Die Notfallkommunikation

ein wesentlicher Bestandteil der NIS2-Richtlinie

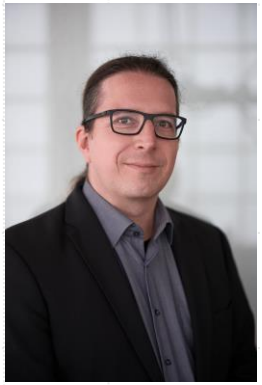
Benjamin Peter & Julian Skribek

ContinueComm GmbH

Kreissparkasse Schlüchtern

28. August 2024

Kurze Vorstellung:



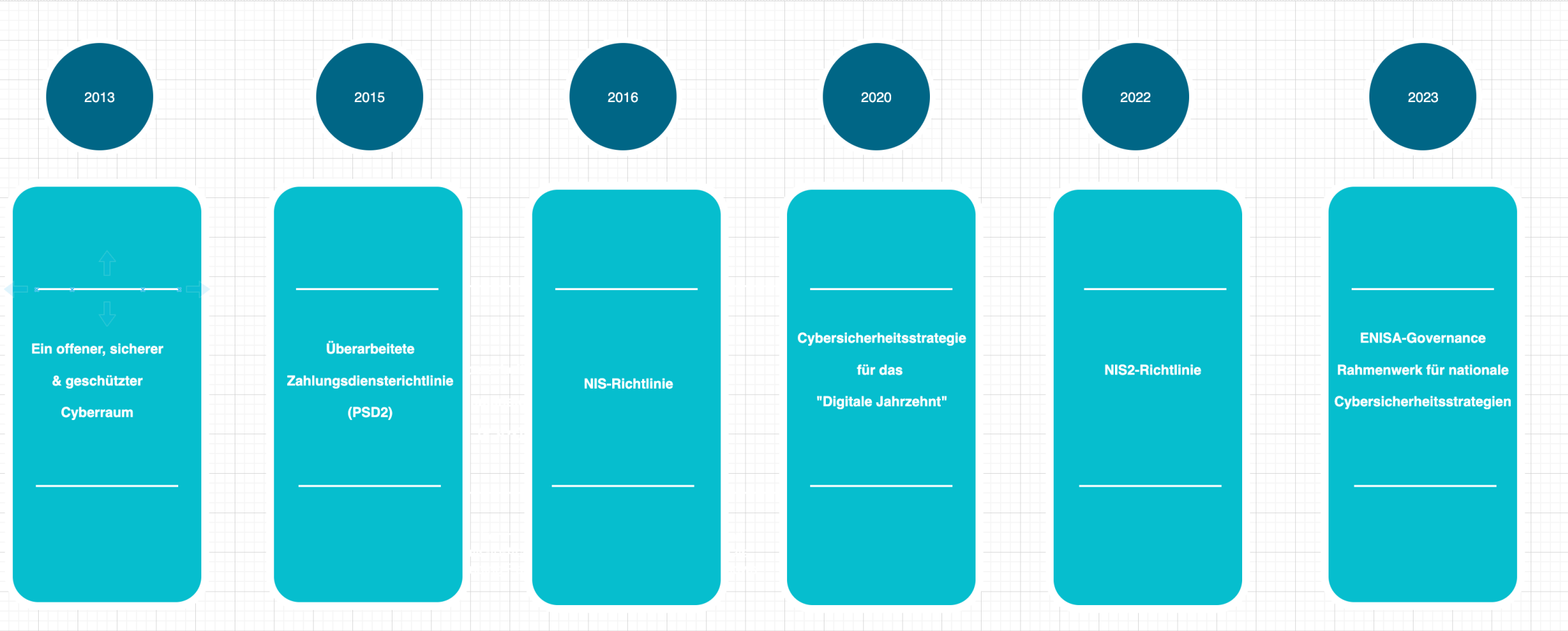
Benjamin Peter

Gründer ContinueComm GmbH

Julian Skribek

Gründer ContinueComm GmbH

Die Entwicklung von NIS zu NIS2



Wichtigste Änderungen zwischen der NIS & NIS2-Richtlinie

- Proaktiver Ansatz
- Benachrichtigung über Bedrohungen und Sicherheitsvorfälle
- Mehrstufiges Meldeverfahren
- Rückmeldungen und gewonnen Erkenntnisse
- Bedrohungsdaten und Informationsaustausch
- Ausweitung der Meldepflicht
- Meldeinstrumente
- Herausforderungen für nationale Behörden

NIS2 - Sind Sie betroffen?

