HANDLUNGSFÄHIG IM ERNSTFALL

Praxisleitfaden für Betreiber Kritischer Infrastrukturen



Resiliente Systeme, belastbare Prozesse und realitätsnahe Krisensimulationen bilden die Grundlage für Handlungsfähigkeit im Ernstfall.

HDC SOLUTIONS

Conducttr Germany

Handlungsfähigkeit wird zur strategischen und regulatorischen Aufgabe

Betreiber Kritischer Infrastrukturen stehen unter wachsendem Druck aufgrund einer zunehmend gezielten Bedrohungslage und verschärften regulatorischen Anforderungen. Dieser Leitfaden zeigt, wie sich Handlungsfähigkeit technisch und organisatorisch stärken lässt.

DIE BEDROHUNG

45.000

Haushalte tagelang ohne Strom

- 2026: Brandanschlag auf Kabelbrücke in Berlin
- längster Stromausfall der Nachkriegszeit
- Auswirkungen bis in Krankenhäuser und Mobilfunknetze

DIE PFLICHT

2

neue Gesetze in Kraft

- NIS2-Umsetzungsgesetz seit 12/2025
- KRITIS-Dachgesetz seit 03/2026
- erweiterte Anforderungen an Risiko-, Krisen- und Nachweismanagement

Mithilfe dieses Leitfadens können Sie ...

- Einflussfaktoren auf die Handlungsfähigkeit Ihrer Organisation bewerten
- technische und organisatorische Risiken gemeinsam statt isoliert betrachten
- Schwachstellen durch Analysen und Krisensimulationen früh erkennen
- Erkenntnisse gezielt in Krisenvorbereitung & Compliance-Nachweis übertragen
- konkrete Ansatzpunkte zur Weiterentwicklung Ihrer Resilienz ableiten

5 Minuten: Ihre Handlungsfelder auf einen Blick.
Ermitteln Sie mit dem Resilienz-Kompass auf Seite 11,
wo aktuell Ihr größter Hebel liegt.

Resilienz entsteht im Zusammenspiel aus Technik, Prozessen und Menschen. Dieser Leitfaden zeigt Ihnen, wo Sie ansetzen.

Krisen sind keine Ausnahmen mehr

Die Bedrohungslage ist längst konkret. Cyberangriffe, physische Angriffe und Ausfälle vernetzter Systeme zeigen, wie schnell einzelne Ereignisse Auswirkungen über die unmittelbar betroffene Infrastruktur hinaus entfalten können.

334.000

registrierte Cybercrime-Fälle in Deutschland (2025)

Cyberkriminalität erreicht ein neues Höchstniveau. Besonders Angriffe auf Unternehmen, Behörden und Betreiber Kritischer Infrastrukturen nehmen zu. Die tatsächliche Bedrohung dürfte aufgrund eines erheblichen Dunkelfelds deutlich höher liegen.

[Quelle: Bundeskriminalamt, Bundeslagebild Cybercrime 2025 (2026)]

36.706

DDoS-Angriffe 2025 im Netz der Deutschen Telekom

Überlastungsangriffe (Distributed Denial of Service, DDoS) zählen zu den bevorzugten Methoden organisierter Gruppen. Allein im Netz der Deutschen Telekom wurden 2025 rund 36.706 DDoS-Angriffe registriert – ein Anstieg von 25 % gegenüber dem Vorjahr. Besonders betroffen waren Behörden, Verwaltungen sowie Verkehrs- und Logistikunternehmen.

[Quelle: Bundeskriminalamt, Bundeslagebild Cybercrime 2025 (2026)]

45.000

Haushalte Anfang 2026 in Berlin ohne Strom

Am 3. Januar 2026 führte ein Brandanschlag auf eine Kabelbrücke am Teltowkanal zu einem großflächigen Stromausfall im Berliner Südwesten. Rund 45.000 Haushalte waren über vier Tage betroffen. Die Auswirkungen reichten weit über die Energieversorgung hinaus und trafen unter anderem Krankenhäuser, Mobilfunknetze und den Verkehr.

[Quelle: Stromnetz Berlin; Senatsverwaltung Berlin; Fraunhofer IEE (2026)]

Die eigentliche Herausforderung besteht darin, die Auswirkungen technischer, digitaler und organisatorischer Risiken auf das Gesamtsystem frühzeitig zu erkennen und zu verstehen.

