BLUE SWAN BULLETIN

Der KRITIS und Supply Chain Newsletter

Januar 2026 | MIT FREUNDLICHER EMPFEHLUNG VON BLUE RISK IQ | AUSGABE 5 | www.blueriskiq.de

Damit wir morgen noch Butter auf dem Brot haben

- was die Butterproduktion über kritische Lieferketten lehrt

Was für Verbraucher selbstverständlich wirkt, ist in Wahrheit das Ergebnis einer hochkomplexen, eng verzahnten Lieferkette – von der Milchverarbeitung über Kühlung, Verpackung und Transport bis ins Supermarktregal. Mit der Verabschiedung des KRITIS-Dachgesetzes durch den Bundestag wird klar: Die Lebensmittelproduktion ist nicht nur Wirtschaftszweig, sondern systemrelevante Infrastruktur. Resilienz ist damit keine freiwillige Vorsorge mehr, sondern ab dann gesetzlicher Auftrag.

Was das KRITIS-Dachgesetz jetzt für Betreiber der Lebensmittelversorgung bedeutet

Die Herstellung und Verteilung von Lebensmitteln – am Beispiel der Butterproduktion – zeigt exemplarisch, wie abhängig unsere Versorgung von funktionierenden Infrastrukturen ist. Ohne Strom keine Kühlung. Ohne Kühlung keine Verarbeitung. Ohne Verarbeitung keine Auslieferung. Und ohne funktionierende Logistik bleibt das Butterfach im Supermarkt leer.

Genau hier setzt das neue KRITIS-Dachgesetz an: Es verpflichtet Betreiber kritischer Infrastrukturen, ihre Widerstandsfähigkeit gegenüber Störungen systematisch zu erhöhen – über alle Sektoren und Abhängigkeiten hinweg.

BLUERISKIQ

Themen im Überblick

Was, wenn der Strom ausfällt?

Wenn ein regionaler Stromausfall über mehrere Tage eine Molkerei trifft, dann könnte die Situation sich folgendermaßen entwickeln:

- Ohne entsprechende Vorsorge könnten die Produktionsanlagen stillstehen;
- Kühlketten sind nur zeitlich begrenzt stabil;
- IT-Systeme zur Steuerung und Rückverfolgbarkeit fallen aus;
- Logistikpartner können nicht disponieren;
- Supermärkte erhalten keine Ware.

Was früher als **„Betriebsstörung“** galt, wird heute als systemisches Risiko verstanden. Das KRITIS-Dachgesetz verlangt, genau solche Szenarien vorab zu analysieren, zu bewerten und abzusichern.

“Alles Käse?” Nein, der Ansatz geht schon auf dem Bauernhof los

Beispielsweise auch die Melkmaschinen brauchen Strom und daher sind Dieselaggregate oder Solar- oder Biogasanlagen keine Seltenheit.

Ein längerer Stromausfall ist für Milchviehbetriebe kritisch:

- Kühe können gesundheitliche Probleme bekommen;
- Milch verdirbt ohne Kühlung;
- Betrieb steht schnell still und somit auch die Lieferkette.

Die ersten Schritte ...

Schritt 1: Meldung an die zuständige Behörde - alles beginnt mit Transparenz

Betreiber kritischer Infrastrukturen sind verpflichtet, sich bei der zuständigen Behörde zu melden. Diese formale Einstufung ist kein Selbstzweck, sondern die Grundlage für einen strukturierten Resilienzprozess.

Schritt 2: Durchführung einer Risikoanalyse

Im nächsten Schritt ist eine systematische Risikoanalyse durchzuführen. Dabei geht es nicht nur um das eigene Werkstor, sondern um die gesamte Lieferkette.

Zentral ist dabei das Erkennen von KRITIS-Interdependenzen: Wo bin ich abhängig von anderen kritischen Systemen – und wer ist wiederum von mir abhängig?

Schritt 3: Von der Feststellung von Schwachstellen zu wirksamen Maßnahmen

Sind diese Abhängigkeiten identifiziert, müssen risikomindernde Maßnahmen umgesetzt werden.