Wesentliche & wichtige Einrichtungen

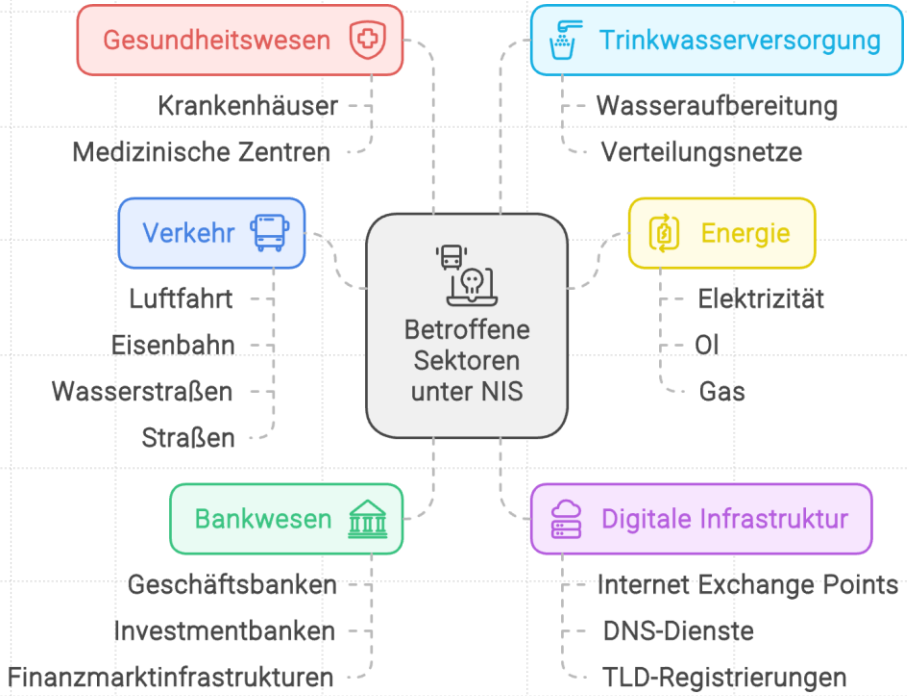
1

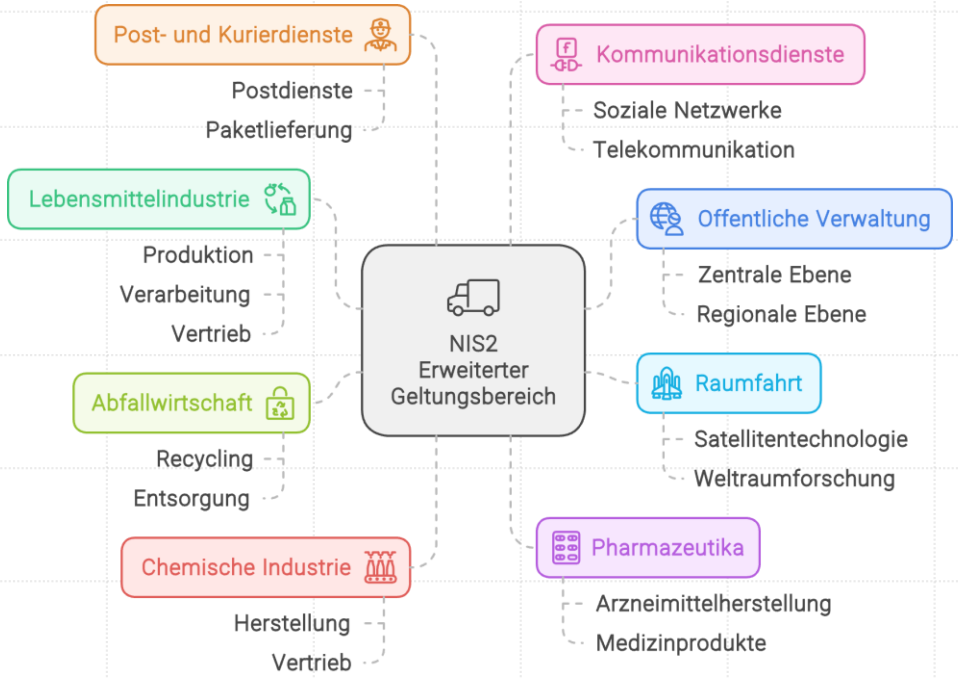
Wesentliche Einrichtungen sind große Organisationen in hochkritischen Sektoren gemäß der Definition im Anhang der NIS-2-Richtlinie. Sie beschäftigen mindestens 250 Personen, haben einen Jahresumsatz von über 50 Millionen Euro oder eine Jahresbilanzsumme von mindestens 43 Millionen Euro.

2

Wichtige Einrichtungen sind mittelgroße Unternehmen in hochkritischen Sektoren (Anhang I) sowie bestimmte große oder mittelgroße Unternehmen in spezifizierten Sektoren (Anhang II) der NIS-2-Richtlinie, die nicht als wesentliche Einrichtungen gelten. Mittelgroße Unternehmen haben mindestens 50 Beschäftigte oder einen Jahresumsatz bzw. eine Jahresbilanzsumme von 10 Millionen Euro oder mehr, jedoch nicht mehr als 250 Beschäftigte und einen Jahresumsatz von höchstens 50 Millionen Euro oder eine Bilanzsumme von 43 Millionen Euro.