08:17 Uhr. Derselbe Auslöser. Zwei Verläufe

Ausgehend vom Stromausfall in Berlin Anfang 2026 zeigt die folgende Zeitachse exemplarisch, worüber in den ersten Minuten einer Krise entschieden wird – und was Vorbereitung dabei verändert.

	OHNE VORBEREITUNG	MIT VORBEREITUNG
08:17 Uhr Erste Auswirkung	Die Notstromversorgung springt an. Aber niemand weiß, welche Bereiche wie lange abgesichert sind.	Notstrom übernimmt planmäßig. Abgesicherte Bereiche und verfügbare Autarkiezeit sind bekannt und dokumentiert.
08:29 Uhr Lage unklar	Meldungen laufen ungefiltert ein. Lokaler Defekt oder Großlage? Niemand ordnet ein.	Ein eingespielter Lageprozess greift. Meldungen werden zentral bewertet, ein erstes Lagebild entsteht.
08:46 Uhr Krisenstab	Der Krisenstab wird spät und unvollständig informiert. Rollen unklar, Rückfragen blockieren, Entscheidungen verzögern sich.	Der Krisenstab ist innerhalb Minuten arbeitsfähig. Rollen, Eskalations- und Entscheidungswege sind geübt, die Kommunikation läuft nach Plan.
09:15 Uhr Dynamik	Die Lage überholt die Organisation. Prioritäten ad hoc, Ressourcen doppelt gebunden, kritische Prozesse geraten ins Rutschen.	Prioritäten stehen, Ressourcen sind koordiniert, kritische Prozesse abgesichert. Die Organisation agiert, statt nur zu reagieren.
Später Ausblick	Man ringt noch mit der Frage „Wer entscheidet was?“ Ebenso mit der Kommunikation nach außen.	Der Fokus liegt bereits auf Wiederanlauf und Nachversorgung.

Was den Unterschied macht:

Vorbereitung schafft Klarheit über kritische Funktionen, verfügbare Ressourcen, Verantwortlichkeiten und Prioritäten – bevor unter Zeitdruck entschieden werden muss.

Wie handlungsfähig wäre Ihre Organisation in den ersten 60 Minuten?

Resilienz wird zur regulatorischen Anforderung

Mit NIS2 und dem KRITIS-Dachgesetz steigen die Anforderungen an Betreiber Kritischer Infrastrukturen. Technische und organisatorische Risiken müssen systematisch betrachtet und geeignete Maßnahmen nachvollziehbar umgesetzt werden.

NIS2

Digitale und organisatorische Resilienz

> Das NIS2-Umsetzungsgesetz verschärft die Anforderungen an das Risikomanagement und die Cybersicherheit betroffener Unternehmen. Gefordert werden unter anderem geeignete technische und organisatorische Maßnahmen sowie klare Verantwortlichkeiten.
> Geschäftsleitungen sind dabei zur Umsetzung und Überwachung der Risikomanagement-maßnahmen sowie zur regelmäßigen Schulung verpflichtet.

KRITIS-Dachgesetz

Physische und organisatorische Resilienz

> Das KRITIS-Dachgesetz erweitert den Blick auf die physische Widerstandsfähigkeit Kritischer Infrastrukturen. Betreiber müssen Risiken bewerten, geeignete Resilienzmaßnahmen vorsehen und ihre Krisenvorsorge systematisch weiterentwickeln.

§ 11 EnWG

Sektorspezifische Anforderungen an Energieinfrastrukturen

> Für Betreiber von Energieversorgungsnetzen ergänzt § 11 EnWG den regulatorischen Rahmen um sektorspezifische Anforderungen an einen sicheren und zuverlässigen Netzbetrieb sowie den Schutz der zugehörigen IT-Systeme.

Was bedeutet das für Betreiber?

Resilienz wird zur Managementaufgabe. Technische und organisatorische Risiken müssen gemeinsam betrachtet und Maßnahmen systematisch priorisiert werden.

Resilienz muss heute vorbereitet, überprüft und kontinuierlich weiterentwickelt werden.