Zum Beispiel:
- Notstrom- und Redundanzkonzepte;
- Absicherung von Kühlketten;
- organisatorische Notfallpläne;
- klare Melde- und Entscheidungswege;
- abgestimmte Krisenkommunikation mit Partnern.

Entscheidend ist dabei nicht die Menge der Maßnahmen, sondern der richtige Weg.

Wir beraten Sie gerne und zeigen Ihnen, wie kostbare Lieferketten wirksam abgesichert werden können!

Die Butter dient lediglich als Beispiel zur Veranschaulichung von KRITIS

Unsere Rolle als Risk Navigator

Genau hier unterstützen wir Betreiber kritischer Infrastrukturen. Das aktuelle Beispiel eines mehrtägigen Stromausfalls in der Hauptstadt verdeutlicht, wie es um die Resilienz in Deutschland bestellt ist. Als Risk Navigator begleiten wir nicht nur die formale Erfüllung gesetzlicher Anforderungen, sondern helfen dabei, Resilienz praktisch und nachhaltig aufzubauen:

- Strukturierte Risikoanalysen;
- Bewertung von KRITIS-Interdependenzen;
- Entwicklung passgenauer Maßnahmen;
- Orientierung im neuen regulatorischen Rahmen;
- Übersetzung von Gesetz in umsetzbare Praxis;
- Business Continuity Pläne.

Unser Anspruch

Damit gesetzliche Pflichten nicht zur Belastung werden, sondern zur echten Stärkung der Versorgungssicherheit beitragen.

BLUERISKIQ

Genauso geht es um Brot, frische Lebensmittel, tiefgekühlte Waren – und um die kontinuierliche Versorgung von Krankenhäusern, Pflegeeinrichtungen und anderen systemrelevanten Abnehmern. Überall dort, wo Kühlketten unterbrechungsfrei funktionieren müssen, entscheidet Resilienz über Versorgung oder Ausfall.

Das KRITIS-Dachgesetz lenkt den Blick weg von einzelnen Betrieben hin zu ganzen Versorgungsketten. Es ist nicht die Frage, ob mein Standort abgesichert ist, sondern: Wie stabil ist das Zusammenspiel von Energie, IT, Personal, Logistik und Partnern – auch unter Stressbedingungen?

Gerade Kühlketten zeigen, wie schnell aus einer lokalen Störung ein gesamtgesellschaftliches Problem werden kann. Stromausfälle, IT-Störungen oder Logistikengpässe gefährden nicht nur Warenwerte, sondern die Versorgung mit lebensnotwendigen Gütern.

Resilienz entsteht deshalb nicht durch Checklisten, sondern durch ein realistisches Verständnis von Abhängigkeiten, klare Verantwortlichkeiten und praktikable Notfallkonzepte über Organisationsgrenzen hinweg.

Denn die entscheidende Frage lautet nicht ob es zu Störungen kommt – sondern ob die Versorgung auch im Falle einer Störung aufrechterhalten werden kann. ■

KRITIS-relevante Fragen auch für Sektor Logistik & Verkehr, Krankenhäuser, Energie, Tankstellen, etc.

Psychologie + Krisenmanagement

Warum Resilienz auch ontologische Sicherheit braucht

Ein Fachbeitrag von Stefan Vito Hiller, Senior Security Advisor, zur Tiefe von Krisen in kritischen Infrastrukturen – und was das KRITIS-Dachgesetz leisten kann

Wenn man von Krisen in kritischen Infrastrukturen spricht, denkt man meist an Stromausfälle, Hochwasser, Systemversagen oder Versorgungslücken. Doch wer sich nur auf technische Resilienzmaßnahmen verlässt, greift zu kurz. Denn Krisen gefährden nicht nur die Funktionalität einer Einrichtung, sondern auch etwas Tieferes: das Selbstverständnis der Organisation, die Rollen ihrer Mitarbeitenden und das Vertrauen der Gesellschaft. All das ist Teil dessen, was Soziologen **ontologische Sicherheit** nennen.