Erweiterter Anwendungsbereich der NIS2-Richtlinie





NIS

NIS2

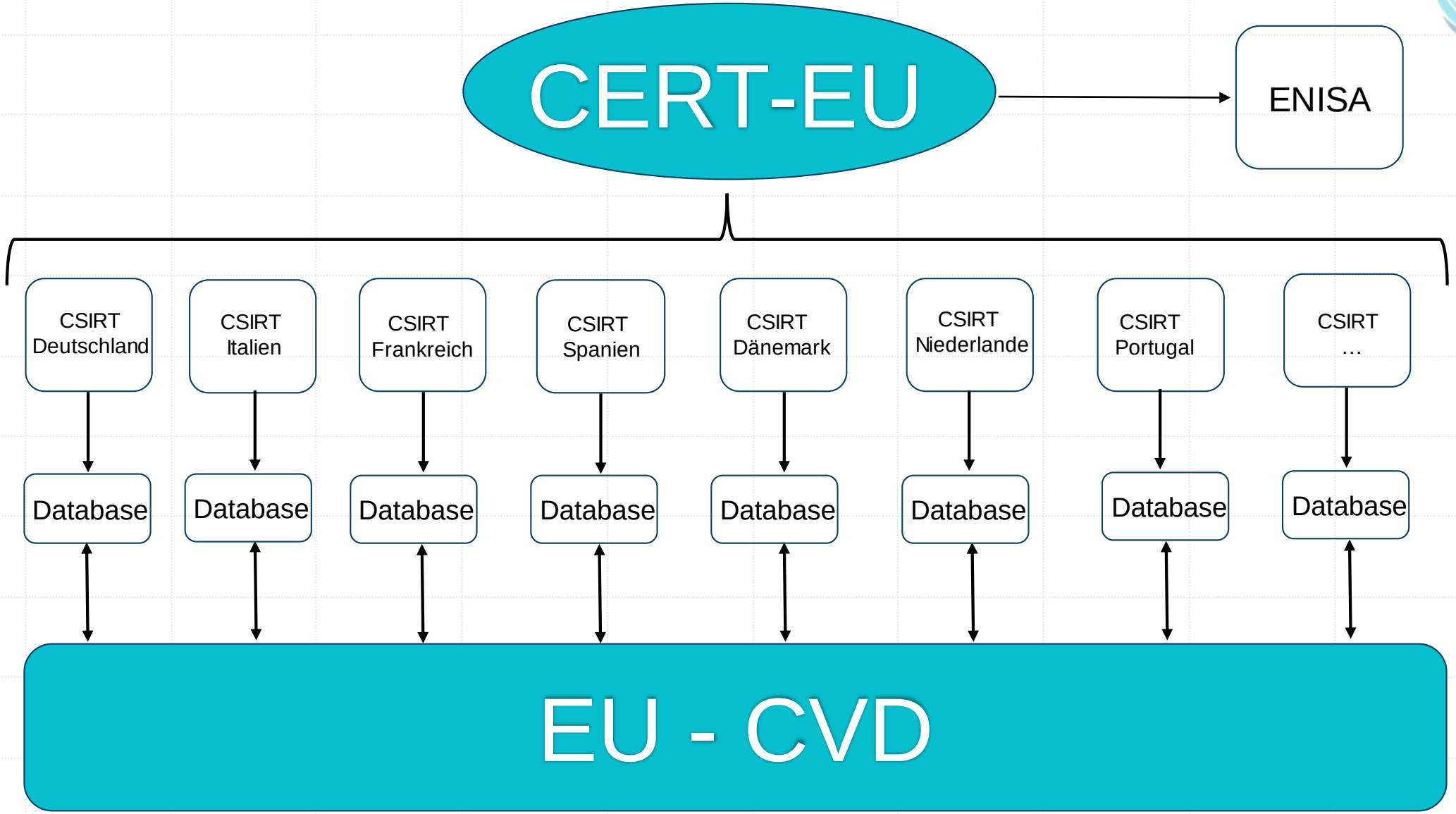
Geldbußen

Wesentliche Einrichtungen können mit Geldbußen von bis zu mindestens 10 Millionen Euro oder bis zu mindestens 2 % des weltweiten Jahresumsatzes des Unternehmens, dem die Einrichtung angehört, im vorhergehenden Geschäftsjahr belegt werden, je nachdem, welcher Betrag höher ist.	**Wichtige Einrichtungen können mit Geldbußen von bis zu mindestens 7 Millionen Euro oder bis zu mindestens 1,4 % des weltweiten Jahresumsatzes des Unternehmens, dem die Einrichtung angehört, im vorhergehenden Geschäftsjahr belegt werden, je nachdem, welcher Betrag höher ist.**

Für den öffentlichen Sektor können die nationalen Gesetze zur Umsetzung der Richtlinie vorsehen, dass Geldbußen auf öffentliche Verwaltungseinrichtungen nicht anwendbar sind. Andere Sanktionen als Geldbußen bleiben jedoch weiterhin möglich.

Die Mitgliedstaaten können zudem die Verhängung von Zwangsgeldern gegen wesentliche oder wichtige Einrichtungen zulassen. Diese Zwangsgelder dienen der Durchsetzung der Richtlinie, indem sie die betroffene Einrichtung verpflichten, festgestellte Verstöße gemäß der Entscheidung der zuständigen Behörde zu beheben.

Aufbau einer European Vulnerability Database



Überblick über die Anforderungen der NIS2-Richtlinie

Effektive Maßnahmen zum Risikomanagement in der Cybersicherheit müssen proportional zu den Risiken sein, denen wesentliche oder wichtige Einrichtungen ausgesetzt sind und den möglichen Auswirkungen von Sicherheitsvorfällen auf Gesellschaft und Wirtschaft Rechnung tragen.
Bei der Entwicklung von Strategien für das Management von Cybersicherheitsrisiken in solchen Einrichtungen ist es entscheidend, ihre unterschiedlichen Risikoprofile zu berücksichtigen, die eine Vielzahl von Faktoren umfassen, darunter:

- **Die Kritikalität der Einrichtung**
- **Das Ausmaß der Risikoexposition der Einrichtung**
- **Die Größe der Einrichtung**
- **Die Wahrscheinlichkeit des Auftretens von Sicherheitsvorfällen**
- **Die Schwere der Sicherheitsvorfälle**
- **Gesellschaftliche und wirtschaftliche Auswirkungen von Sicherheitsvorfällen**

Zuständige Behörden und zentrale Anlaufstelle

Die Mitgliedstaaten sind verpflichtet, Behörden zu benennen, die für Cybersicherheit und Aufsichtsaufgaben verantwortlich sind.

Darüber hinaus müssen sie eine zentrale Anlaufstelle einrichten, die den Austausch und die Kommunikation mit anderen Mitgliedstaaten und relevanten Behörden koordiniert.

Diese Behörden überwachen die Umsetzung der Richtlinie, fördern die Zusammenarbeit und müssen über ausreichende Ressourcen verfügen. Die Mitgliedstaaten sind zudem verpflichtet, die Europäische Kommission unverzüglich über die Identität ihrer zuständigen Behörden zu informieren.

Gemäß Artikel 9 der NIS2-Richtlinie, der nationale Rahmen für das Cyberkrisenmanagement betrifft, sind die Mitgliedstaaten für folgende Aufgaben verantwortlich:

- Die Benennung oder Einrichtung von Behörden, die für die Aufsicht über das Management von großangelegten Cybersicherheitsvorfällen und kritischen Situationen zuständig sind, und die als Behörde für das Cyberkrisenmanagement bezeichnet werden.

- Die Sicherstellung, dass diese Behörden über ausreichende Ressourcen verfügen, um ihre Aufgaben effektiv und kompetent zu erfüllen.

- Die Ausrichtung dieser Behörden am bestehenden Rahmen für das nationale Krisenmanagement.

- Die klare Festlegung, welche dieser Behörden als Koordinator für das Management von großangelegten Cybersicherheitsvorfällen und Krisen fungiert, insbesondere wenn mehrere Behörden benannt oder eingerichtet werden.

- Die Identifikation von Kapazitäten, Mitteln und Verfahren, die im Krisenfall gemäß dieser Richtlinie eingesetzt werden können.

- Die Erstellung eines umfassenden nationalen Plans zur Bewältigung erheblicher Cybersicherheitsvorfälle und Krisen, der die Ziele, Verantwortlichkeiten der Behörden, Krisenmanagementverfahren, Integration in den nationalen Krisenrahmen, Informationsaustausch, Vorsorgemaßnahmen, relevante Akteure und Regelungen für eine koordinierte Reaktion festlegt.

