Neue Zeiten, neue Bedrohungen

Die Welt verändert sich - rasant, digital & unberechenbar.

KRITIS-Dachgesetz, **NIS2**-Richtlinie & **CRA**

Neue Zeiten, neue Bedrohungen

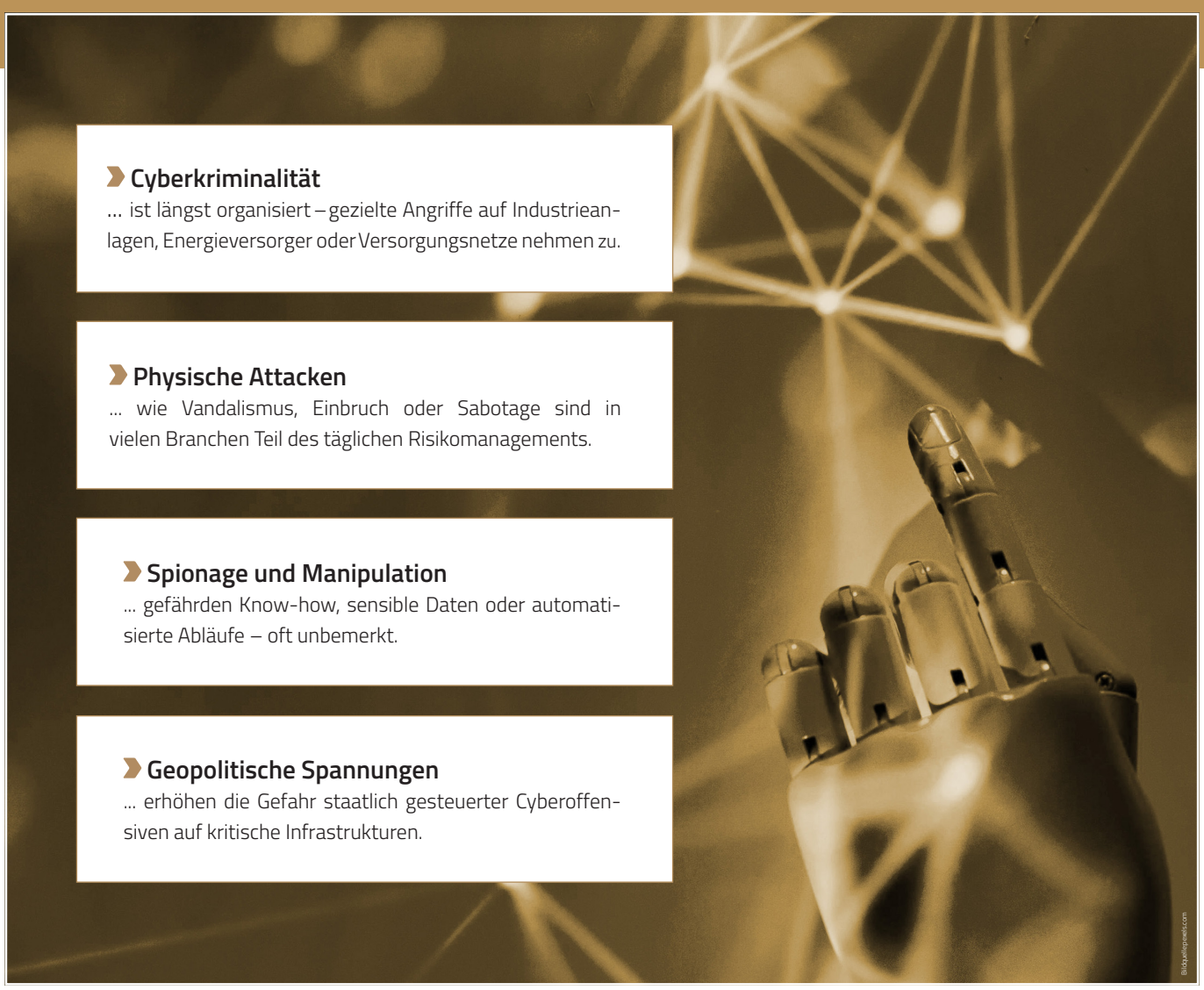
Die Welt verändert sich - rasant, digital & unberechenbar.