Dieser Beitrag zeigt, warum Resilienzarbeit bei Betreibern kritischer Anlagen mehr leisten muss als Notfallpläne und Risikoanalysen – und wie das KRITIS-Dachgesetz wichtige Impulse geben kann, ohne dabei das Menschliche aus dem Blick zu verlieren.

Ontologische Sicherheit – was bedeutet das?

Der Begriff der ontologischen Sicherheit stammt aus der Sozialtheorie, insbesondere von Anthony Giddens.
Er bezeichnet das Grundgefühl von Stabilität, Kontinuität und Vorhersehbarkeit im Leben – also das Vertrauen, dass **„die Welt in Ordnung ist“** und ich **„weiß, wer ich bin und wie ich handeln kann“.**

Übertragen auf Organisationen – und insbesondere auf **Betreiber kritischer Infrastrukturen** – bedeutet ontologische Sicherheit:

- klare Rollenverständnisse;
- stabile Routinen;
- verlässliche Kommunikation und
- ein kollektives Selbstbild, das Sicherheit erzeugt.

In Krisen wird genau dieses Gefüge bedroht. Und das oft tiefgreifender als jede physische Störung.

Krise als identitätsbezogene Erschütterung

Krisen – ob Naturereignis, Versorgungsengpass, gesellschaftlicher Konflikt oder Personalausfall – durchbrechen Routinen, erzeugen Kontrollverlust und bringen Handlungslogiken durcheinander.
Sie stellen damit nicht nur Systeme infrage, sondern auch die Frage: *Wer sind wir jetzt noch – als Menschen, als Organisation, als Gesellschaft?*

Einige typische Auswirkungen sind:

- Verlust des Selbstverständnisses: *„Wir konnten nicht mehr leisten, wofür wir stehen.“*
- Desorientierung im Team: *„Ich wusste nicht mehr, was ich tun sollte.“*
- Vertrauensbruch bei Stakeholdern: *„Ist diese Einrichtung überhaupt noch verlässlich?“*

Diese tiefere Verunsicherung ist nicht technischer Natur, sondern betrifft die **ontologische Sicherheit** aller Beteiligten – von der Führungsebene über Mitarbeitende bis hin zur Bevölkerung.

Resilienz braucht mehr als Technik

Klassisches Krisenmanagement zielt auf:

- Risikoanalyse;
- Notfallpläne;
- Wiederanlaufverfahren (Recovery);
- Ressourcensteuerung.

Diese Maßnahmen sind zentral – aber sie reichen nicht aus, wenn es darum geht, **ontologische Sicherheit** aufrechtzuerhalten.
Resilienz muss heute mehr sein als Widerstandsfähigkeit im technischen Sinne. Sie muss auch identitätsstabilisierend, sinnstiftend und beziehungsorientiert sein.

Als jemand, der sich ehrenamtlich im Katastrophenschutz engagiert, beobachte ich, wie die Anforderungen an Resilienz und Krisenmanagement in der Praxis oft komplexer und vielschichtiger sind, als es in gesetzlichen Vorgaben wie dem KRITIS-Dachgesetz abgebildet wird. Die Gesetze legen zwar einen wichtigen Rahmen fest, fokussieren jedoch meist auf Strukturen, Prozesse und technische Absicherung.

In der Praxis spielen jedoch auch zwischenmenschliche Dynamiken, informelle Netzwerke, situative Flexibilität und nicht zuletzt die **ontologische Sicherheit** aller Beteiligten eine entscheidende Rolle. Das erfordert, die Gesetzesvorgaben mit einem erweiterten Blick zu betrachten, der:

- die Mensch-zu-Mensch-Beziehungen in Krisen betont;
- die emotionale und psychologische Belastung anerkennt und
- die Dynamik sich ständig ändernder Situationen und Prozesse berücksichtigt.

