprozess beteiligt
- generell am Thema interessiert

Dann finden Sie im Folgenden eine Auswahl an Fragen, die Sie als Entscheider oder als an der Entscheidung Beteiligter bei der Initialisierung, Planung und Durchführung Ihrer Videosicherheitsanlage begleiten können.

Dilemma des Entscheiders: Marktintransparenz und Technikvielfalt
Der Markt für Videosicherheitstechnik befindet sich im stetigen Wandel. Heute stehen Mehrwerte über die reine Bilderfassung und das reine „optische Sehen" hinaus im Fokus der Branche. Dazu gehören etwa die auf Computer Vision basierenden Analysetechniken, mit denen Anwender sowohl Sicherheitsthemen als auch Geschäftsprozesse verschiedenster Branchen optimieren können. Videotechnik entwickelt sich immer mehr vom Kostenfaktor zum „Business Enabler", also zum Wegbereiter einer erfolgreichen Geschäftstätigkeit und neuer Geschäftsfelder.

Neben dem stetigen Wandel machen es die Funktionsvielfalt und das Leistungsvermögen von technischen Investitionsgütern wie z. B. Videosystemen dem verantwortlichen Entscheider oft sehr schwierig und fast unmöglich, einen vergleichenden Marktüberblick zu behalten und fundierte Kaufentscheidungen treffen zu können.

Zweites Dilemma des Entscheiders: Entscheidung naht – „was tun?"
Wenn dann die Entscheidung für ein neues System bzw. eine Ersatzinvestition ansteht, frägt sich so mancher Verantwortliche zu Recht:

- „Was tun?"
- Nach welchen Kriterien entscheiden?
- Das Billigste nehmen ist eine / keine Option?
- Nach Technik und technischer Leistung?
- Nach wertmäßigen Aspekten wie Kosten und Ertrag/Return?
- Nach beidem? Technik und Geld?
- Nach Preis? Nach gutem Preis-/Leistungsverhältnis?
- Nach weichen Faktoren wie Herstellerherkunft (Made in Germany oder Made in Europe), nach Vertrauen in Anbieter oder deren Mitarbeiter, nach Erfahrung, nach zukunftssicheren Technologieansätzen, nach Referenzen, nach Datenschutz und Datensicherheit, Nachhaltigkeit, Ethik etc.?

Kleiner Exkurs zu weichen Entscheidungs-Faktoren:
Wie die leidvolle Corona-Pandemie und der Krieg zeigen und lehren:

- Aus weichen Kauffaktoren können schnell harte, monetäre Faktoren werden
- In einer TCO-Betrachtung würden diese als Wagnis- und Risikokosten bezeichnet und angesetzt werden (können)
- Bitte selber entscheiden, ob diese Entscheidungsfaktoren bei Ihnen Berücksichtigung finden sollen

Beispiel 1: Supply Chain (Corona / Krieg)

- Zuverlässige Lieferketten wichtig, gewährleistet?
- Welche Auswirkungen hätten instabile Lieferketten (monetär und/oder Image, Produktion, Auslieferung, Kundenbeziehung etc.)?
- Redundante Lieferkette (Lieferanten / Menge) vorhanden?
- Made in Germany bzw. Made in Heimatland / eigenem Land wichtig ? Vertrauliches Supply-Ökosystem?
- Vermeidung Supply-Verwundbarkeit durch multilaterale, undurchsichtige Herstellerabhängigkeiten, Hersteller-heterogenität, politische Einflussnahmen

Beispiel 2: Datenschutz- und Datensicherheit (DSGVO-Einführung 2018)

