KENTIX
Innovative Security

# KRITIS im Jahr 2023 - neue und höhere Anforderungen an die physische Sicherheit

**Was kommt in 2023 auf aktuelle – und künftige – Betreiber von kritischen Infrastrukturen zu? Die Messlatte liegt hoch. Um den neuen Anforderungen aus dem KRITIS Dachgesetz und dem IT-Sicherheitsgesetz 3.0 gerecht zu werden, müssen Betreiber wesentlich mehr Auflagen erfüllen. Wie können wesentliche Ansprüche an die physische Sicherheit einfach und Ressourcen schonend erfüllt werden?**

Kritische Infrastrukturen können effizient und effektiv vor Einbruch, unberechtigtem Zutritt, Brand, unerwünschten Umgebungsbedingungen uvm. geschützt werden. Foto: Unsplash

Aktuelle Krisensituationen wie die Pandemie, die Hochwasserkatastrophe an der Ahr, Russlands Angriff auf die Ukraine und die Sabotageakte auf die Ostseepipelines oder die Deutsche Bahn haben das Brennglas direkt auf die Schwachstellen unserer kritischen Infrastrukturen gerichtet. Und schmerzlich gezeigt: Nicht nur die Versorgung mit essenziellen Gütern wie Energie, Wasser oder Lebensmitteln ist gefährdet. In unserer global vernetzten Welt können ganze Lieferketten durch negative Vorfälle empfindlich gestört werden. Kritische und volkswirtschaftlich schwächende Versorgungsengpässe sind die Folge.

Im unserem täglichen Leben wie in der Politik setzt sich zunehmend die Erkenntnis durch, dass unsere kritischen Infrastrukturen bislang bei weitem nicht ausreichend auf Krisen und Sabotageangriffe vorbereitet und dagegen abgesichert sind. Zu viele voneinander abhängige Systeme sind teilweise gar nicht geschützt und bringen durch den Dominoeffekt auch diejenigen ins Wanken, die bereits mit viel Aufwand und Sorgfalt abgesichert wurden. Der Druck der Öffentlichkeit und der offensichtliche Nachholbedarf bei der Schließung von Schwachstellen in

der KRITIS-Sicherheit beschleunigen die politischen Entscheidungsprozesse zuletzt erheblich. Mit weiteren schnellen Umsetzungen bereits vorbereiteter Gesetze zur Erhöhung der Sicherheit und Resilienz ist zu rechnen.

**2023 - Deutliche Verschärfung der IT-Sicherheit in der KRITIS**
Bereits 2015 setzte die Bundesregierung die NIS-Direktive der EU mit dem IT-Sicherheitsgesetz (IT-SiG) um, das zuletzt im Mai 2021 in einer Novellierung mehr Pflichten für einen größeren Betreiberkreis sowie mehr Befugnisse in der Durchsetzung für den Staat und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mit sich brachte. Mit dem IT-SiG 2.0 gelten nun neben den Sektoren Energie, Wasser, Ernährung, Gesundheit, Transport/Verkehr, IT/TK, Finanzen/ Versicherungen voraussichtlich im ersten Halbjahr 2023 auch die Entsorgung (s.g. Siedlungsabfallentsorgung) sowie Unternehmen im besonderen öffentlichen Interesse zur neu definierten kritischen Infrastruktur. Auch wurden niedrigere Schwellwerte für Betreiber festgelegt und stärkere Sanktionen (ähnlich zur DSGVO) festgelegt. Mit dem IT-SiG 2.0 geht man nun von rund 1.600 KRITIS-Betreibern in Deutschland aus – ein Plus von 300.
Experten und viele KRITIS-Betreiber bemängeln, dass der allgemein gültige Schwellwert von 500.000 versorgten Menschen das Ziel einer resilienten Versorgung der Bevölkerung verfehlt. Beispielsweise werden damit aktuell nur 47 von 5.500 Wasserwerken als KRITIS definiert. Das sind gerade einmal 0,8%. Gleiches gilt für 11.000 Kommunen, die derzeit gar nicht vom IT-SiG Radar erfasst werden.
Mit der durch das EU-Parlament und den EU-Rat verabschiedeten NIS2-Direktive steht bereits in 2023, spätestens Anfang 2024, die Umsetzung dieser Direktive mit dem **IT-SiG 3.0** an. Zusätzlich zu bereits definierten KRITIS-Sektoren kommen voraussichtlich die Sektoren Raumfahrt, Chemie, Industrie, Digitale Dienste, ICT Services (Managed Service/Security Provider), Öffentliche Verwaltungen und Forschung hinzu. Entscheidend ist neben einer weiteren Verschärfung von Pflichten, Sanktionen und Befugnissen des BSI, dass sich die Schwellwerte für die Identifikation der KRITIS Unternehmen und Organisationen nach der Unternehmensgröße richten. Demnach wird voraussichtlich ein Unternehmen aus den o.g. Sektoren als KRITIS definiert, sobald es mehr als 50 Mitarbeiter hat und mehr als 10 Mio. Euro Umsatz im Jahr verzeichnet. Von der Einführung der umgesetzten NIS2-Direktive versprechen sich die regulierenden Behörden eine stärkere und resilientere Abdeckung gegen potentielle IT-Bedrohungen.