Dieser Blick eröffnet zusätzliche Handlungsfelder und sensibilisiert dafür, wie wichtig es ist, Resilienz nicht nur technisch, sondern auch sozial und kulturell zu stärken.

Checkliste zur Stärkung ontologischer Sicherheit

Rollen und Verantwortlichkeiten klären

Klare Zuordnung der Zuständigkeiten in Krisen

Transparente Kommunikation sicherstellen

Regelmäßige Updates auch bei Unsicherheit

Sinnstiftende Botschaften senden

Werte und Mission hervorheben

Psychosoziale Unterstützung anbieten

Zugang zu Beratung und Feedback

Informelle Netzwerke aktivieren

Nutzung von sozialen Bindungen zur Stabilisierung

Empfehlungen für Führungskräfte

- Menschen in ihren Rollen halten und stärken;
- Kommunikation, die nicht nur informiert, sondern orientiert;
- Verlust von Sinn vermeiden durch klare Werte-kommunikation;
- Organisationale Identität schützen – auch unter Druck.

Organisationen, die Resilienz ernsthaft leben wollen, sollten das KRITIS-Dachgesetz nicht nur als Regulierung, sondern als Gestaltungsraum verstehen. Folgende Fragen können dabei helfen, ontologische Sicherheit systematisch mitzudenken:

Reflexionsfragen an das Management

1. Welche Routinen und Rollen geben uns im Alltag Sicherheit?
2. Was bedeutet es für unsere Identität, eine „kritische Infrastruktur“ zu sein?
3. Wie erhalten wir Sinn und Vertrauen, wenn unsere Leistung eingeschränkt ist?
4. Wie können wir im Krisenfall nicht nur Systeme, sondern auch das Selbstverständnis unserer Organisation schützen?

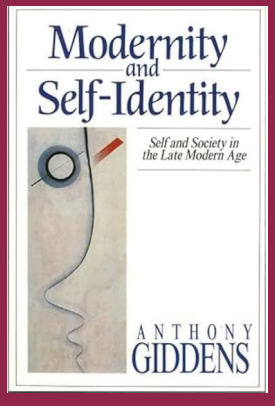
Fazit

Das KRITIS-Dachgesetz ist ein notwendiger Schritt in Richtung strukturierter Resilienz für systemrelevante Organisationen. Doch seine volle Wirkung entfaltet es erst, wenn es mit einer tieferen Dimension verbunden wird: **dem Schutz der ontologischen Sicherheit.**

Wer Resilienz heute gestaltet, schützt nicht nur Versorgungssysteme – sondern auch das, was Menschen und Organisationen zusammenhält. Es ist das Vertrauen, dass man selbst im Ausnahmezustand weiß, wer man ist, was zu tun ist und wofür es sich lohnt zu handeln. ■

Buchtipp

Giddens betrachtet Identität als reflexives Projekt, das aktiv gestaltet werden muss. Zentrale Kernkonzepte sind u. a.:
- **Ontologische Sicherheit -** Grundvertrauen in die Welt und das eigene Sein zur Abwehr existenzieller Angst.
- **Reflexivität -** Das ständige Hinterfragen und Neuentwerfen der eigenen Identität.
- **Biografisches Narrativ -** Eine konsistente Lebensgeschichte, die Vergangenheit und Zukunft verbindet.



Analyse

Umfrage zum Warntag 2025

Im letzten Jahr führten wir eine Umfrage anlässlich des bundesweiten Warntags durch, um herauszufinden, wie häufig die bundesweiten Warntests aus Sicht der Bevölkerung durchgeführt werden sollten.

Die Ergebnisse zeigen ein sehr klares Stimmungsbild: Mit **64 %** spricht sich die große Mehrheit dafür aus, die Tests alle drei Monate durchzuführen. Weitere **18 %** wünschen sich sogar eine monatliche Durchführung, ähnlich wie es beispielsweise in den 80er Jahren der Fall war.
Zusammen ergibt das beeindruckende **82 %**, die sich deutlich häufigere Warntests wünschen, als sie derzeit stattfinden.