Unterschiedliche Auslöser, ähnliche Muster

Krankenhaus, Flughafen, Kommune, Energieversorger oder Logistik: Kritische Infrastrukturen unterscheiden sich in Auftrag und technischer Ausprägung. Im Ernstfall folgen Ausfälle jedoch häufig ähnlichen Mustern: **Aus einer Einzelstörung kann durch technische und organisatorische Wechselwirkungen eine dynamische Lage entstehen.** Wer diese Zusammenhänge kennt, kann kritische Entwicklungen früher erkennen.



Krankenhaus — **Notstrom → Abhängigkeiten → Priorisierungsdruck**

> Notstrom sichert OP und Intensivversorgung zunächst ab. Mit abnehmender Autarkiezeit werden Abhängigkeiten von IT, Medizintechnik, Kühlung, Labor und Kommunikation zunehmend kritisch.



Flughafen — **Einzelstörung → Prozesskaskade → Betriebsstörung**

> Ein Ausfall betrifft neben der Energieversorgung auch Sicherheitskontrollen, Gepäckförderung, Vorfeld und digitale Abfertigungsprozesse. Einschränkungen einzelner Systeme können sich so auf weitere Betriebsprozesse ausweiten.



Kommune — **Parallele Ausfälle → Koordination → Priorisierung**

> Verwaltung, Leitstellen, Wasser- und Abwassersysteme, Verkehrssteuerung und Wärmeversorgung können gleichzeitig betroffen sein. Die Herausforderung liegt dann vor allem in der Koordination und Priorisierung kritischer Leistungen.



Energieversorger — **Mehrfachstörung → Kaskade → Wiederherstellung**

> Redundanzen können einzelne Ausfälle auffangen. Bei mehreren gleichzeitigen Störungen können jedoch auch diese an ihre Grenzen kommen und eine aufwendige Wiederherstellung erforderlich machen.



Logistik & Verkehr — **Knotenausfall → Rückstau → Folgeauswirkungen**

> Störungen bei Umschlag, Kühlketten, Disposition, IT oder Zugangskontrollen können einzelne Knoten lahmlegen. Daraus entstehen Rückstaus und weitere Auswirkungen entlang der Lieferkette.

Was die Sektoren verbindet:

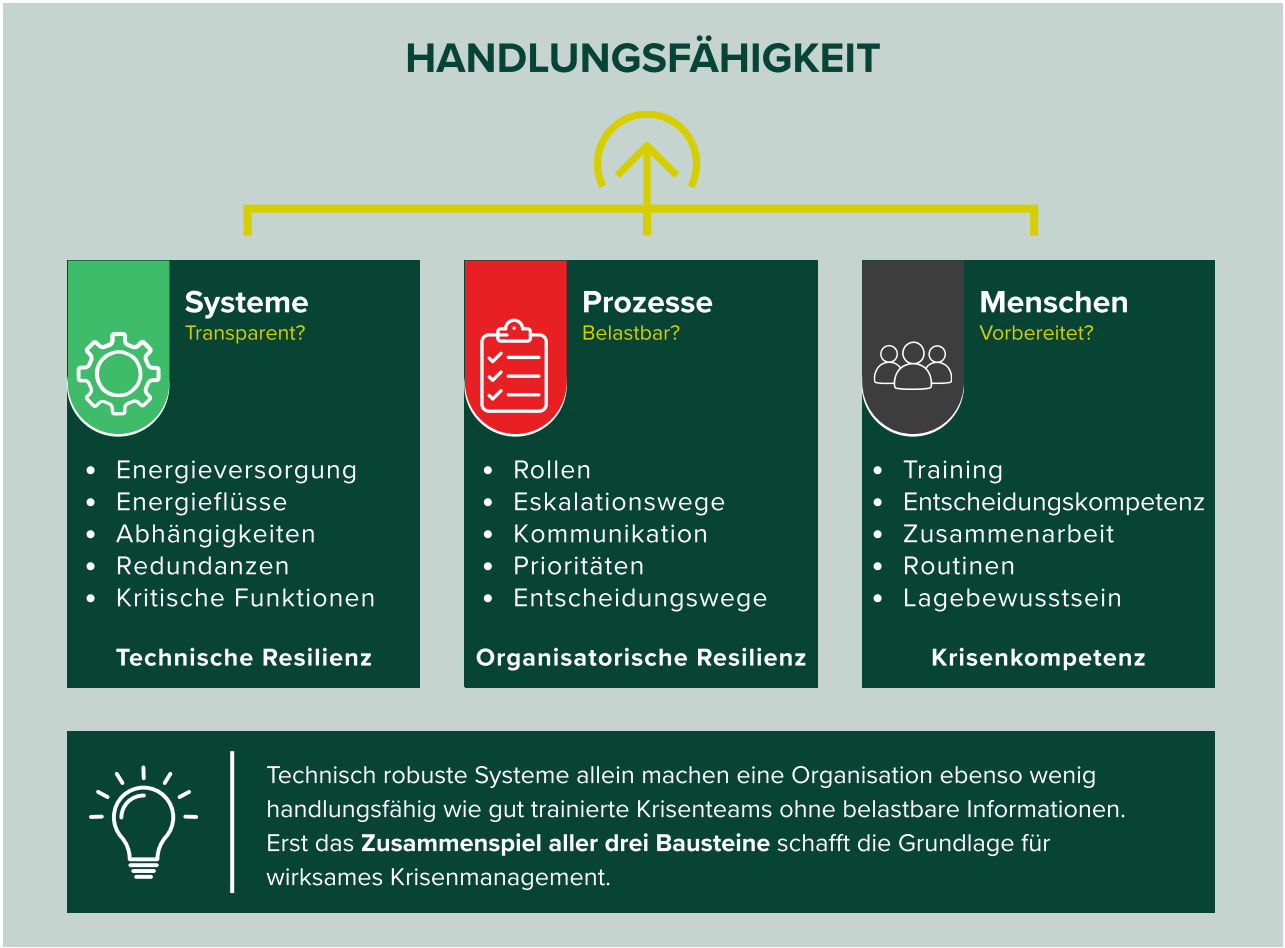
Zusammenhänge erkennen → Auswirkungen bewerten → kritische Funktionen priorisieren

Die Auslöser unterscheiden sich. Handlungsfähigkeit entscheidet sich im Zusammenspiel von Systemen, Prozessen und Menschen.

Handlungsfähigkeit entsteht im Zusammenspiel

Ob Stromausfall, Cyberangriff, Sabotage oder Naturereignis – für den Verlauf einer Krise ist weniger die Ursache ausschlaggebend als vielmehr das **Zusammenspiel von technischen Systemen, organisatorischen Prozessen und Menschen** im Ernstfall. Erst diese Wechselwirkung bestimmt, wie handlungsfähig Ihre Organisation bleibt.

Das Modell der Handlungsfähigkeit



Resilienz entsteht dort, wo technische und organisatorische Vorbereitung gemeinsam mit gut vorbereiteten Menschen ineinandergreifen.

Das Energiesystem als Ganzes verstehen

Energie ist der gemeinsame Nenner aller Kritischen Infrastrukturen. Energieerzeuger, Speicher, Verbraucher und Netze bilden gemeinsam ein integriertes Energiesystem. Wie resilient dieses Gesamtsystem ist, zeigt sich erst, wenn unterschiedliche Betriebs- und Ausfallszenarien betrachtet werden.

Energiesystem-Simulationen machen Auswirkungen analysierbar und ermöglichen es, technische Maßnahmen nach ihrer Wirksamkeit zu bewerten, zu priorisieren und die Energiearchitektur gezielt weiterzuentwickeln.

Sechs Dimensionen technischer Resilienz

Wie gut kennen Sie Ihr integriertes Energiesystem?

KRITISCHE FUNKTIONEN.
Wissen Sie, welche Funktionen im Ernstfall priorisiert versorgt werden müssen?

ABHÄNGIGKEITEN.
Wissen Sie, welche Komponenten für Ihr Gesamtsystem besonders kritisch sind?

TRANSPARENZ.
Wissen Sie, wie Energieflüsse und Wechselwirkungen Ihr Gesamtsystem beeinflussen?

AUTARKIE.
Wissen Sie, wie lange Ihr System unabhängig betrieben werden kann?

AUSFALLSICHERHEIT.
Wissen Sie, wie sich unterschiedliche Störungen auswirken?