- Unsichere Videotechnik als potentielles, zusätzliches „Cybersecurity-Einfallstor“
- Seit DSGVO-Einführung empfindliche Bußgelder bei Verletzung Datenschutz und Datensicherheit
- Kein Datenschutz ohne Datensicherheit
- Neben Bußgeldern möglicher Imageverlust, Vertrauensverlust, Kundenbeziehungsverlust (neben einem möglichem kritischen Geschäftsdatenverlust / Datenmanipulation)
- Business Continuity gefährdet durch Ausfallzeiten und Wiederherstellungszeiten
- Vermeidung von IT-Verwundbarkeit durch multilaterale, undurchsichtige Hersteller-abhängigkeiten, Herstellerheterogenität, politische Einflussnahmen in Herstellerländern
- Videotechnik neben Sicherheitsdaten zunehmend Generierung von Prozess- und Geschäftsdaten per Videoanalyse und KI (Zähldaten, Messdaten, Objektklassifizierungsdaten, „Bewegungsdaten“ etc.)
- Videotechnik als IoT zunehmend Teil der Industrie 4.0
- IT-Sicherheit / OT-Sicherheit in Produktions- und Automationssystemen – die informationstechnische Vernetzung macht produktionstechnische Anlagen und die dort hergestellten Produkte verstärkt zu einem attraktiven Ziel für digitale Angriffe auf Industrieunternehmen.
- Welche Auswirkungen hätten unsichere Systeme (monetär und/oder Image, Produktion, Auslieferung, Kundenbeziehung, etc.)?
- Datenschutz und Datensicherheit Made in Europa / DSGVO – ein Paradigmenwechsel ist zu beobachten, eine neue Unternehmenskultur, die Cyber-Resilienz und EU-Datenschutz wertschätzt, respektiert und die Integrität und Verfügbarkeit von Diensten und Daten als Differenzierungsmerkmal in der Digitalwirtschaft versteht. Auch für Sie wichtig?

9.1 POLITISCHE, ORGANISATORISCHE UND GESETZLICHE RAHMENBEDINGUNGEN

- Sind alle **Beteiligten** am Projekt bekannt?
- Wie ist das unternehmenspolitische Stimmungsbild und der Aufklärungsstand der Beteiligten über die heute umsetzbaren **Datenschutzstandards** im Zusammenhang mit Videoüberwachung?
- Gibt es kritische Branchenverbände / Bürgerinitiativen / Parteien, bei denen sich ein **proaktiver Dialog** anbietet?
- Gibt es **besonders gefährdete** oder kriminogene **KRITIS-Bereiche**?
- Wie ist das Thema Videoüberwachung durch internationale, nationale- und (bundes-) länderspezifische **Datenschutz-Gesetze** geregelt?
- Würde die **Maßnahme** durch internationale, nationale- und länderspezifische Gesetze **bestätigt werden**?
- Sind Aufsichtsbehörden, Behörden oder andere öffentliche Stellen, die Politik oder gar die Exekutive (Ministerien) mit involviert und haben aktives Interesse bzw. **Mitbestimmungs- oder Vetorecht**?
- Würde die Maßnahme durch Datenschutzaufsichtsbehörden bzw. Cybersecurity-Aufsichtsbehörden wie z. B. dem BSI **genehmigt bzw. mitgetragen** werden?
- Bestehen **Melde-, Anzeige-, Genehmigungs- oder Nachweispflichten** gegenüber Aufsichtsbehörden (wie dem BSI), z. B. bzgl.
  - Sicherheitsstandards, Stand der Technik, Gewährleistung IT-Schutzziele
  - kritischer Komponenten, Herstellergarantieerklärungen, Drittstaatenhersteller
- Welche KRITIS-spezifischen **Gesetze und Regelungen** müssen beachtet werden (wie in Deutschland z. B. das BSIG, Kritisverordnung)?
- Gibt es noch weitere zu beachtende sektorspezifische oder spezialgesetzliche Regelungen? Gibt es zusätzliche **„Branchenspezifische Sicherheitsstandards (B3S)“** zu beachten?
- Sind die **Anforderungen an die Videoüberwachung** klar formuliert (beispielsweise Auflösungsdichte, zu beobachtende Bereiche / Flächen)? Anforderungen definiert nach DIN 62676-4?
- Gibt es ein **Meinungsbild** der Mitarbeiter oder Bürger (Umfragen usw.)?
- Sind **Datenschutzbeauftragte**, Datenschutzaufsicht und/oder **Betriebsrat** informiert und integriert?

- Warum sind die Videoüberwachung und die Videobeobachtung geeignet und erforderlich, den festgelegten Zweck zu erfüllen? **Zweckbindung und Zweckerfüllung** erfüllt und dokumentiert? (siehe Kap. 5.3)

- **Weitere Fragen zur DSGVO** und der Begründung der Videoüberwachung und Videobeobachtung finden sich auch in der Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, im DSK Kurzpapier Nr. 15 (jeweils mit Fokus auf nicht-öffentlichen Bereich) sowie beispielhaft für Baden-Württemberg (für öffentliche Stellen).