Lediglich **10 %** der Befragten sind mit dem aktuellen jährlichen Rhythmus zufrieden. Halbjährliche Tests (**4 %**) oder alternative Testmethoden ohne öffentliche Warntage (**4 %**) stoßen kaum auf Interesse.

Bemerkenswert ist, dass keine einzige Stimme dafür abgegeben wurde, Warntests nur bei konkreten Bedrohungslagen durchzuführen.

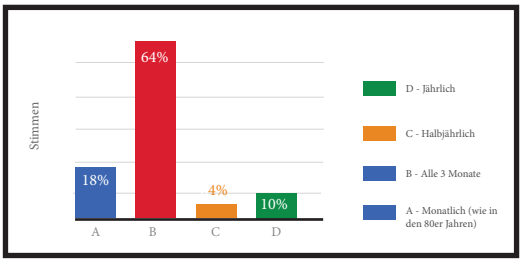
Fazit

Die Ergebnisse verdeutlichen den klaren Wunsch nach regelmäßigen und verlässlichen Tests unserer Warnsysteme für den Katastrophenfall. Der derzeitige jährliche Warntag wird von der überwältigenden Mehrheit als nicht ausreichend empfunden. Besonders die starke Zustimmung für einen vierteljährlichen Rhythmus zeigt, dass Sicherheit und Funktionsfähigkeit der Systeme für die Menschen eine hohe Priorität haben.

WSD permanent security

Warntag 2025 - Auswertung unserer Umfrage

Wie oft sollten bundesweite Warntests durchgeführt werden?



Quelle: linkedin.com/company/wsdpermanentsecuritygmbh/

Auszug aus unserer aktuellen Ursachenanalyse

Die Forderung nach häufigeren Warntests ist aus unserer Sicht kein Meinungsphänomen, sondern das Ergebnis wiederkehrender Beobachtungen aus Risiko-, Krisen- und Resilienzanalysen.

Sie verweist auf ein strukturelles Grundproblem, das sich über Jahre hinweg aufgebaut hat. Historisch waren Warnsysteme stärker im Alltag verankert – in Westdeutschland etwa durch regelmäßige Sirenentests, in Ostdeutschland durch andere, zentral organisierte Strukturen.
Trotz unterschiedlicher Ausprägungen war der Ernstfall gedanklich präsent. Diese gemeinsame Referenz fehlt heute weitgehend, insbesondere bei jüngeren Generationen, für die ziviler Bevölkerungsschutz kein erlebtes, sondern häufig ein abstraktes Konzept ist. Jedoch gibt es auch Ausnahmen.

Diese Entwicklung spiegelt sich oftmals auch in Unternehmen wider. Der Katastrophenschutz ist heute fragmentierter organisiert, Verantwortlichkeiten sind auf Staat, Betreiber kritischer Infrastrukturen und Wirtschaft verteilt. Unsere Beobachtungen zeigen, dass Krisenmanagement in vielen Organisationen unterschiedlich ausgeprägt ist.

Gleichzeitig hat sich die Bedrohungs- und Belastungslage objektiv verändert. Deutschlands Rolle als logistische Drehscheibe, zunehmende militärische Bewegungen und hybride Risiken sind sichtbare Faktoren. Dass grundlegende Regeln und Verhaltensweisen vielen nicht bekannt sind – etwa wie man sich als Autofahrer bei einer Kolonne (§27, STVO) verhält –, ist dabei kein individuelles Versäumnis, sondern Ausdruck fehlender Vorbereitung auf Systemebene.

Vor diesem Hintergrund sind Warntests nicht nur technische Prüfungen, sondern ein Indikator für Resilienz. **Warntests, ebenso wie Übungen des Katastrophenschutz, wirken als kognitives Training unter realen Bedingungen. Je häufiger Abläufe bewusst durchgespielt werden, desto schneller und sicherer erfolgt die Reaktion im Ernstfall.** Sie machen sichtbar, ob Systeme, Prozesse und Menschen tatsächlich miteinander verzahnt sind.