Technologischer Fortschritt macht unser Leben effizienter und vernetzter. Doch mit dieser Entwicklung wächst auch eine andere Realität: Die Bedrohungslage wird komplexer – durch Cyberangriffe, Industriesabotage, digitale Spionage und physische Übergriffe. Gefahren, die nicht mehr nur getrennt betrachtet werden können, sondern oft miteinander verknüpft auftreten.

Heute ist jede Sicherheitslücke ein mögliches Einfallstor – mit realen Konsequenzen.

Unternehmen, Behörden und öffentliche Einrichtungen geraten zunehmend unter Druck. Der Anspruch an Sicherheit steigt – ebenso wie die Verantwortung. Wer in der heutigen Zeit Schutz bieten will, muss ganzheitlich denken: physisch, digital und strategisch.

Ein Blick auf die Bedrohungslage zeigt die Dringlichkeit:



Cyberkriminalität
... ist längst organisiert – gezielte Angriffe auf Industrieanlagen, Energieversorger oder Versorgungsnetze nehmen zu.

Physische Attacken
... wie Vandalismus, Einbruch oder Sabotage sind in vielen Branchen Teil des täglichen Risikomanagements.

Spionage und Manipulation
... gefährden Know-how, sensible Daten oder automatisierte Abläufe – oft unbemerkt.

Geopolitische Spannungen
... erhöhen die Gefahr staatlich gesteuerter Cyberoffensiven auf kritische Infrastrukturen.

Schutz für Menschen, Anlagen & Daten

Fazit - Umdenken ist Pflicht!

Klassische, groß angelegte Sicherheitssysteme stoßen immer öfter an ihre Grenzen – sie sind teuer, schwerfällig und oft unflexibel. Die Zukunft gehört smarteren Konzepten: Kompakt, vernetzt, KI-gestützt – und vor allem cybersicher. Denn Systeme, die heute Menschen, Gebäude oder Infrastrukturen schützen, müssen auch digitalen Angriffen standhalten. Was früher oft vernachlässigt wurde, ist heute unverzichtbar. Gefragt sind Lösungen mit maximaler Wirkung bei minimalem Aufwand – die sich nahtlos integrieren lassen, sich intelligent anpassen und mehr leisten als bloße Überwachung.

Was heißt das in der Praxis?

Wenn Menschen, Anlagen und Daten geschützt werden müssen, zählen Klarheit, Reaktionsschnelligkeit und Vertrauen – in jeder Branche, bei jedem Wetter, zu jeder Tageszeit.

Ob unübersichtliches Werksgelände, sensibler Klinikbereich oder hochfrequentierter Bahnhofsvorplatz: Intelligente Videosicherheit mit MOBOTIX erkennt Risiken, bevor sie zum Problem werden. Dank smarter Kameraarchitektur, KI-gestützter Analyse und zielstrebiger Cybersicherheit entstehen Lösungen, die verstehen, was wirklich zählt und die im Ernstfall selbstständig handeln.

Der Handlungsdruck wächst

Sicherheit ist kein „Nice-to-have"

Für Betreiber kritischer Infrastrukturen, öffentliche Einrichtungen und viele Unternehmen ist sie längst gesetzlich verankerte Pflicht. Wer nicht schützt, riskiert nicht nur Datenverluste oder Betriebsunterbrechungen – sondern auch empfindliche Bußgelder, Imageschäden oder sogar ein Betriebsverbot. Der Druck nimmt zu. Und zwar nicht nur aus der Praxis, sondern vor allem aus der Gesetzgebung.

Nationale wie europäische Institutionen reagieren mit neuen Vorschriften.