9.2 BETRIEBLICHE RAHMENBEDINGUNGEN

- **Wer entscheidet über das Videoprojekt?** Gesamtentscheider/Management und/oder Entscheider Physische Unternehmenssicherheit und/oder IT-Leitung und/oder IT- und Cybersicherheit / CISO und/oder Einkauf und/ oder x oder „Entscheidergremium“?

- Wer ist verantwortlich für die Umsetzung Videoprojekt? Gibt es sich **überschneidende Verantwortungsbereiche?** (Physische Sicherheit / IT / Cybersicherheit)?

- Gibt es evtl. gesellschaftsrechtlich verbundene Betriebe wegen optional **gemeinsamer Nutzung von Infrastruktur?** Um gemeinsame Ressourcen zu nutzen und so beispielsweise die Zahl der Planstellen für Implementierung und Betrieb gering zu halten.

- Wie viele Mitarbeitende und **Bediener** stehen für welche Videoüberwachungsaufgabe zur Verfügung?

- **Welche Bereiche** sollten überwacht werden?

- Welche Lösung bietet mir die maximale **„Bedienereffizienz“**?

9.3 INFRASTRUKTUREN & SYNERGIEN

- Gibt es **Pläne** des zu überwachenden Bereiches / der Fläche?

- Gibt es **Leitungs- und Trassenpläne** von vorhandenen Infrastrukturen wie z. B. Gas, Fernwärme, Telekommunikation usw.?

- Sind Infrastrukturen wie für die Verkabelung von **Strom und Netzwerk** bekannt / vorhanden?

- Wie erfolgt die **Netzwerkanbindung** für die Kameras?

- Wie kommt **Strom** zur geplanten Kameraposition?

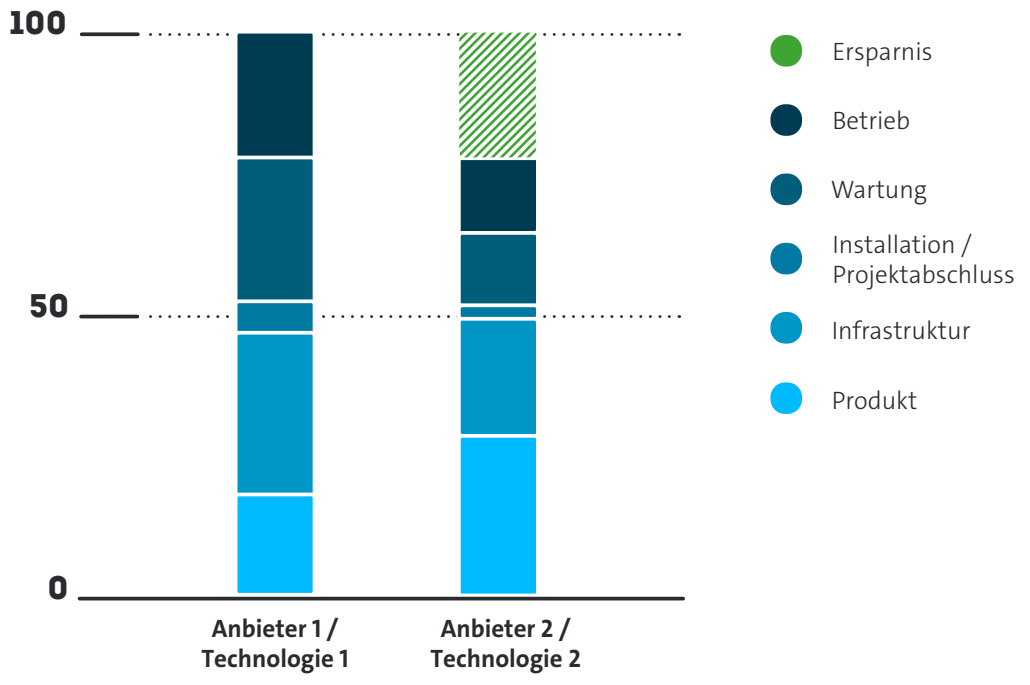
- Können **vorhandene Lichtmasten** genutzt werden?
- Müssen **neue Masten** errichtet werden?
- Gibt es eventuell **vorhandene Netzwerkressourcen** wie z. B. von gesellschaftsrechtlich-verbundenen Betrieben usw., die man mitnutzen oder gemeinsam nutzen kann? Um so beispielsweise die Zahl der Planstellen für Inbetriebnahme und den Betrieb gering zu halten?
- Welche **Einwilligungen** müssen eingeholt werden, wenn man Kameras an Gebäuden / Wänden platzieren möchte?