Dass diese Notwendigkeit heute stärker in den Fokus rückt, erklärt auch die Einführung des KRITIS-Dachgesetzes – weniger als Reaktion auf einen einzelnen Auslöser, sondern als Versuch, zumindest eine belastbare Mindestbasis an Vorsorge, Verantwortlichkeit und Widerstandsfähigkeit sicherzustellen.

Resilienz entsteht nicht durch Annahmen, sondern durch überprüfbare Vorbereitung. Die aktuellen Ergebnisse sind daher Teil einer Ursachenanalyse – und kein Alarmismus. ■

Stefan Vito Hiller,

Head of Blue Risk IQ
Senior Security Advisor
letstalk@blueriskiq.de

Wenn der Pegel sinkt, darf die Sicherheit nicht fallen

Der Wasserstand ist kein fixer Wert

In Häfen verändert er sich täglich – durch Wetter, Ebbe und Flut, Hochwasser oder betriebliche Einflüsse. Für den Hafenbetrieb ist das Routine. Für die Sicherheit jedoch oft eine stille Schwachstelle.

Was bei Normalpegel noch klar als geschlossene Hafenzufahrt gilt, kann bei Hoch- oder Niedrigwasser plötzlich neue Annäherungswege eröffnen. Kaimauern, Böschungen und Bauwerke verändern ihre Zugänglichkeit, Sichtachsen verschieben sich, technische Schutzlinien verlieren ihre definierte Lage. Genau dort, wo Land und Wasser ineinander übergehen, entstehen Zonen, die sicherheitsseitig schwer zu fassen sind – und deshalb besonders relevant.

Für KRITIS-Betreiber, Hafenbehörden und **ISPS-pflichtige Anlagen***[1] ist diese Dynamik kein theoretisches Szenario, sondern tägliche Realität. Die Verantwortung endet nicht am Kai, und sie endet auch nicht bei gleichbleibenden Umweltbedingungen.
Sicherheit muss dort wirken, wo sich Risiken tatsächlich entwickeln – und das ist in Hafenzufahrten ein beweglicher Raum.

Eine wirksame Perimetersicherung beginnt daher nicht mit Technik, sondern mit der richtigen Risikobetrachtung: *Welche Bereiche sind unter welchen Pegelständen sicherheitsrelevant?*
Welche Annäherungswege entstehen situativ?
Und wie lässt sich der ISPS-Code[1]* *so umsetzen, dass Schutzmaßnahmen auch dann greifen, wenn sich die Umweltbedingungen ändern?*

Die Antwort liegt in adaptiven Sicherheitskonzepten, die den Perimeter nicht als statische Linie verstehen, sondern als dynamische Schutzzone – intelligent geplant, regulatorisch sauber und technisch präzise umgesetzt.

Vom risikobasierten Ansatz zur adaptiven Technologie

Genau an diesem Punkt stößt klassische Perimetersensorik an ihre konzeptionellen Grenzen. Systeme, die auf fest definierten Linien, Höhen oder Reflexionsflächen basieren, verlieren ihre Wirksamkeit, sobald sich der Referenzraum verändert. In Hafenzufahrten mit variierenden Wasserständen führt dies entweder zu sicherheitsrelevanten Lücken oder zu einer hohen Anzahl von Fehlalarmen – beides ist im ISPS- und KRITIS-Umfeld nicht akzeptabel.

Der risikobasierte Ansatz verlangt daher nach einer Technologie, die den Überwachungsraum selbst erfassen und situativ neu bewerten kann. Hier setzen moderne 3D-LiDAR-Systeme von Blickfeld an.

Blickfeld-LiDAR erfasst den überwachten Bereich als dreidimensionalen Raum, unabhängig von Lichtverhältnissen, Wasserreflexionen oder festen Referenzlinien.

Der aktuelle Wasserstand wird nicht vorausgesetzt, sondern ist Bestandteil der Messung. Dadurch kann die sicherheitsrelevante Zone dynamisch definiert und bei Pegelveränderungen automatisch angepasst werden – ohne manuelle Nachjustierung und ohne Verlust der Detektionsqualität.