PRIORITÄTEN.
Wissen Sie, welche technischen Maßnahmen Ihre Versorgungssicherheit am wirksamsten erhöhen?

Energiesystem-Simulationen schaffen Transparenz darüber, wie das Gesamtsystem unter unterschiedlichen Bedingungen reagiert und wo kritische Schwachstellen liegen.

Je besser eine Organisation ihr Energiesystem versteht, desto gezielter kann sie Risiken bewerten und technische Maßnahmen priorisieren.

Krisenreaktionsfähigkeit gezielt stärken

Technische Resilienz schafft die Grundlage für eine stabile Versorgung. Ob eine Organisation im Ernstfall handlungsfähig bleibt, hängt jedoch auch davon ab, wie Menschen, Prozesse und Entscheidungen unter Zeitdruck zusammenwirken.

Realitätsnahe Krisensimulationen zeigen, ob Rollen, Abläufe und Zusammenarbeit auch in dynamischen Lagen funktionieren und wo Verbesserungsbedarf besteht.

Sechs Dimensionen organisatorischer Resilienz

Wie gut kennen Sie die Krisenreaktionsfähigkeit Ihrer Organisation?

ROLLEN & VERANTWORTLICHKEITEN.
Wissen alle Beteiligten, welche Verantwortung sie im Ernstfall übernehmen?

ENTSCHEIDUNGSWEGE.
Sind Entscheidungswege auch unter Zeitdruck eindeutig geregelt?

KOMMUNIKATION.
Ist der Informationsfluss zwischen Krisenteam und relevanten Stakeholdern sichergestellt?

ZUSAMMENARBEIT.
Sind interne und externe Schnittstellen aufeinander abgestimmt?

TRAINING.
Werden Krisenszenarien regelmäßig realitätsnah geübt?

AUSWERTUNG & VERBESSERUNG.
Werden Schwachstellen aus Übungen systematisch ausgewertet und Maßnahmen abgeleitet?

Krisensimulationen schaffen ein kontrolliertes Umfeld, um Rollen, Entscheidungswege und Zusammenarbeit realitätsnah zu erproben. Erkenntnisse daraus führen zu konkreten Verbesserungen.

Je besser Organisationen ihre Abläufe trainieren, desto sicherer können sie auch unter Druck handlungsfähig bleiben.

Aus Erkenntnissen werden Maßnahmen

Handlungsfähigkeit entsteht Schritt für Schritt. Technische Risiken zu verstehen und Krisenszenarien vorzubereiten schaffen die Voraussetzung, Erkenntnisse anschließend in konkrete Maßnahmen zu überführen.

System verstehen & bewerten

- Das integrierte Energiesystem als Gesamtsystem verstehen
- Abhängigkeiten und Energieflüsse transparent machen
- Technische Szenarien simulieren und Auswirkungen bewerten

Ziel: Versorgungssicherheit erhöhen.

Szenarien vorbereiten

- Krisenszenarien unter realistischen Bedingungen trainieren
- Entscheidungen, Rollen und Zusammenarbeit testen
- Schwachstellen erkennen und konkrete Verbesserungsmaßnahmen ableiten

Ziel: Krisenreaktionsfähigkeit stärken.

Maßnahmen ableiten

- Technische & organisatorische Erkenntnisse zusammenführen
- Maßnahmen priorisieren
- Ressourcen & Investitionen gezielt einsetzen
- Resilienz kontinuierlich weiterentwickeln

Ziel: Handlungsfähigkeit stärken.

Technische und organisatorische Maßnahmen entfalten ihre größte Wirkung, wenn sie auf gemeinsamen Erkenntnissen basieren und systematisch aufeinander abgestimmt werden.

Beispiel: Zeigt die Energiesystem-Simulation eine begrenzte Autarkiezeit, kann dieses Ergebnis direkt in eine Krisensimulation einfließen – etwa als Zeitfenster für Priorisierung, Kommunikation und Nachversorgung.

Der nächste Schritt: herausfinden, wo für Ihre Organisation aktuell der größte Hebel liegt.

Wo liegt aktuell Ihr größter Hebel?