9.4 TECHNOLOGIEENTSCHEIDUNG & KOSTENBETRACHTUNG

- Ist die **Beratung kostenlos** oder bereits mit Kosten verbunden?
- Was sind die genauen **Anforderungen an Auflösungsdichte und Bildqualität?** Wie viele Pixel pro Meter (px/m) nach DIN EN 62676-4 werden mindestens benötigt? Wie groß ist die zu überwachende Fläche?
- Daraus ergibt sich je nach eingesetzter Technologie die Anzahl der Kameras: **Wie viele Quadratmeter Fläche** können die Kamerasysteme abdecken (Faustformel bei Multifocal-Sensorsystemen: mehr als 1.000 Quadratmeter pro System bei 250 px/m oder mehr sind möglich)?
- Wie **zeitaufwendig ist die Planung?** Welche digitalen Systeme kommen dabei zum Einsatz?
- Wie hoch sind die **Kosten für die Infrastruktur** – inklusive Arbeitskosten (Masten, Tiefbau, Kabel, Netzwerktechnik)?
- Wie hoch sind die **Kosten für die Installation?** Hier spielt die Anzahl der insgesamt benötigten Kameras eine Schlüsselrolle.
- Gibt es **Montagesysteme** u. ä., die die Installation besonders teuer oder günstig machen?
- Inwiefern können **Daten aus der Planung** direkt **bei der Installation** vor Ort genutzt werden? Manche Hersteller können direkt aus der Planung heraus Installationsunterlagen generieren.
- Wie hoch sind die **Kosten für die technischen Komponenten** (Kameras, Recorder, Software)?
- Wie verhält es sich mit den Kosten für die laufende **Wartung**?
- Auf welche Höhe belaufen sich die **Kosten für den Betrieb** – hier vor allem die Lohnkosten für die Bediener? **Wie viele Bediener** werden bei welcher Lösung benötigt?

- Wie hoch sind die Kosten für „unproduktives Handling“: Wie bedienerfreundlich sind die Lösungen, wie viele Monitore muss jeder Bediener im Auge behalten bzw. **wie viele Personenstunden erfordert welche Lösung** bei der Videobeobachtung?
- Wo und wie soll das **Deployment** der Lösung erfolgen? **On-Premise, Cloud oder hybrid?**
- Welcher Lösungsansatz ist zielführend: **Best-of-Breed** oder **Alles aus einer Hand** oder beides?
- Evtl. erstellen: **ROI-Gesamtbetrachtung**. Wie hoch ist der ROI der Lösung? Habe ich neben der Erhöhung der Sicherheit und der Vermeidung von Schadenskosten (durch Einbruch, Diebstahl, Sabotage, etc.) durch Videosicherheitstechnik evtl. auch noch einen zusätzlichen Nutzen/ Return durch Prozessverbesserungen oder Prozessautomatisierungen durch smarte Videotechnik und KI-basierte Videoanalyse?
- Evtl. erstellen: **TCO-Gesamtbetrachtung** (Total Cost of Ownership)
(Abstraktes Beispiel nachfolgend)

Gesamt-Kostenbetrachtung, über den ganzen Produktlebenszyklus per TCO-Ansatz, ein abstraktes Beispiel mit 2 Lösungsalternativen



9.5 CHECK DES HERSTELLERS BEZÜGLICH DATENSCHUTZ, DATENSICHERHEIT, ETHIK UND KI

- Wie neutral erfolgt die Prüfung der Sicherheit? Wie viel Wert legt der Hersteller auf die **neutrale Bewertung des Sicherheitsniveaus** seiner Systeme, z. B. durch unabhängige Penetrationstests während und nach der Entwicklung?

- Wie **tief ist die Wertschöpfung** in Fertigung und Entwicklung? Eine tiefe Integration erhöht meist die Qualität von Gesamtlösungen und damit den Kundennutzen. Welcher Anteil des Portfolios kommt aus dem eigenen Hause? **Wo findet die Produktion** statt?

- Lebt der Hersteller den **„Plattformgedanken“**? Bei allen Trends zu mehr „Herstellereinheitlichkeit“ ist es bei der heute vorhandenen Komplexität sehr wichtig, dass Systeme offen sind, **Standards** wie z. B. ONVIF umfassend unterstützt werden und sich Drittsysteme leicht integrieren lassen.