**2023 - Das Jahr der physischen physischen Sicherheit in der KRITIS**
Bereits 2015 sind für die IT-Sicherheit in kritischen Infrastrukturen entsprechende Gesetze und Anforderungen in Kraft getreten. Sie regeln in Teilen auch die physische Sicherheit der zu schützenden IT-Infrastruktur nach den Vorgaben des BSI-Grundschutzkompendiums (Modul INF.2). Doch was bislang vollständig fehlt, ist eine eine sektoren- und gefahrenübergreifende gesetzliche Grundlage, die *explizit* den physischen Schutz von kritischen Infrastrukturen abdeckt.

Diese Lücke in der gesetzlichen Regelung zur physischen Absicherung von kritischen Infrastrukturen schließt die Bundesregierung nun mit dem **KRITIS-Dachgesetz**, dessen Eckpunkte-Papier im Dezember 2022 vom Bundestag verabschiedet wurde. Es soll noch vor der Sommerpause 2023 in einem entsprechenden Gesetz umgesetzt werden. Mit dem KRITIS-Dachgesetz beugt sich die Bundesregierung dem Handlungsdruck und nimmt gleichzeitig die aktuell zur Entscheidung stehende EU-Direktive RCE/CER vorweg. Ziel ist es, einen gesamtheitlichen Schutz und damit eine deutliche Resilienz von kritischen Infrastrukturen zu erreichen.
Die vom KRITIS-Dachgesetz betroffenen Sektoren sind Energie, Verkehr, Banken, Finanzmärkte, Gesundheit, Trinkwasser, Abwasser, Ernährung, Digitale Infrastruktur, öffentliche Verwaltungen, Raumfahrt, Medien/Kultur sowie Bildung und Betreuung. Die Identifikation der Betreiber soll nach quantitativen und qualitativen Kriterien erfolgen, die im Gesetz noch zu definieren sind.
Schwerpunkt der Schutzmaßnahmen sind einheitliche Mindestvorgaben für die physische Sicherheit sowie personelle und organisatorische Maßnahmen für die Sicherheit und Widerstandsfähigkeit. Die Ausgestaltung der konkreten Anforderungen bleibt abzuwarten, jedoch stehen Zugangskontrollen, Detektionssysteme und das Monitoring des Anlagenzustands an vorderer Stelle.
Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) wird zur nationalen Behörde für den physischen Schutz kritischer Infrastrukturen und wird – in Zusammenarbeit mit dem BSI – die Meldungen über Sicherheitsvorfälle übernehmen sowie als übergreifende Behörde die

sektorenübergreifende Auswertung vornehmen. Im Eckpunktepapier ist zudem ein klare Aufgabenverteilung zwischen BBK, BSI und BNetzA benannt, um doppelte Zuständigkeiten auszuschließen und einen schnellen Informationsfluss sicherzustellen.