Was all diese Regelungen vereint: Sie fordern aktives, nachvollziehbares Handeln – keine Alibi-Maßnahmen. Sicherheitsverantwortliche müssen heute mehr denn je beweisen, dass sie Risiken vorausschauend erkennen, dokumentieren, kontrollieren und kommunizieren können.

Investition in Zukunftssicherheit

Die wichtigsten Regelwerke:

- **KRITIS-Dachgesetz (Deutschland):**
  Stellt erhöhte Anforderungen an Ausfallsicherheit und Resilienz in kritischen Sektoren wie Energie, Wasser, Gesundheit und Verkehr.
- **NIS2-Richtlinie (EU):**
  Gilt für 18 definierte Sektoren – mit klaren Vorgaben zu Cyber- und physischen Sicherheitsmaßnahmen, Meldepflichten und Risikomanagement.
- **Cyber Resilience Act (CRA):**
  Verpflichtet Hersteller digitaler Produkte zu „Secure by Design" – Sicherheit wird damit zur Pflicht von Anfang an.

Die neue Gesetzgebung fragt nicht, ob etwas passiert – sondern wie gut Sie vorbereitet sind, wenn es passiert und was Sie im Ernstfall tun können.

Was bedeutet das für Sie?

Sicherheit darf nicht länger als Reaktion verstanden werden – sie muss integraler Bestandteil der Unternehmensstrategie sein. Das heißt konkret:

- Risiken identifizieren, dokumentieren und bewerten
- Sicherheitskonzepte planen und umsetzen
- Schutzsysteme wie Videoüberwachung gesetzeskonform einsetzen
- Melde- und Nachweispflichten erfüllen (externe Kommunikation)

Was auf den ersten Blick nach Mehraufwand klingt, ist in Wahrheit eine Investition in Zukunftssicherheit. Unternehmen, die heute aktiv werden, können, Compliance-Risiken minimieren, Angriffe frühzeitig erkennen, kostenintensive Ausfälle vermeiden und Vertrauen bei Kunden, Partnern und Behörden stärken.

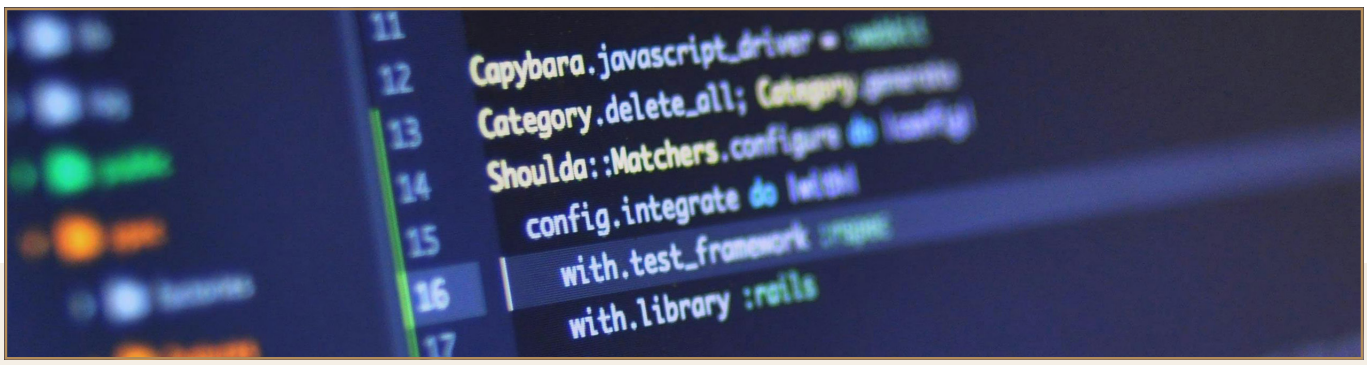
Und der richtige Zeitpunkt zum Handeln ist jetzt!

Zielgruppen - wer muss handeln?