- Wie gut kennt der Hersteller Technik und Branche? **Jahrelange Erfahrung** in der Videosicherheitstechnik und tiefe Branchenkenntnis lassen sich nicht so leicht ersetzen. Der Hersteller sollte diese Kompetenz ausreichend darstellen können als „Vertrauenswürdiger Trusted Advisor“

- Bietet der Hersteller **Komplettlösungen oder Bausteine oder beides?**

- Gibt es eine **Dokumentation** der Maßnahmen und Funktionen **für Datensicherheit** und **Datenschutz?** Die DSGVO droht mit rigiden Maßnahmen bei Missachtung ihrer Prinzipien. Ein Hersteller sollte glaubhaft und nachvollziehbar dokumentieren, wie der Themenkomplex Datenschutz und Datensicherheit adressiert wird.

- Wendet der Hersteller als Vorlieferant von KRITIS-Betreibern bei der Entwicklung seiner Produkte die in der **DSGVO geforderten Prinzipien „Security by Design“** und „Privacy by Design“ an?

- Kommt der **Hersteller aus Drittstaaten?** Wird der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen, eines Drittstaates kontrolliert? Oder besteht im Krisenfall die Gefahr eines „staatlich verordneten Durchgriffsrechts“ auf den Hersteller?

- Wie sieht die **Wertschöpfungskette des Herstellers** aus und wo findet diese statt? In Deutschland oder Europa oder in Drittstaaten? Wie sieht es mit der generellen Lieferverbindlichkeit und Lieferfähigkeit aus?

- Entwickelt und fertigt der Hersteller unter **rechtsstaatlichen Rahmenbedingungen?**

- Liefert der Hersteller „Kritische Komponenten“ nach § 2 Absatz 13 und § 9b BSIG? Könnte der Hersteller eine positive **Vertrauenswürdigkeitserklärung / Garantieerklärung** gegenüber dem Betreiber der Kritischen Infrastruktur abgeben bzgl. den IT-Sicherheits-Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität? Ist eine unternehmerische und IT-technische (und datenschutzrechtliche) Vertrauenswürdigkeit gegeben und nachweisbar? Achtung: Augen auf bei Schein-oder Pseudo-Zertifikaten.

- Erfüllt der Hersteller bzw. dessen Produkte neben den **einschlägigen Anforderungen aus den KRITIS-Gesetzen** weitere sektorspezifische oder spezialgesetzliche Regelungen oder zusätzliche **„Branchenspezifische Sicherheitsstandards (B3S)“**?

- Sind die Produkte des Herstellers evtl. auf irgendeiner gesetzlichen **„Blacklist“** (Beispiel aus der Videobranche: NDAA in den USA – Verbot bestimmter chinesischer Hersteller bei Bundesbehörden und Kritischen Infrastrukturen seit dem Jahre 2019. In UK artähnliches Verbot seit 2022)?

- Wie dokumentiert der Hersteller die **Einhaltung von ethischen Standards und Menschenrechten** sowohl in der eigenen Unternehmung als auch entlang seiner Lieferkette?

- Apropos Ethik in der Lieferkette: Ist der Hersteller ab dem Jahr 2023 durch das **Lieferkettensorgfaltsgesetz** sogar rechtlich verpflichtet zur Einhaltung und Dokumentation ethischer Standards?

- Ethik bei KI: Wie dokumentiert der Hersteller und Entwickler von KI-Anwendungen den Aspekt der **Einhaltung ethischer Prinzipien** bei der Entwicklung und beim Einsatz von KI?

- Wie wird **Fairness & Ethik** zum einen bei den Trainingsdaten und bei den Videobilddaten, zum anderen und insbesondere beim Output der KI-Systeme, z. B. Klassifizierungen, Einteilungen, Ergebnissen, Schlussfolgerungen oder Handlungsempfehlungen, gewährleistet?

- Wie werden **negative ethische Folgen** im Hinblick auf mögliche Diskriminierungen, unfaire Ungleichgewichte oder Ungleichbehandlungen, Verzerrungen oder andere soziale Schäden verhindert? Werden sie überhaupt verhindert?

- Entwickelt der Hersteller gar KI-Systeme mit **„unannehmbarem Risiko“** nach dem risikobasierten KI-Gesetzesentwurf der EU?