**Was sind die neuen Herausforderungen aus dem neuen IT-Sicherheitsgesetz 3.0 und dem KRITIS DACH Gesetz?**
Wie auch immer die genauen Anforderungen letztlich ausfallen werden, ohne rechtzeitige und ernsthafte Vorbereitung wird es sehr schwierig, ihnen gerecht zu werden.
Auch wenn das Eckpunkte-Papier des KRITIS Dachgesetzes auf die Verhältnismäßigkeit zwischen Risikoeinschätzung und Kosten hinweist: Es ist absehbar, dass die Erhöhung der Anzahl der KRITIS Betreiber und die höheren Anforderungen einen erheblichen Mehraufwand an Personal und Material bedeuten. Wer also frühzeitig seinen Bedarf kennt, kann sich entsprechende Ressourcen rechtzeitig sichern, bevor diese nicht mehr ausreichend und kostengünstig am Markt verfügbar sind.
Eine weitere Herausforderung besteht auch im Betrieb der physischen Sicherheitsanlagen, denn mehr Anlagen benötigen mehr Wartung und erzeugen mehr Meldungen, denen rund um die Uhr an 365 Tagen im Jahr nachgegangen werden muss.

**Wie können die neuen Anforderungen mit keinem bzw. möglichst geringen zusätzlichen Aufwand umgesetzt werden?**
Mehr physische Sicherheit benötigt gerade zu Beginn einen Mehraufwand in Planung und Umsetzung. Doch es gibt Wege, um diese Kosten zu amortisieren. Ein für verteilte Infrastrukturen geeignetes, voll digitalisiertes IoT-Sicherheitssystem ist in der Anschaffung bis zu 40% günstiger als konventionelle Sicherheitssysteme und kann, je nach Ausbau, die Mehrkosten der zusätzlichen Installationen durch einen deutlich geringeren Aufwand in Betrieb, Wartung und Instandhaltung voll kompensieren. Um möglichst effizient mit allen Ressourcen umzugehen, sollte man bei der Auswahl des Systems auf folgende Punkte achten:

- Das System sollte aus möglichst wenigen Komponenten bestehen und gleichzeitig Einbruchs- und Brandmeldung, Umgebungsmonitoring, Zutrittskontrollsystem und optional Videodokumentation abdecken. Auf diese Weise reduzieren sich die Anschaffungskosten (CAPEX) und wird ein erhöhter Aufwand für Integration, Wartung und Instandhaltung verschiedener Systeme vermieden (geringe OPEX).

- Alle eingesetzte Komponenten sollten in einem PoE IP-Netzwerk betrieben werden können, welches zeitgemäß und zukunftssicher ist. Oftmals kann auf eine bestehende Infrastruktur zurückgegriffen werden. Damit entsteht ein sehr hoher Standardisierungsgrad der Verkabelung und Infrastruktur, der langfristig die Wartungs- und Instandhaltungskosten senkt.

- Den wesentlichen Unterschied eines digitalen Sicherheitssystems macht die Software aus. Diese sollte einfach sowie intuitiv zu bedienen sein. Wichtig ist, dass alle Geräte die gleiche Software nutzen und sich damit einfach und stabil vernetzen lassen. Eine zentrale Monitoringfunktion aller Komponenten sowie das Zutritts-, Benutzer- und Alarmmangement sollte unbedingt enthalten sein. Das Management und Monitoring über mobile Apps sollte optional möglich sein und das Gesamtsystem über moderne nicht-proprietäre Schnittstellen wie SNMP, LDAP, Webhooks, ReST-API, etc. verfügen. Zentrale Software-Updates sollten aus der Ferne möglich sein, um mühelos neue Funktionen zu erhalten oder notwendige Sicherheits-Patches einzuspielen. Alle Konfigurations- und Nutzerdaten sollten immer On-Site und nicht in der Cloud gehalten werden können. Der Hersteller von Hard- und Software sollte aus einem vertrauenswürdigen EU-Land stammen und es sollten keine Software-Lizenzkosten entstehen.