Technische und organisatorische Resilienz greifen ineinander. **Die folgenden zwölf Aussagen helfen Ihnen, beide Bereiche für Ihre Organisation zu reflektieren und zu erkennen, wo aktuell der größte Handlungsbedarf liegt.**

Bitte bewerten Sie jede Aussage mit Ja / Teilweise / Nein und notieren Sie sich Ihre Antworten. Entscheidend ist nicht die Anzahl der Ja-Antworten, sondern wo sich offene Handlungsfelder zeigen.

Technische Resilienz

KRITISCHE FUNKTIONEN
Prioritär zu versorgende Funktionen sind bekannt.
☐ Ja ☐ Teilweise ☐ Nein

ABHÄNGIGKEITEN
Kritische Abhängigkeiten im Energiesystem sind bekannt.
☐ Ja ☐ Teilweise ☐ Nein

TRANSPARENZ
Energieflüsse und Wechselwirkungen sind transparent.
☐ Ja ☐ Teilweise ☐ Nein

AUTARKIE
Die mögliche Dauer eines unabhängigen Betriebs ist bekannt.
☐ Ja ☐ Teilweise ☐ Nein

AUSFALLSICHERHEIT
Auswirkungen unterschiedlicher Störungen sind bekannt.
☐ Ja ☐ Teilweise ☐ Nein

PRIORITÄTEN
Technische Maßnahmen können nach ihrer Wirksamkeit priorisiert werden.
☐ Ja ☐ Teilweise ☐ Nein

Organisatorische Resilienz

ROLLEN & VERANTWORTUNG
Verantwortlichkeiten für den Ernstfall sind eindeutig geregelt.
☐ Ja ☐ Teilweise ☐ Nein

ENTSCHEIDUNGSWEGE
Entscheidungswege funktionieren auch unter Zeitdruck.
☐ Ja ☐ Teilweise ☐ Nein

KOMMUNIKATION
Der Informationsfluss zu relevanten Stakeholdern ist sichergestellt.
☐ Ja ☐ Teilweise ☐ Nein

ZUSAMMENARBEIT
Interne und externe Schnittstellen sind aufeinander abgestimmt.
☐ Ja ☐ Teilweise ☐ Nein

TRAINING
Krisenszenarien werden regelmäßig realitätsnah geübt.
☐ Ja ☐ Teilweise ☐ Nein

AUSWERTUNG & VERBESSERUNG
Erkenntnisse aus Übungen werden systematisch in Verbesserungen überführt.
☐ Ja ☐ Teilweise ☐ Nein

Wo können Sie jetzt ansetzen?

Betrachten Sie technische und organisatorische Resilienz zunächst getrennt. **Wo haben Sie häufiger „Teilweise“ oder „Nein“ angekreuzt?** Dort liegt aktuell Ihr größerer Handlungsbedarf. Entscheidend ist das Gesamtbild beider Bereiche.

TECHNISCHER SCHWERPUNKT

Ihr Energiesystem sollte systematisch analysiert und weiterentwickelt werden.

Offene Punkte auf der technischen Seite zeigen, dass kritische Funktionen, Wechselwirkungen oder Auswirkungen möglicher Ausfallszenarien noch nicht ausreichend bewertet werden können.

▶ **Ihr nächster Schritt:**
Analysieren Sie Ihr Gesamtsystem, bewerten Sie relevante Szenarien und priorisieren Sie technische Maßnahmen nach ihrer Wirksamkeit.

ORGANISATORISCHER SCHWERPUNKT

Ihre Krisenvorbereitung sollte stärker erprobt werden.

Offene Punkte auf der organisatorischen Seite zeigen Handlungsbedarf bei Rollen, Entscheidungswegen, Kommunikation oder Zusammenarbeit.

▶ **Ihr nächster Schritt:**
Trainieren Sie relevante Krisenszenarien realitätsnah und prüfen Sie, welche Abläufe auch unter Zeitdruck funktionieren.

HANDLUNGSFELDER IN BEIDEN BEREICHEN

Technische & organisatorische Resilienz gemeinsam weiterentwickeln.

Zeigen sich auf beiden Seiten offene Punkte, sollten Erkenntnisse zusammengeführt und Maßnahmen gemeinsam priorisiert werden.