Computer-Notfallteams (CSIRTs):

Gemäß Artikel 10 der NIS2-Richtlinie ist jeder Mitgliedstaat verpflichtet, ein oder mehrere CSIRTs zu benennen oder einzurichten.
Diese CSIRTs können auch innerhalb einer zuständigen Behörde eingerichtet werden, wenn dies als sinnvoll erachtet wird.

Die Aufgaben der CSIRTs umfassen:

- Erfüllung der in Artikel 11 Absatz 1 festgelegten Anforderungen.
- Abdeckung der in den Anhängen I und II aufgeführten Sektoren, Teilsektoren und Arten von Einrichtungen.
- Bearbeitung von Sicherheitsvorfällen nach einem festgelegten Verfahren.

Die Mitgliedstaaten müssen sicherstellen, dass jedes CSIRT über ausreichende Ressourcen verfügt, um seine in Artikel 11 Absatz 3 beschriebenen Aufgaben wirksam zu erfüllen.

Berichtspflichten

Die NIS2-Richtlinie zielt darauf ab, das Meldesystem für Sicherheitsvorfälle zu optimieren, Fragmentierung zu vermeiden und die Berichterstattung durch folgende Maßnahmen zu verbessern:

Vorgeschlagene Reformen:
Vereinheitlichung der Schwellenwerte für die Meldung von Sicherheitsvorfällen.
Einführung eines gestaffelten Meldeplans, um eine umfassende Abdeckung sicherzustellen.

Meldeanforderungen:

Erstmeldung:
Innerhalb von 24 Stunden nach Feststellung eines erheblichen Sicherheitsvorfalls muss eine vorläufige Meldung erfolgen.

Offizielle Meldung:
Eine vollständige Meldung muss innerhalb von 72 Stunden nach dem Vorfall abgegeben werden.

Berichterstattung:
Auf Anfrage muss ein Zwischenbericht erstellt werden, und ein Abschlussbericht folgt zu einem späteren Zeitpunkt.

Interaktion mit der meldenden Einrichtung:
Die nationale zuständige Behörde oder das CSIRT nimmt Kontakt mit der meldenden Einrichtung auf, reagiert innerhalb von 24 Stunden auf die Frühwarnung und gibt Feedback.
Bei Bedarf erhalten Organisationen Anleitungen oder operative Beratung zur Umsetzung von Minderungsmaßnahmen.

Umgang mit der Cyberbedrohungslandschaft:
Die nationalen Behörden müssen auf neue Cyberbedrohungsszenarien vorbereitet sein.

Notwendige Maßnahmen nach NIS2

(Stand: Regierungsentwurf 22.07.2024)

Policies	Konzepte für Risikoanalyse & Sicherheit für Informationssysteme vorhanden
Vorfallsbewältigung	Erkennung, Analyse, Eindämmung und Reaktion auf Vorfälle (=Incident Response)
Business Continuity	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Vorfall, sowie Krisenmanagement
Supply Chain	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
Einkauf	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz -und Informationssystemen einschließlich Management und Offenlegung von Schwachstellen

Notwendige Maßnahmen nach NIS2

(Stand: Regierungsentwurf 22.07.2024)

Wirksamkeit	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
Cyberhygiene & Schulung der Mitarbeiter	Grundlegende Verfahren im Bereich der Cyberhygiene (z.B. Updates) und Schulungen im Bereich der Cybersicherheit
Kryptographie	Konzepte und Verfahren für den Einsatz von Kryptographie und gegebenfalls Verschlüsselung
Personal, Zugriffs-und Assetmanagement	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen
Authentifizierung	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung
Kommunikation	gesicherte Sprach-, Video -und Textkommunikation sowie gegebenfalls gesicherte Notfallkommunikationssysteme

Implementierung der NIS2-Richtlinie

Die Implementierung der NIS-2-Richtlinie erfordert besondere Aufmerksamkeit in drei kritischen Bereichen:

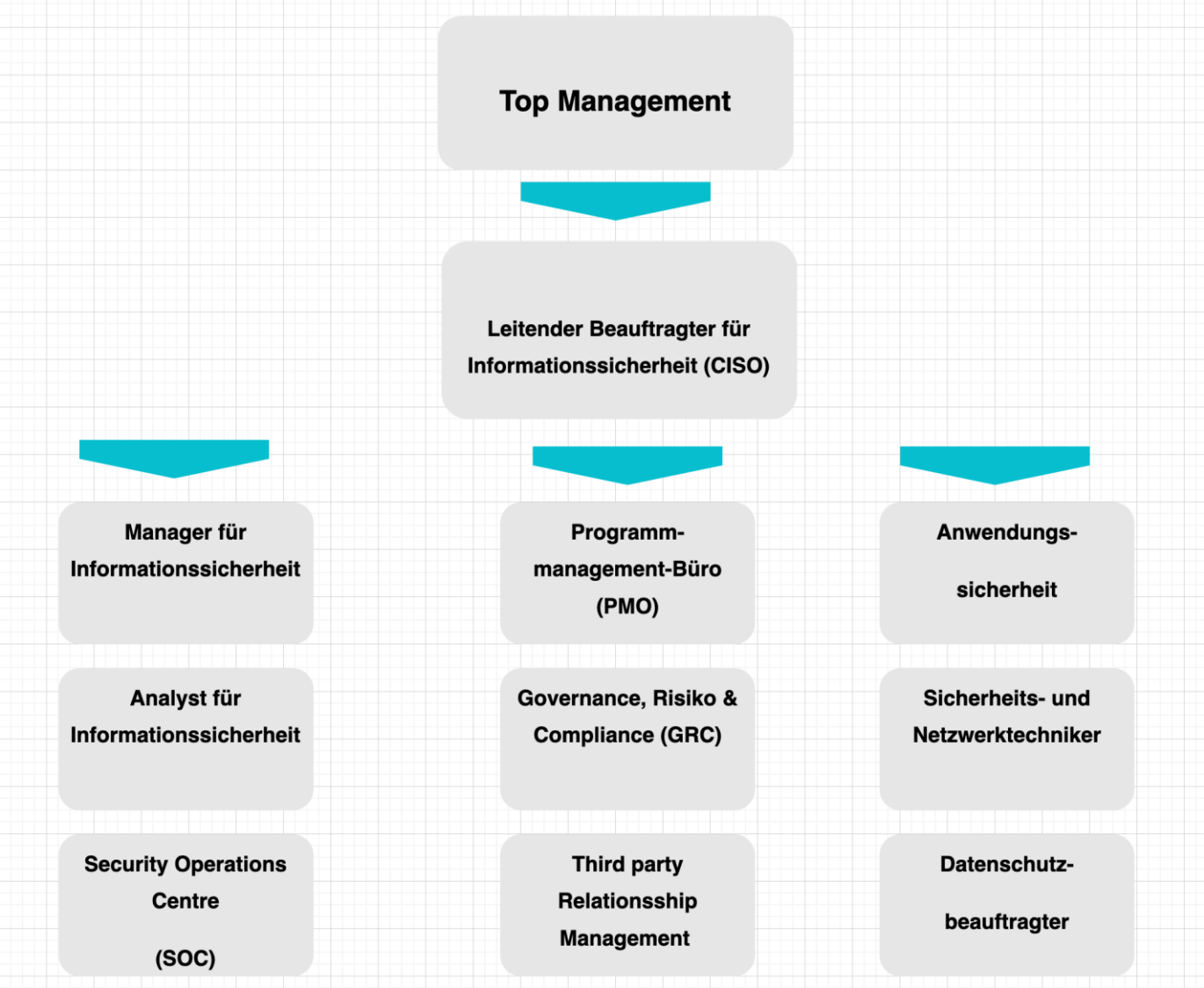
Cyber-Strategie und Governance:	Erkennung und Reaktion:	Infrastruktur- und Anwendungssicherheit:
• Verstärkung der Maßnahmen im Informationssicherheitsmanagement	• Stärkung der Reaktionsfähigkeit auf Sicherheitsvorfälle zur schnellen Bewältigung von Cybervorfällen	• Einführung fortschrittlicher Maßnahmen zur Sicherung der Infrastruktur und des Netzwerks der Organisation
• Förderung einer Sensibilisierungskultur und Durchführung umfassender Schulungsprogramme	• Gewährleistung zeitnaher und präziser Verfahren zur Meldung von Sicherheitsvorfällen	• Schwerpunkt auf sicheren Entwicklungspraktiken für Anwendungen und Software
• Einrichtung eines robusten Cyberrisikomanagements sowie von Protokollen zur Einhaltung von Vorschriften	• Entwicklung umfassender Strategien für die Aufrechterhaltung der Betriebsfähigkeit und das Krisenmanagement	• Optimierung der Identitäts- und Zugriffskontrollmechanismen
		• Sorgfältige Verwaltung von Risiken im Zusammenhang mit Drittparteibeziehungen

Die Geschäftsführung muss Treiber sein und haftet!

Das Top-Management muss die Cybersicherheitsrichtlinie formal unterstützen und genehmigen.

Die Richtlinie sollte von einem geeigneten Vertreter des Unternehmens, wie dem CEO, unterzeichnet werden!

Die Organisationsstruktur für Cybersicherheit mit einer CISO-Rolle



Die Rolle und Verantwortlichkeiten eines CISO

Der Chief Information Security Officer (CISO) ist eine Führungskraft auf Executive-Ebene, die für die Erfüllung der Anforderungen im Bereich Cybersicherheit verantwortlich ist.

Um einen kontinuierlichen Fokus auf Cybersicherheit zu gewährleisten, leitet der CISO ein Programm zur ständigen Verbesserung. Dies kann unter anderem durch folgende Maßnahmen erreicht werden:

- Entwicklung und Aufrechterhaltung von Richtlinien und Standards für Cybersicherheit
- Führung und Beratung bei der Implementierung von Cybersicherheitsverfahren und -richtlinien
- Aufbau einer umfassenden Cybersicherheitsstrategie, -architektur und eines Risikomanagementprozesses
- Budget- und Finanzmittelzuteilung für den Bereich Cybersicherheit
- Durchführung von Initiativen und Programmen zur Sensibilisierung für Cybersicherheit und Schulungen
- Proaktive Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
- Beratung zu bewährten Branchenpraktiken, einschließlich der Konfiguration von Infrastrukturen und Anwendungen

Die Rolle und Verantwortlichkeiten eines ISM

Der Informationssicherheitsmanager ist verantwortlich für:

- Effektives Management und Koordination von Reaktionen auf Cybersicherheitsvorfälle und Anpassung an sich verändernde Bedrohungen und Schwachstellen.
- Festlegung und Einhaltung von Cybersicherheits-Protokollen und Richtlinien sowie deren kontinuierliche Pflege.
- Bereitstellung von fachkundiger Beratung zu den Cybersicherheitsrisiken, die sich aus Veränderungen in den geschäftlichen und operativen Bereichen eines Unternehmens ergeben.
- Überwachung des gesamten Lebenszyklus von Cybersicherheitsplattformen, einschließlich Design, Bereitstellung, Betrieb und Außerbetriebnahme.
- Sicherstellung der Verfügbarkeit, Kapazität und Leistung von Hardware und Anwendungen im Zusammenhang mit der Cybersicherheit.
- Unterstützung bei regulatorischen Compliance- und Assurance-Aktivitäten sowie effektives Management von erforderlichen Maßnahmen.
- Entwicklung eines umfassenden Rahmens von Metriken und Versicherungen zur Bewertung der Wirksamkeit von Kontrollen.
- Management und Überwachung der operativen Durchführung im Bereich der Cybersicherheit.

Cybersicherheitsbewusstsein

Cybersicherheitsbewusstsein, -bildung und -schulung sind entscheidend, um sicherzustellen, dass alle Mitarbeiter die Bedeutung des Datenschutzes verstehen und entsprechend handeln.

