Dallmeier

Inkl. Projekt-Checklisten und Ausblick KRITIS-Dachgesetz

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

03/2023 . V1.0.0

EDITORIAL

Sehr geehrter Leser, sehr geehrte Leserin,

Kritische Infrastrukturen, im Folgenden kurz „KRITIS“ genannt, zählten, wie der Name schon sagt, schon immer zu den kritischen, besonders lebenswichtigen und daher auch besonders „angriffsgefährdeten“ Organisationen einer Volkswirtschaft – und das im wahrsten Sinne des Wortes.

Im Zusammenhang mit der russischen Invasion in der Ukraine zeigte ein Sonderlagebericht des Bundesamts für Sicherheit in der Informationstechnik, dass Deutschlands „Hochwertziele“ verstärkt zum Ziel für politisch motivierte Cyberattacken werden könnten. Die Sicherheit, der Schutz und die Resilienz von KRITIS umfassen aber mehr als Cybersicherheit. So bestehen zudem konventionelle, physische Gefährdungen sowie geopolitische Risiken durch Investoren und Hersteller aus Drittstaaten.

Wir als Sicherheitsunternehmen mit 38 Jahren Erfahrung rund um das Thema Sicherheit und KRITIS hören bei fast allen KRITIS-Überwachungsprojekten von artverwandten Problemen und Fragestellungen – egal ob bei der Entscheidungsfindung, der Genehmigung, in der öffentlichen Diskussion, bei der Planung, bei der Technologie-entscheidung oder bei der Umsetzung. Das ist auch in vielerlei Hinsicht verständlich: Im Gegensatz zu den gewohnten Routineaufgaben führen viele Verantwortliche von Kritischen Infrastrukturen ein Videoprojekt vielleicht nur ein- oder zweimal in ihrem Berufsleben durch.

Dennoch haben andere KRITIS-Betreiber und KRITIS-Verantwortliche bereits viele Erfahrungen gemacht. Also haben wir uns als Hersteller und Dallmeier-Gruppe mit einer Vielzahl an KRITIS-Projekten gedacht: Lasst uns diese Erfahrungen doch sammeln und allen Interessierten zur Verfügung stellen. Schließlich gilt der altbekannte Leitsatz: „Die gesamte Kette ist nur so stark wie ihr schwächstes Glied.“

Herausgekommen ist dieser Praxisleitfaden für Beteiligte am Entscheidungsprozess, für Fachleute aus den Bereichen „Physische Unternehmenssicherheit“, „IT- und Informationssicherheit“ und „Datenschutz“, für angrenzende Fachverantwortliche, beteiligte Ausschreibungsinstanzen, Planer und Facherrichter, für Aufsichts- und Zuständigkeitsbehörden und für die ausführende und gesetzgebende Politik.

Wir hoffen, Sie finden in diesem Dokument hilfreiche und interessante Informationen, um Videoüberwachungs-projekte in KRITIS zu bewerten, sie zu planen, über sie zu entscheiden und diese erfolgreich durchzuführen.

Ich wünsche Ihnen viel Spaß beim Lesen.

Jürgen Seiler,
Geschäftsführer der Dallmeier Consulting-Tochter davidiT GmbH

PS: Sollten Sie Ideen, Kritik oder Feedback für uns haben, so freuen wir uns über eine E-Mail an kritis@dallmeier.com

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.

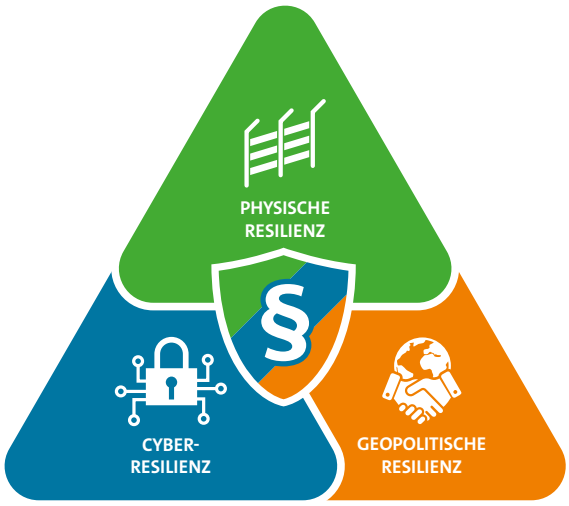
Es geht um die Souveränität Europas

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".

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".

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.

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