LIDAR-Punktwolken ersetzen die Kameralinse und ermöglichen datenschutzarme Erfassung.

* International Ship and Port Facility Security Code. Hafensicherheitstandards.

Für Hafenzufahrten bedeutet dies:

1.) Der Perimeter bleibt wirksam, auch wenn sich Wasserstände verändern;
2.) Annäherungen über Wasser, Uferbereiche und Übergangsbauwerke werden lageabhängig erkannt;
3.) Der Übergang zwischen Land- und Wasserseite wird als zusammenhängender Schutzraum überwacht.

Im Sinne des ISPS Codes entsteht so eine durchgängige, nachvollziehbare und auditfeste Überwachung sicherheitsrelevanter Bereiche – unabhängig von äußeren Bedingungen.

Mehrwert für See- und Binnenhäfen

Insbesondere Binnenhäfen von Kraftwerken sowie Energie- und Kohleumschlagplätzen profitieren von diesem Ansatz. Wassergebundene Annäherungspfade, die bislang schwer zu erfassen oder zu bewerten waren, lassen sich erstmals risikogerecht in die Perimetersicherung integrieren – ohne zusätzliche physische Barrieren oder komplexe Sonderlösungen.

Für Hafenbehörden und Betreiber erhöht sich damit die Resilienz der Gesamtanlage, für Leitstellen die Qualität der Alarme und für Auditoren die Nachvollziehbarkeit der Schutzmaßnahmen.

Für Betreiber kritischer Anlagen im Hochsicherheitsbereich entsteht ein klarer Mehrwert, denn die Technologie folgt der Risikoanalyse – nicht umgekehrt. Blickfeld-LiDAR wird so zum Werkzeug einer adaptiven Sicherheitsarchitektur, die regulatorische Anforderungen, Umweltbedingungen und operative Realität in Einklang bringt. ■

WSD permanent security

Bundesweiter Errichter von Blickfeld auf Basis unserer Risikoanalysen

Mehr Sicherheit an Schulen

Ob **kleine** oder **große** – Kinder sind unser kostbarstes Gut

Prävention und der Umgang mit extremen Bedrohungsszenarien sind leider Themen, die in der Vergangenheit oft unbeachtet blieben.
Doch wenn tragische Ereignisse geschehen, stellt sich unweigerlich die Frage: Was hätten wir tun können? Wie können wir uns und unsere Kinder besser schützen? Wie kann man Schüler*innen sowie Studierende besser auf solche Situationen vorbereiten?

Wir möchten Ihnen dabei helfen, Antworten auf diese Fragen zu finden. Aus diesem Grund haben wir ein speziell auf Ihre Bedürfnisse abgestimmtes Programm entwickelt. Denn auch wir sind Eltern, teilen Ihre Besorgnis und möchten unser Wissen nutzen, um gemeinsam für die Sicherheit unserer Kinder zu sorgen.

Seminar für Erzieher*innen und Lehrkräfte

In diesem Seminar vermitteln Ihnen erfahrene Spezialisten das Wesentliche zum Umgang mit aktuellen Bedrohungsszenarien – von Messerangriffen bis hin zu Amoktaten.

Sie erhalten praxisnahe Einblicke, wie solche Bedrohungen aussehen und lernen, wie Sie in akuten Situationen richtig reagieren können, um sich selbst und Ihre Schützlinge zu schützen. Diese Schulung bietet Ihnen konkrete Handlungsmöglichkeiten und Strategien zur Prävention.

Inhalte, die wir in einem 3-stündigen Seminar vermitteln:

- Erkennen von potenziellen Bedrohungslagen und deren Warnsignale;
- Notfallstrategien bei Messerangriffen und Amoktaten;
- Praktische Handlungsanweisungen und Deeskalationstechniken;
- Psychologische Erste Hilfe für betroffene Kinder und Erwachsene;
- Kommunikation und Zusammenarbeit mit Sicherheitsbehörden;
- Präventive Maßnahmen zur Sicherheit im Alltag.