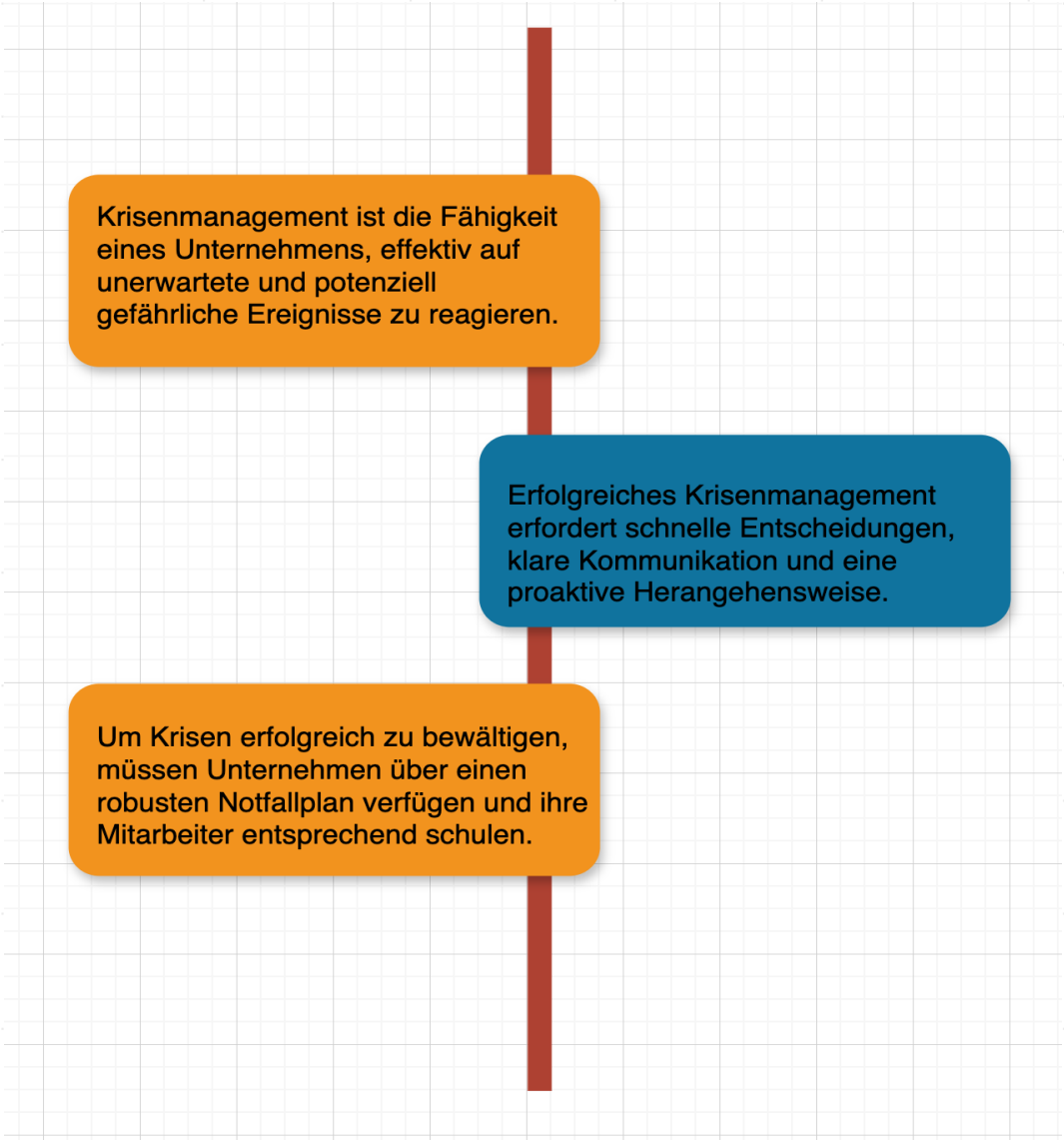
Ein effektives Cybersicherheitsprogramm muss sowohl technische als auch organisatorische Aspekte abdecken,
um die Mitarbeiter auf alle möglichen Bedrohungen vorzubereiten.

Ein Mitarbeiter, der nicht über ausreichendes Cybersicherheitsbewusstsein verfügt, kann ein Sicherheitsrisiko für das Unternehmen darstellen!