- Werden mit den KI-Produkten des Herstellers im Projekteinsatz **Menschenrechte gravierend verletzt**?

10 UNTERSTÜTZUNG BEI IHREM KRITIS-PROJEKT

Benötigen Sie Unterstützung bei Ihrem KRITIS-Projekt?
Dann schreiben Sie uns oder rufen Sie uns an:

KRITIS.Sicherheit.Experten.Dallmeier

Lassen Sie uns über Ihr Projekt sprechen! kritis@dallmeier.com +49 941 8700-0

11 SAMMLUNG WEITERFÜHRENDER INFORMATIONEN

KRITISCHE INFRASTRUKTUREN (KRITIS)

Gesetze/Recht/Institutionen/Definitionen

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Das BSI arbeitet auf Grundlage unterschiedlicher (spezial-)gesetzlicher Regelungen und Verordnungen
- Definition Kritische Infrastrukturen (KRITIS) nach Website BSI
- Sektoren- und Sub-Brancheneinteilung von KRITIS nach BBK
- Definition Regulierte Kritische Infrastrukturen (KRITIS) nach §2 Absatz 10 BSIG
- Die nähere Definition / Bestimmung Kritischer Infrastrukturen durch die Rechtsverordnung nach § 10 Absatz 1 BSIG
- Rechtsverordnung „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“, kurz BSI-Kritisverordnung (BSI-KritisV)
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik: BSI-Gesetz (BSIG)
- § 8a BSIG: Sicherheit in der Informationstechnik Kritischer Infrastrukturen
- § 8b BSIG: Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen
- § 8c BSIG: Besondere Anforderungen an Anbieter digitaler Dienste
- § 8f BSIG: Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse (UBI)
- § 9b BSIG: Untersagung des Einsatzes kritischer Komponenten
    - „Lex Huawei“ / Sicherheitsanforderungen an Hersteller/Vorlieferanten von kritischen Komponenten / Drittlandgefahr
    - § 9b BSIG Absatz (3): Hersteller-Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung)
- § 2 Absatz 13 BSIG: Kritische Komponenten
- UP KRITIS als Kür
- IT-Sicherheitsgesetz 1.0
- IT-Sicherheitsgesetz 2.0
- IT-Sicherheitsgesetzes 2.0 auf der Webseite des BSI

- NIS-Richtlinie 1 (Netz-und Informations-Richtlinie 1.0)
- NIS-2 Richtlinie: Das EU-Parlament und der Rat haben im November 2022 dem NIS-2 Entwurf zugestimmt
- NIS-2 Richtlinie: Offizielles Dokument RICHTLINIE (EU) 2022/2555 „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“ (Sprachauswahlseite | Deutsche Fassung PDF)
- CER/RCE Richtlinie: EU Parlament nimmt im November 2022 neue Regeln zum Schutz und Resilienz kritischer Infrastruktur in der EU an
- CER/RCE Richtlinie: Offizielles Dokument RICHTLINIE (EU) 2022/2557 „Über die Resilienz kritischer Einrichtungen“ (Sprachauswahlseite | Deutsche Fassung PDF)
- Weitere Info zu NIS2- und CER-Richtlinie (Dallmeier Webseite)
- KRITIS-Dachgesetz (Eckpunkte):
  - Die Meldung: Bundeskabinett verabschiedet die Eckpunkte des sogenannten KRITIS-Dachgesetzes (07.12.2022)
  - Eckpunkte für das KRITIS-Dachgesetz (Originalwortlaut/pdf)
  - Einschätzung der Eckpunkte KRITIS-Dachgesetz aus Herstellersicht – Physische Sicherheit und deren Regulierung im Fokus
- Außenwirtschaftsgesetz (AWG)
- Außenwirtschaftsgesetz (AWG), § 4 Abs. 1 Nr. 4 , Beschränkungen und Handlungspflichten zum Schutz der öffentlichen Sicherheit und der auswärtigen Interessen
- Außenwirtschaftsverordnung (AWV)
- Außenwirtschaftsverordnung (AWV) §55, Anwendungsbereich der sektorübergreifenden Prüfung
- Außenwirtschaftsverordnung (AWV) §55a Absatz 1 Satz1, Voraussichtliche Beeinträchtigung der öffentlichen Ordnung oder Sicherheit, Fall inländisches Unternehmen ist Betreiber einer Kritischen Infrastruktur
- Lieferkettensorgfaltspflichtengesetz/ Lieferkettengesetz (LkSG) auf Wikipedia
- Lieferkettensorgfaltspflichtengesetz/ Lieferkettengesetz (LkSG) im Wortlaut
- OpenKRITIS: Sehr gute und unabhängige Informationsplattform zu allen regulativen Fragen rund um KRITIS