- Das System sollte so beschaffen sein, dass es jederzeit modular und unbegrenzt mitwächst, z.B. bei Standorterweiterungen, Unternehmenszukäufen oder Expansionen.

- Zutritts- und Zugriffssysteme sollten online und in Echtzeit betrieben und verwaltet werden können. Hierdurch entfällt die Programmierung an den jeweiligen Schließpunkten und es ist eine lückenlose Dokumentation möglich, wer wann wie lange Zutritt/Zugriff genommen hat. Auch der Türstatus jeder einzelnen Tür ist so 24/7 bekannt. Systeme, bei denen die Programmierung an jedem einzelnen Schließpunkt erfolgt oder keine Echtzeit-Dokumentation vorhanden ist, sind nicht mehr „State of the Art“.

- Wo immer möglich, sollte bei Zutritt- und Zugriffssystemen eine Multifaktor-Authentifizierung genutzt werden, um eine starke Authentifizierung zu gewährleisten. Das gilt sowohl für die Hardware als auch für die Verschlüsselungstechnologie der Software.

- Um jede Art von Ereignis, z. B. Einbruchmeldung, Zutrittsbuchung oder Schwellwertüberschreitungen beim Umgebungsmonitoring zu dokumentieren, sollte das System IP-Kameras integrieren können. So können Ereignisse, aber auch ein Live-Bild von jedem Standort einfach verifiziert werden.

**Fazit**
Unsere aktuelle Zeit schafft ganz neue Herausforderungen an die Sicherheit und Resilienz von kritischen Infrastrukturen, die der Gesetzgeber bereits in 2023 mit der Verschärfung des IT-Sicherheitsgesetzes 3.0 und der Neueinführung des KRITIS Dachgesetz zur physischen Absicherung von kritischen Infrastrukturen in neue Gesetze und Vorgaben umsetzt.
Diese neuen Gesetze werden nicht nur die Anzahl der als kritische Infrastruktur definierten Unternehmen und Organisationen mehrfach erhöhen, sondern diese auch mit erheblichen Anforderungen konfrontieren müssen, um in Zukunft besser auf Angriffe und Vorfälle vorbereitet zu sein. Die Umsetzung kann nur dann gänzlich ohne oder mit nur geringem zusätzlichen Aufwand gelingen, wenn ingesamt der Bereich der physischen Sicherheit mit einem digitalisierten und standardisierten Ansatz erfolgt, bei dem Investitions-, Betriebs-, Wartungs- und Instandhaltungskosten signifikant eingespart werden können.

**Jan Sanders – Autor und Experte rund um die digitale physische Sicherheit von Unternehmen, Organisationen und kritischen Infrastrukturen**

**Kontakt:**
Jan Sanders
Kentix GmbH
Carl-Benz-Str. 9
D-55743 Idar-Oberstein

Phone: 06781 56 25 10
E-Mail: j.sanders@kentix.com

**Über Kentix:**
Sicherheitstechnik wird EINFACH und DIGITAL
Jedes Unternehmen hat einen Bedarf an physischer Sicherheit. Dieser muss schnell und skalierbar zu erfüllen sein. Darauf hat Kentix eine revolutionär einfache Antwort entwickelt: Diese heisst KentixONE, von der Zutrittskontrolle bis zur Alarm- und Videotechnik ist alles 100% IoT-basiert und in einer Plattform zusammengefasst. KentixONE verschmilzt 8 herkömmliche Sicherheitssysteme und erkennt vorausschauend über 40 Gefahren. Einfacher geht's nicht.
Unternehmen aus allen Branchen sichern durch Produkte der Kentix GmbH ihr Geschäft und Infrastruktur gegen physische Gefahren sowie menschliches Fehlverhalten ab und halten gesetzliche Anforderungen ein. Die Entwicklung und Produktion erfolgt ausschließlich in Deutschland.