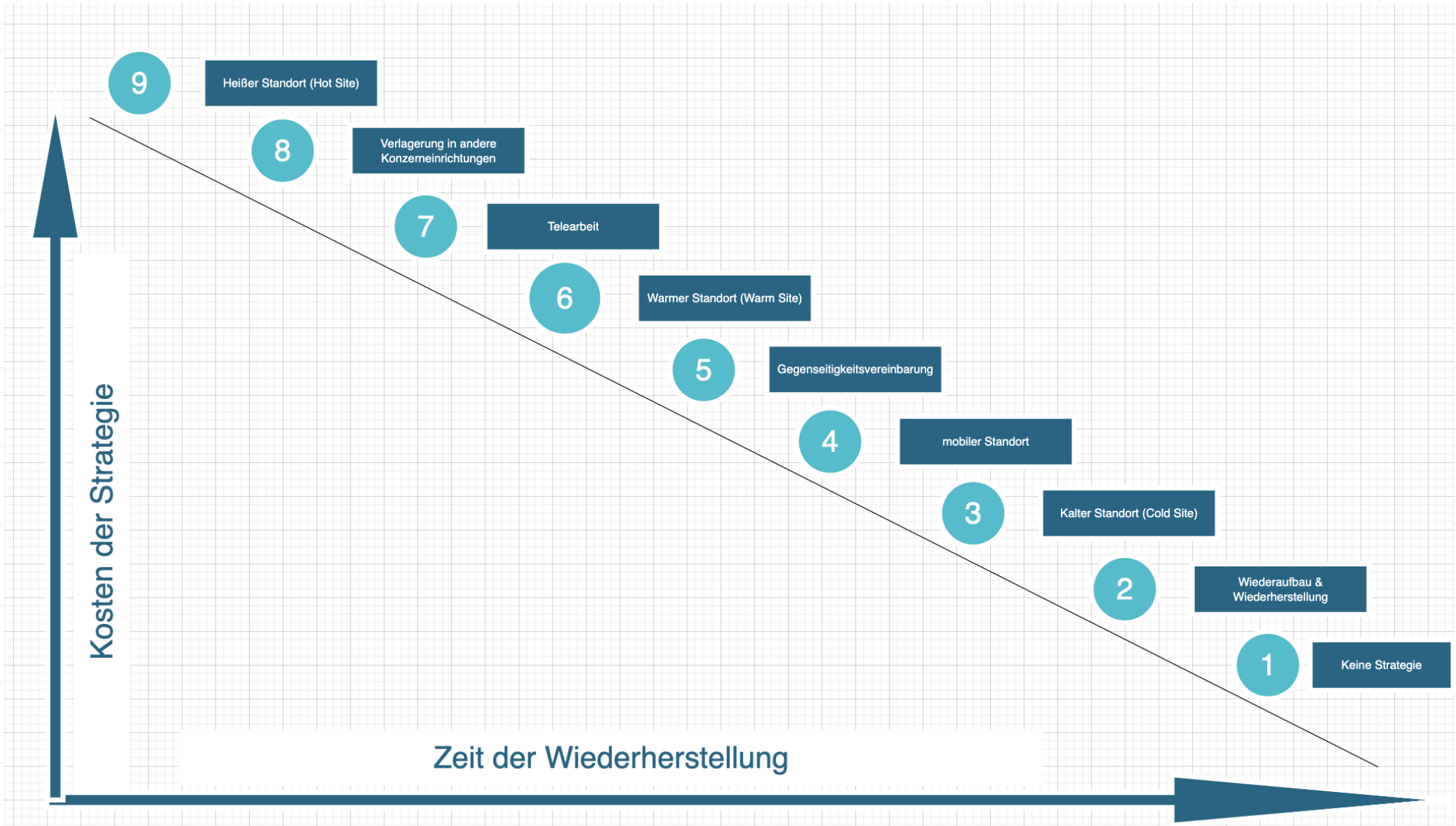
Planen und Vorbereiten

- Eine umfassende Cybersicherheits-Notfallplan entwickeln und vom Top-Management genehmigen.
- Die bestehenden Cybersicherheitsrichtlinien auf Unternehmens- und Systemebene aktualisieren.
- Einen detaillierten Cybersicherheits-Notfallplan erstellen.
- Ein Notfallreaktionsteam zusammenstellen.
- Kontakte zu internen und externen Organisationen aufbauen.
- Unterstützende Mechanismen für den Notfallplan implementieren.
- Sensibilisierungstrainings durchführen.
- Den Notfallplan testen.

Erfolgreiches Krisenmanagement



Ziele von Business Continuity Plänen (BCP)



Ziele von Business Continuity Plänen (BCP)

- Identifizierung von Notfallwiederherstellungsteams
- Bewertung von potentiellen Risiken
- Beschreibung der aktuellen Präventivmaßnahmen
- Bereitstellung schrittweiser Wiederherstellungsverfahren
- Angabe des Standorts von kritischen Werten und Daten
- Festlegung alternativer Standorte & Ressourcen
- Einrichtung der Notfallkommunikation
- Aufzeigen von Schwachstellen und Vorschlagen von Lösungen
- Erfüllung externer Anforderungen

Wer sind meine Kommunikationspartner im Krisenfall?

Ergebnis mangelnder Notfallkommunikation

Beispiele aus der nahen Vergangenheit

Wilken Software Group

KISTERS

UNIVERSITÄTS MEDIZIN FRANKFURT
GOETHE-UNIVERSITÄT

All4Labels
GLOBAL PACKAGING GROUP

twl

Technische Werke Ludwigshafen

CROWDSTRIKE

Stadtverwaltung Rodgau

NOTFALLTELEFONIE

Damit Sie im Notfall erreichbar bleiben und wichtigste Telefonate führen können, sollte für interne und externe Kontakte eine telefonische Erreichbarkeit sichergestellt werden.

VERSCHLÜSSELTE VIDEOKONFERENZEN

Organisieren Sie die ersten Maßnahmen mit Ihrem Krisenteam auch per Videokonferenz. Informieren Sie Ihre Kollegen in gewohnter Umgebung.

NOTFALL E-MAIL

E-Mail ist ein elementarer Baustein Ihres Notfallsystems.
Eine unabhängige E-Mail Kommunikation muss gegeben sein,
um alle Kommunikationspartner effektiv erreichen zu können.

NOTFALLDOMAIN / NOTFALLWEBSITE

Informieren Sie Ihre Kunden sofort mit einer vorbereiteten
Webseite über die Krisensituation und halten Sie diese auf
dem Laufenden.