Artikel/Berichte

- Quo vadis KRITIS? KRITIS-Dachgesetz, neue Vorschriften, Sicherheitsaspekt und Videotechnik (GIT-Sicherheit, 03_2023, ab Seite 42)
- Sonderlagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) (spiegel.de / 03_2022)
- Investor Drittstaat – Fall 50 Hertz - komplexer Sachverhalt hier verständlich nachzulesen
- Investor Drittstaat – Fall Gazprom - komplexer Sachverhalt hier verständlich nachzulesen
- Investor Drittstaat – Fall Gazprom - Kauf von deutschen Gasspeichern im Jahre 2015 (welt.de / 09_2015)

- Luftverkehr: Kein Ende des Chaos an Flughäfen in Sicht (zeit.de / 06_2022)
- Lufthansa fordert Einsatz modernerer Scanner-Technik (faz.net / 07_2022)
- Flughafenchaos und Handwerker-Mangel: Letzter Ausweg Automatisierung (xing/handelsblatt / 07_2022)
- Supply Chain Attacks wie z. B. der Fall Solarwinds (all-about-security.de)
- Sabotage bei Nordstream: Warum Deutschlands kritische Infrastruktur gefährdet ist (augsburger-allgemeine.de / 10_2022)
- Bahn-Sabotage: Angriff auf kritische Infrastruktur (merkur.de / 10_2022)
- Diskussion um den Verkauf von Teilen des Hamburger Hafens an den chinesischen Staatskonzern Cosco (tagesschau.de / 10_2022)
- Nato und EU wollen enger kooperieren beim Schutz kritischer Infrastruktur (sueddeutsche.de / 01_2023)
- Nato und EU wollen enger kooperieren beim Schutz kritischer Infrastruktur: Offizielles 14 Punkte Papier – KRITIS: v.a. Punkte 4, 11, 12
- Spionagevorwürfe gegen China: Baden-Württemberg prüft Ausschluss chinesischer Produkte (stuttgarter-nachrichten.de / 02_2023)
- Überwachung in Deutschland – made in China: Einige Länder haben den Einsatz der Kameras aus Sicherheitsgründen bereits eingeschränkt, Deutschland hingegen noch nicht. Wie gefährlich ist das für die kritische Infrastruktur? (handelsblatt.com / 03_2023)
- Datensicherheit: Das Risiko mit Überwachungskameras aus China (mdr.de / 03_2023)
- Fall Huawei 5G-Netz, Stand März 2023: Bundesregierung plant Huawei-Verbot (handelsblatt.com / 03_2023)
- Weitere Quellen zum geplanten Huawei-5G-Verbot: ZEIT ONLINE (03_2023) und heise online (03_2023)

DATENSCHUTZ, DATENSICHERHEIT, INFORMATIONSSICHERHEIT, IT- UND CYBERSICHERHEIT

- Art. 6 f DSGVO: Rechtmäßigkeit der Verarbeitung
  - Die „Generalklausel“ für Rechtmäßigkeit der Verarbeitung von (Video-)Daten
- Art. 13 DSGVO: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- Art. 25 DSGVO – Datenschutz durch Technikgestaltung („Privacy by Design“)
- Art. 32 DSGVO – Sicherheit der Verarbeitung („Security by Design“)
- Transparenzanforderungen und Hinweisbeschilderung bei einer Videoüberwachung nach der DSGVO
- Art. 5 (1) b DSGVO: Grundsätze für die Verarbeitung – Zweckbindung
- DSK Orientierungshilfe Videoüberwachung für nicht-öffentliche Stellen