GEFÄHRDUNG RECHTZEITIG ERKENNEN MEHR SICHERHEIT SCHAFFEN

Diese Präsenzschulung führen wir gerne in Ihrer gewohnten Umgebung vor Ort durch. So können Sie direkt auf Ihre spezifischen Gegebenheiten eingehen und sich optimal auf den Ernstfall vorbereiten. Dieses Seminar wird von Fachdozenten durchgeführt, die über fundiertes Wissen und praxisnahe Fähigkeiten verfügen, um auf Bedrohungssituationen sicher und besonnen reagieren zu können.

Kontaktieren Sie uns für weitere Informationen
letstalk@blueriskiq.de

Unser Ausbildungsleiter

Björn Erdmann ist Fachkraft (2007) und Meister (2017) für Schutz und Sicherheit und Fachkraft für Arbeitssicherheit. Seine in über 20 Jahren gesammelte und vielseitige Erfahrung sowie seine Tätigkeitsreferenzen zeichnen seine Sicht- und Herangehensweise zur Gefahrenerkennung und Findung von Lösungsmöglichkeiten in besonderem Maße aus.

Zusätzlich ist Herr Erdmann bei mehreren Kammern der „IHK“ und dem „TÜV Rheinland Nord“ als Trainer, Dozent und Prüfer tätig und besitzt eine Reihe weiterer Zusatzqualifikationen. Er ist ein wesentlicher Bestandteil unseres Risk Consultings und für die Durchführung von Schulungen verantwortlich.

BLUERISKIQ

Wir bringen Resilienz in jede Klasse.

Nicht KRITIS, aber für uns ein gesellschaftlich wichtiges Thema.

Unser Leistungspektrum richtet sich an Bildungseinrichtungen

- Spezialisiert auf die Durchführung von Risikoanalysen in Schulen
- Erstellung von maßgeschneiderten Sicherheitsstandards
- Erstellung von Sicherheitskonzepten für Amoktaten und Krisenmanagement
- Sensibilisierungsschulungen
- Sicherheitstechnik und Schutzraumkonzeption
- Spezialisiert auf die Absicherung von Chemieräumen in Schulen

Lösungen auf Basis der DIN VDE V 0827 bilden die Grundlage moderner Notfall- und Gefahren-Reaktions-Systeme (NGRS)

Gemeinsam mit GISBO, unserem starken und erfahrenen Partner im Alarmmanagement, setzen wir auf modernste Sicherheitstechnik.
GISBO hat eine leistungsfähige Softwarelösung entwickelt, die speziell für den Einsatz an Schulen konzipiert ist und höchste Anforderungen an Zuverlässigkeit, Bedienbarkeit und schnelle Reaktionszeiten erfüllt.

Das Notfall- und Gefahren-Reaktions-System ermöglicht eine flexible Nutzung für unterschiedliche Szenarien - etwa bei Bedrohungs oder Amokalarmen, stillen Alarmen oder Hilferufen. Die Systeme sind insbesondere für öffentliche Einrichtungen wie Schulen, Universitäten, Kindergärten, Behörden und vergleichbare Einrichtungen ausgelegt.

Kontaktieren Sie uns gerne für mehr Informationen rund um das Thema sichere Schulen.

Ihr Sicherheitspartner für KRITIS-Fragen

Resilienz entsteht, wenn Schutz-, Anpassungs- und Wiederherstellungsfähigkeiten eines Systems die Intensität, Dauer und Komplexität der jeweiligen Bedrohung übersteigen.

BLUERISKIQ

IMPRESSUM

Herausgeber
BLUE RISK IQ ist ein
spezialisierter Geschäftsbereich von
WSD permanent security GmbH
Neißestraße 1, 14513 Teltow

E-MAIL letstalk@blueriskiq.de
TELEFON 03328 - 432 444

#blue-risk-iq

www.blueriskiq.de