Die Zeiten, in denen nur Großkonzerne in den Fokus gesetzlicher Sicherheitsanforderungen gerieten, sind vorbei. Immer mehr Organisationen – auch aus dem Mittelstand – stehen heute in der Verantwortung, ihre IT- und physische Sicherheit professionell zu organisieren. Besonders im Licht der NIS2-Richtlinie, des KRITIS-Dachgesetzes und des Cyber Resilience Acts wird klar:

Sicherheitsverantwortung ist keine Frage der Unternehmensgröße, sondern der Systemrelevanz.

Zwei Kategorien stehen im Zentrum der neuen Regulierung – mit jeweils klaren Pflichten:



Wesentliche Einrichtungen (Essential Entities)

Organisationen mit besonders hoher Bedeutung für das tägliche Leben und die öffentliche Ordnung, wie:

- Energieversorger & Netzbetreiber
- Betreiber von Verkehrsinfrastruktur (z. B. Flughäfen, Bahnhöfe)
- Kliniken, Pflegeeinrichtungen & Gesundheitseinrichtungen
- Banken & Finanzdienstleister
- Betreiber von Wasserversorgung & Abwasserentsorgung
- Digitale Infrastrukturen (z. B. Rechenzentren, Cloud-Anbieter)

Wichtige Einrichtungen (Important Entities)

Auch Unternehmen ohne lebenswichtige Aufgaben, aber mit erheblichem Einfluss auf Versorgung oder Infrastruktur, sind betroffen – beispielsweise:

- Post- & Kurierdienste
- Entsorgungsunternehmen
- Maschinen- & Anlagenbau
- Chemieunternehmen
- Lebensmittelproduktion & -logistik

Diese Einteilung schafft Rechtsverbindlichkeit

Warum ist diese Einteilung so entscheidend?

Weil sie **Rechtsverbindlichkeit schafft**. Sobald ein Unternehmen in eine dieser Kategorien fällt, gelten gesetzlich festgelegte Anforderungen – etwa in puncto **Videoüberwachung, Zutrittskontrollen, Netzwerksicherheit oder Meldepflichten**.

Ob Klinik, Entsorgungsbetrieb oder Maschinenhersteller
– alle betroffenen Organisationen müssen:

- Physische und digitale Risiken systematisch analysieren
- Präventive Maßnahmen einführen und dokumentieren
- Im Ernstfall schnell und koordiniert reagieren
- hre Resilienz gegenüber Angriffen und Ausfällen gezielt stärken
  (z.B. mit den branchenspezifischen Videosicherheitslösungen von MOBOTIX)

Wie ist die Lage außerhalb der EU?

Auch wenn sich viele neue Anforderungen – wie NIS2, KRITIS oder der Cyber Resilience Act – auf den europäischen Raum beziehen, spiegeln sie einen globalen Trend wider: Sicherheitsanforderungen steigen weltweit.

In den **USA** etwa greifen Vorgaben wie der **National Defense Authorization Act (NDAA)**, die **Cybersecurity Executive Orders** oder branchenspezifische Normen für kritische Infrastrukturen. Auch in **Asien**, dem **Mittleren Osten** und **Australien** rücken Themen wie physische Resilienz, IT-Sicherheit und Auditfähigkeit zunehmend in den Fokus.

Für MOBOTIX ist eine professionelle Videolösung mit entschlossener Cybersecurity und IT-Sicherheit ein globales Fokusthema: Unsere Produkte orientieren sich an internationalen Anforderungen und sind **weltweit einsatzfähig** – von der Klinik in Bayern bis zum Solarpark in Kalifornien.

Sicherheit im digitalen Zeitalter

Digitalisierung, Automatisierung und Vernetzung schaffen neue Möglichkeiten

– aber auch neue Risiken!

In einer immer stärker vernetzten Welt werden Sicherheitspannen nicht nur wahrscheinlicher, sondern auch folgenreicher. Angriffe auf kritische Infrastrukturen, Sicherheitslücken in vernetzten Geräten und die steigende Komplexität von IT-Systemen verlangen nach klaren Spielregeln – und genau die liefern drei zentrale Regelwerke: das **KRITIS-Dachgesetz**, die **NIS2-Richtlinie** und der **Cyber Resilience Act (CRA)**.