- DSK Kurzpapier Nr. 15 – Videoüberwachung nach der Datenschutz-Grundverordnung
- Videoüberwachung durch öffentliche Stellen – Beispiel Baden-Württemberg (Vortrag)
- Videoüberwachung durch öffentliche Stellen – Beispiel Bayern – Artikel 24 BayDSG
- Informationsseite zu Datenschutz & Datensicherheit (Dallmeier Website)
- Cybersecurity für Kritische Infrastrukturen (Dallmeier Webseite)
- Broschüre zu Datenschutz- und Datensicherheitsfunktionen
- Quick Guide Datenschutz – DSGVO-konforme Videoüberwachung
- Best Practice Guide Cybersecurity – Cybersichere Videoüberwachung
- Videotechnik und Cybersecurity Ausgabe 3 der VIDEOEXTRA
- EDPB: European Data Protection Board
- EU Cybersecurity Act (CSA)
- EU Cyber Resilience Act (CRA)
- SBOM „Software Bill of Materials“ – Software-Stückliste – Software supply chain

KÜNSTLICHE INTELLIGENZ, VIDEOANALYSE UND CO.

- Vertrauenswürdige Künstliche Intelligenz (EU-KI-Verordnung Kommissionsvorschlag 2021 / AI Act)
- DSK Positionspapier zur biometrischen Analyse
- DSK Hambacher Erklärung zur Künstlichen Intelligenz
- Praxisleitfaden „Videoanalyse: Wie gut ist eine Künstliche Intelligenz?“
- Expertentipp „Videotechnik und KI“
- Smarte Videoanalyse- und KI-Technologie (Dallmeier Webseite)

VIDEOTECHNIK UND VIDEOPLANUNG

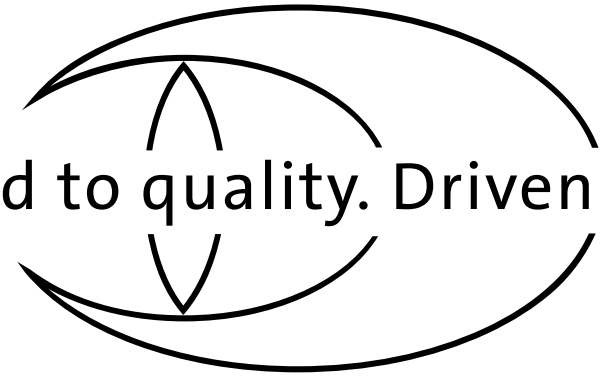
- Fachartikel: „Welche Kameratechnologie für welchen Zweck?“ aus dem PROTECTOR 09/2020
- Projekt Stadt Köln: Einblicke in die Planung, Implementierung und den Betrieb
- Der interaktive Kamerasimulator – am Beispiel KRITIS-Perimeterüberwachung – zum Selbstausprobieren (Desktop empfohlen)

- KI-basierte Videoanalyse für KRITIS-Areal- und Perimeterschutz im Echteinsatz (Video-Casestudy) – KRITIS-Sektor „Transport und Verkehr“
- KI-basierte Videoanalyse und Multifocal-Sensortechnologie für Perimeterschutz branchenneutral und allgemein erklärt (Video)
- Multifocal-Sensortechnologie (Multifocal-Sensorsystem/Panomera-Technologie) allgemein erklärt auf wikipedia.de
- Multifocal-Sensortechnologie (Multifocal-Sensorsystem/Panomera-Technologie) detailliert erklärt auf der Herstellerseite
- Best-of-Breed Ansatz am Beispiel Hersteller Dallmeier
- Branchenbezogene Lösungen für Sicherheit und Prozessautomatisierungen
- 3D-Planung am Beispiel KRITIS-Sektor „Transport und Verkehr – Hafen“
- 3D-Planungstool zur eigenen Nutzung: Professionelle 3D-Planungen intuitiv und einfach selber erstellen
- DIN EN 62676-4 – Videoüberwachungsanlagen für Sicherungsanwendungen
- Industriestandard ONVIF

AUSSCHREIBUNG & WIRTSCHAFTLICHKEIT

- Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie – Das wirtschaftlichste Angebot Hinweise zur richtigen Gestaltung und Wertung im Vergabeverfahren
- Vergabe- und Vertragsordnung für Bauleistungen – Teil A
  - § 3a Zulässigkeitsvoraussetzungen
  - § 3a EU-Zulässigkeitsvoraussetzungen
  - § 7 Leistungsbeschreibung

Dallmeier



Dallmeier electronic GmbH & Co.KG
Bahnhofstr. 16
93047 Regensburg
Deutschland

Tel: +49 941 8700-0
Fax: +49 941 8700-180

info@dallmeier.com
www.dallmeier.com

MADE IN GERMANY

See more.