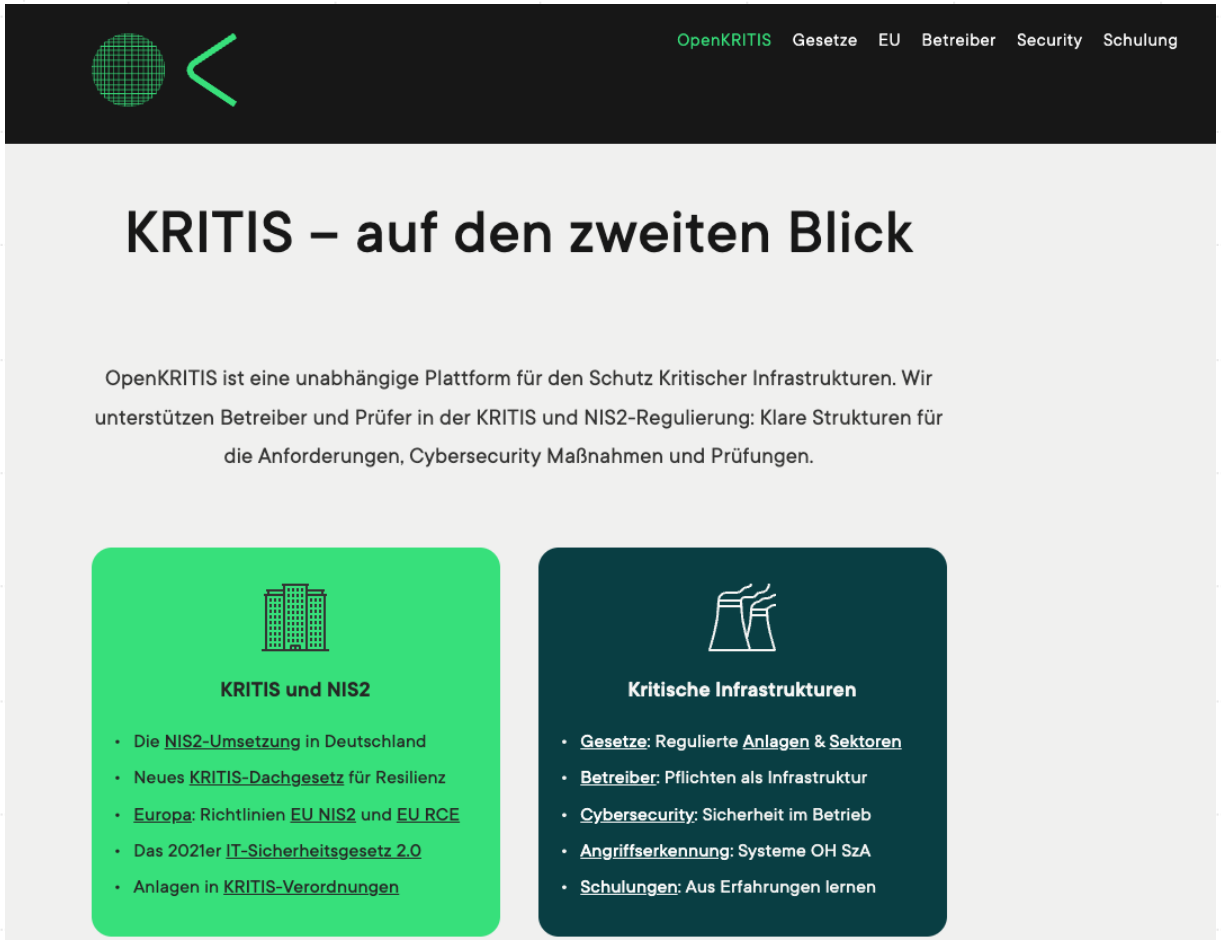
VERSCHLÜSSELTER NOTFALLCHAT

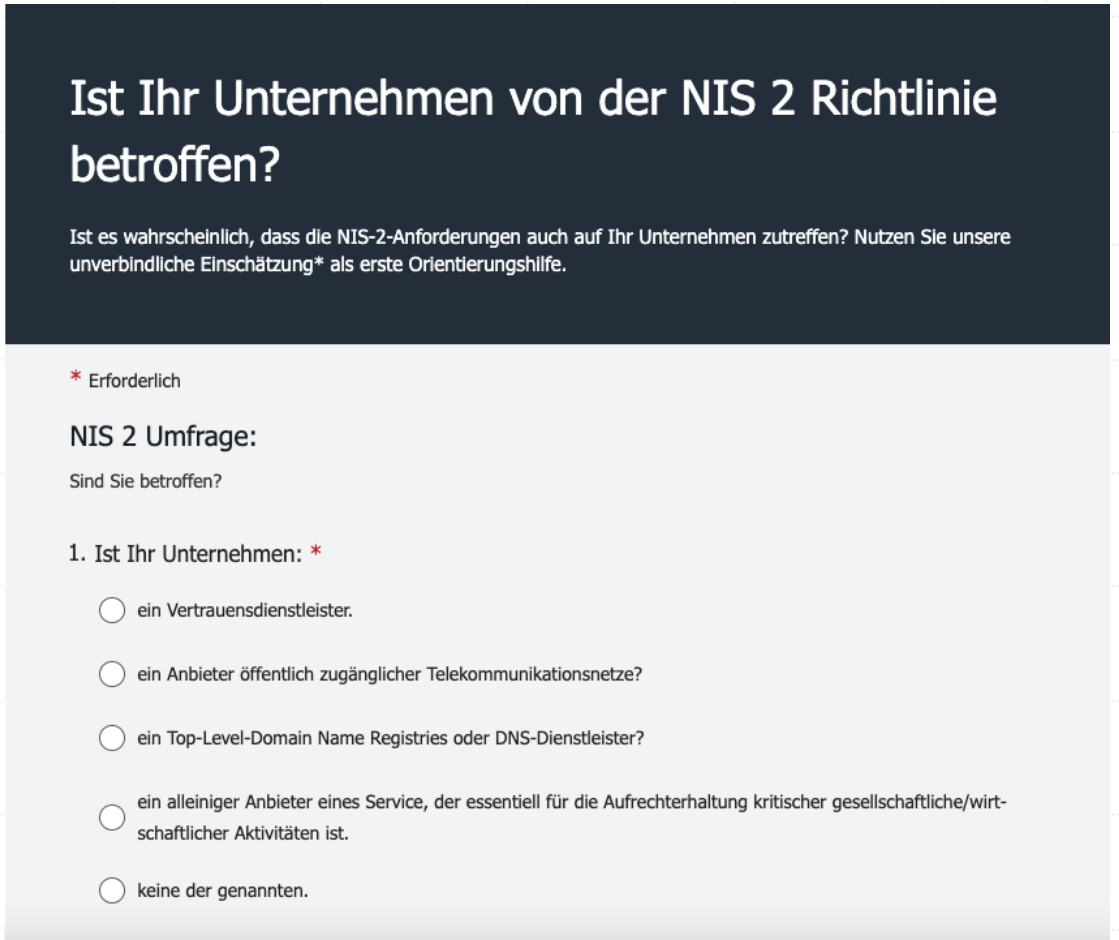
Kommunizieren Sie schnell, effizient, und direkt mit Ihren Beschäftigten und Entscheidern.

SECURE DATASTORE

Sichern Sie Ihre wichtigsten Daten, wie IP-Listen, Telefonlisten, Notfallpläne, usw. sicher und jederzeit verfügbar

Weitere Informationen unter www.openkritis.de





Wir freuen uns, dass Sie sich heute Abend die Zeit und das Interesse genommen haben, um mehr über NIS2 und Notfallkommunikation zu erfahren.

Gerne stehen wir für Fragen im Anschluss zur Verfügung!

VIELEN DANK!

kontakt@continuecomm.de

ContinueComm GmbH
Umgehungsstr. Nord 1
36381 Schlüchtern