▶ **Ihr nächster Schritt:**
Starten Sie bei den für Ihre Handlungsfähigkeit kritischsten Funktionen und verbinden Sie technische Analysen mit realitätsnahen Krisenszenarien.

Der Resilienz-Kompass zeigt, wo aktuell die größten Hebel liegen.
Jetzt gilt es, die richtigen Prioritäten abzuleiten.

Vom Handlungsfeld zum nächsten Schritt

Je nachdem, wo Ihr größter Hebel liegt, unterscheiden sich auch die nächsten Schritte. Technische Analyse und organisatorische Krisenvorbereitung können dabei gezielt ansetzen – einzeln oder im Zusammenspiel.

HDC Solutions

Technische Resilienz verstehen und weiterentwickeln

Unterstützung bei:

- Analyse integrierter Energiesysteme
- Simulation von Betriebs- und Ausfallszenarien
- Bewertung technischer Risiken und Abhängigkeiten
- Entwicklung resilienter Energiearchitekturen
- Priorisierung technischer Maßnahmen

Resilienz umfassender einordnen
Vertiefen Sie Ihre Standortbestimmung mit der **HDC Resilienz-Checkliste**.

Kostenlos herunterladen

hdc-solutions.de/checkliste-energiesicherheit

Conducttr

Organisatorische Resilienz trainieren und stärken

Unterstützung bei:

- maßgeschneiderten, realitätsnahen Krisensimulationen
- Krisenstabs- und Entscheidungstrainings
- Übungen für Kommunikation und Zusammenarbeit
- Auswertung und kontinuierlicher Verbesserung
- Aufbau organisatorischer Krisenreaktionsfähigkeit

Krisenreaktionsfähigkeit erproben
Erleben Sie in einer **Live-Simulation**, wie Ihr Team unter realen Bedingungen entscheidet.

Kostenlos anmelden

krisen.fit/hdc26

Ihr größter Hebel bestimmt den nächsten Schritt. Handlungsfähigkeit entsteht, wenn erkannte Lücken zu konkreten Maßnahmen führen.

Zwei Perspektiven. Ein gemeinsames Ziel.

HDC Solutions und Conducttr verbinden zwei Perspektiven auf Handlungsfähigkeit: die technische Resilienz integrierter Energiesysteme und die organisatorische Krisenvorbereitung. Gemeinsam unterstützen wir Betreiber Kritischer Infrastrukturen dabei, Risiken frühzeitig zu erkennen, Szenarien vorzubereiten und ihre Handlungsfähigkeit gezielt weiterzuentwickeln.

Technische Resilienz

HDC Solutions entwickelt resiliente Energiesysteme für Kritische Infrastrukturen und den Defence-Bereich. Mithilfe einer modularen Plattform zur Energiesystem-Simulation werden Risiken analysiert, Szenarien bewertet und technische Maßnahmen systematisch geplant.

HDC Solutions GmbH
Philipp Klein (CEO)
hdc-solutions.de
✉ contact@hdc-solutions.de

Gespräch vereinbaren:

hdc-solutions.de/kontakt

Organisatorische Resilienz

Conducttr unterstützt DAX-Unternehmen sowie Organisationen aus Cybersecurity und Defence dabei, ihre Krisenreaktionsfähigkeit gezielt zu stärken. Durch realitätsnahe Krisensimulationen werden Entscheidungen, Abläufe und Zusammenarbeit unter realistischen Bedingungen trainiert und kontinuierlich weiterentwickelt.

Conducttr Germany GmbH
David Peter-Gumbel (CEO)
conducttr.de
✉ info@conducttr.de

Kontakt aufnehmen:

conducttr.de/kontakt

Wir freuen uns darauf, Sie auf Ihrem Weg zu mehr Handlungsfähigkeit im Ernstfall zu begleiten.

Bildnachweis
Das Titelbild wurde mithilfe generativer KI erstellt.

© **2026 I HDC Solutions GmbH & Conducttr Germany GmbH.**
Alle Rechte vorbehalten.
Inhaltliche Änderungen vorbehalten.
Version 1.0 – Oktober 2026
Entstanden in gemeinsamer Zusammenarbeit von HDC Solutions und Conducttr.
Kontakt: hdc-solutions.de I conducttr.de