Diese Gesetze und Richtlinien bilden gemeinsam den rechtlichen Rahmen für ein neues IT-Sicherheitsverständnis. Sie schreiben nicht nur vor, was getan werden muss – sondern definieren auch, wie Sicherheit strukturiert, geplant und nachgewiesen werden muss. Wer heute sicher sein will, braucht mehr als nur Technik:

Die richtige Strategie!

Die 3 Säulen der digitalen Sicherheitsregulierung

1 KRITIS-Dachgesetz (Deutschland):

Ein nationales Gesetz zum Schutz kritischer Infrastrukturen. Ziel: lebenswichtige Dienste wie Strom, Wasser, Gesundheit oder Verkehr gegen Ausfälle und Angriffe abzusichern. Für Betreiber bedeutet das: **Erhöhte Anforderungen an Resilienz, Erkennung, physische Sicherheit – und klare Nachweispflichten gegenüber Behörden.**

2 NIS2-Richtlinie (EU-weit):

Seit Okt. 2024 verpflichtend für Unternehmen aus 18 Sektoren. Der Fokus liegt auf **Risikomanagement**, **Meldepflichten** und **Business Continuity** – inklusive Anforderungen an physische Sicherheit und Videoüberwachung.

3 Cyber Resilience Act (CRA):

Der CRA betrifft vor allem Hersteller digitaler Produkte und Software – also auch Kameras, Recorder oder VMS-Systeme.

Ab 2027 gilt: Produkte mit digitalen Komponenten müssen Cybersicherheit bereits in der Entwicklung („Secure by Design“) und im Standardbetrieb („by Default“) gewährleisten – inklusive CE-Kennzeichnung.

Die Regelwerke

Die Regelwerke im Vergleich

Während das **KRITIS-Dachgesetz** auf nationale Betreiber kritischer Infrastrukturen abzielt, ist **NIS2** deutlich breiter gefasst – und gilt für zahlreiche Sektoren quer durch die EU. Der **CRA** hingegen konzentriert sich auf die Produktsicherheit selbst: Entwickler und Anbieter müssen sicherstellen, dass ihre Lösungen den höchsten Sicherheitsstandards entsprechen.

So greifen die drei Regelwerke ineinander:

KRITIS schützt die Versorgung, **NIS2** regelt den organisatorischen Umgang mit Risiken, und der **CRA** stellt sicher, dass die eingesetzten Technologien auf Produktebene überhaupt sicher verwendet werden können.

Video Security

Rechtlich gefordert in vielen Regionen

Aspekt	KRITIS-Dachgesetz (D)	NIS2-Richtlinie	Cyber Resilience Act (CRA)
Geltungsbereich	Kritische Infrastrukturen in Deutschland	Wesentliche & wichtige Einrichtung in der gesamten EU	Hersteller digitaler & Software in der EU
Ziel	Schutz lebenswichtiger Dienstleistungen	Erhöhung der Cybersicherheit & Meldepflicht bei Vorfällen	Verpflichtende Cybersicher-heitsstandards für Produkte
Status	In Umsetzung (DE)	Gültig ab Oktober 2024	Verabschiedet, Anwendung ab 2027
Betroffene Sektoren	Energie, Gesundheit, Wasser, Transport, usw.	18 Sektoren inkl. öffentl. Ver-waltung, Gesundheitswesen, digitale Infrastruktur	Hersteller, Händler, Inver-kehrbringer digitaler Geräte
Schwerpunkt	Resilienz physischer und digitaler Systeme	Risikomanagement, Business Continuity, Incident Reporting	Sicherheit im Design und bei Markeinführung
Aufsichtsbehörden	BSI & sektorspezifische Behörden	National Cybersicherheits-behörden der EU-Staaten	Marktaufsichtsbehörden & EU-Kommission

CN H&D GmbH - Am Kirchfeld 10 - 84431 Heldenstein - info@cn-hd.de - www.cn-hd.de