primion

Strategisches Whitepaper für sicherheitsrelevante Behörden.

Handlungsfähigkeit in Krisensituationen

INHALT

Summary

Die nächste Entwicklungsstufe für die öffentliche Sicherheit ist die intelligente Verbindung vorhandener Systeme auf einer gemeinsamen Identitäts-, Daten- und Prozessebene.

Primion verbindet Zutrittskontrolle, Workforce Management und Critical Event Management zu einem integrierten Sicherheitsökosystem.

Gemeinsam lässt sich analysieren, wo Informationsbrüche entstehen und wie ein schrittweiser Umsetzungsplan zu mehr Transparenz, Koordination und Handlungsfähigkeit aussehen kann.

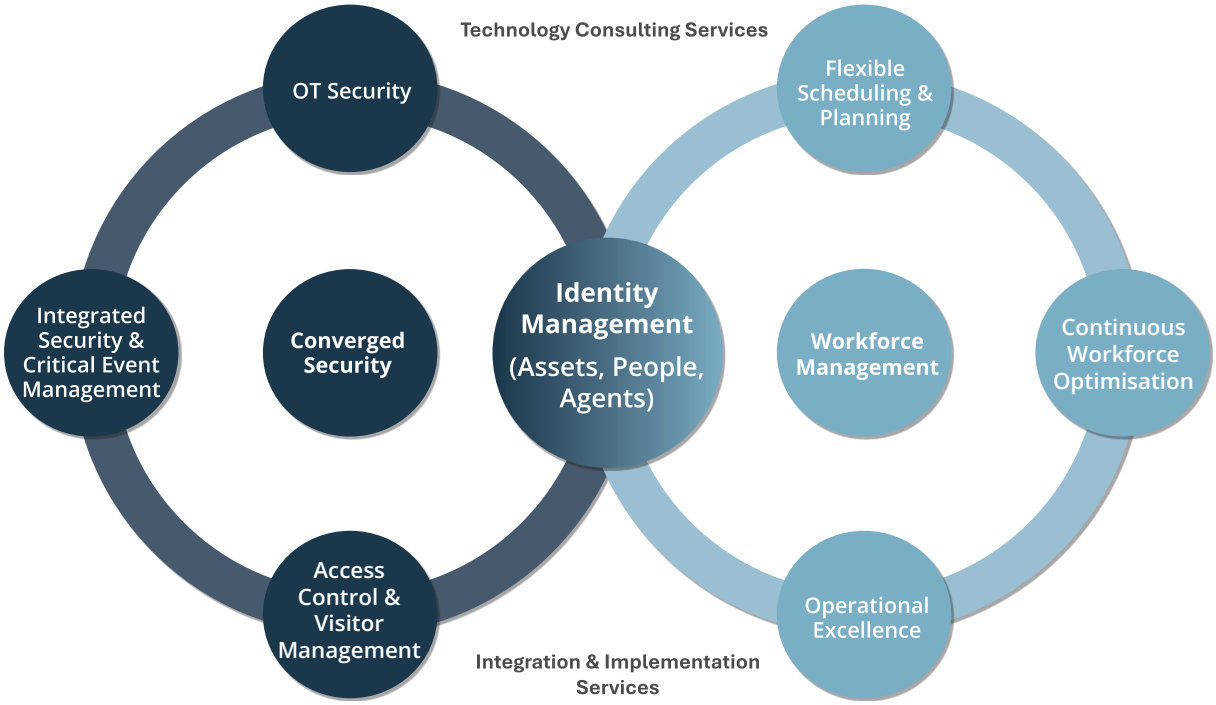
Die Herausforderung: Warum öffentliche Sicherheit an fehlender Koordination scheitern kann.

Wenn Stromnetze ausfallen, Verkehrswege blockiert sind und Kommunikationssysteme ausfallen, zählt jede Minute. Öffentliche Einrichtungen müssen diese als kritisch bewerteten Leistungen aufrechterhalten und in Minuten über das weitere Vorgehen entscheiden. Die dafür notwendigen Informationen sind in unterschiedlichen Systemen gespeichert und lassen sich häufig nicht in einem Gesamtüberblick darstellen. Die Systeme für die Zutrittskontrolle, Videoüberwachung, IT, Gebäudetechnik, Personalplanung und Notfallorganisation sowie das Alarmmanagement, liefern jeweils einzelne Ausschnitte, aber keinen Überblick. Solange die Technik funktioniert, diese Daten aber nicht zusammengeführt werden, bleibt das Gesamtbild unscharf. Das kann im Ernstfall Konsequenzen haben, weil keine konkreten Handlungsszenarien abgeleitet werden können.

Dieses Whitepaper beleuchtet, wie Informations- und Koordinationslücken entstehen können und bietet konkrete Impulse, um Sicherheitsarchitekturen besser zu vernetzen und die Handlungsfähigkeit in Krisensituationen zu stärken.

Lösungsansatz Konvergente Sicherheit

Konvergente Sicherheit verbindet Identitäten, Berechtigungen, Anwesenheit, Qualifikationen, Ereignisse und operative Abläufe. Verantwortliche erkennen schneller, was passiert, welche Bereiche betroffen sind, wer verfügbar ist und welche Maßnahmen greifen. Ereignisse werden nicht nur angezeigt, sondern im organisatorischen Kontext bewertet.



Durch den unterstützenden Einsatz von künstlicher Intelligenz können im System große Datenmengen vorsortiert, Muster erkannt und mögliche Entwicklungen simuliert werden. In sicherheitskritischen Umgebungen bleibt die Verantwortung jedoch beim Menschen. Empfehlungen müssen nachvollziehbar und korrigierbar sein und einem Audit standhalten.

Erfolgsfaktoren konvergenter Sicherheit

KLARHEIT	Ein gemeinsamer Informationsstand über Standorte, Personen und Ereignisse.
KOORDINATION	Definierte Verantwortlichkeiten, Eskalationen und Maßnahmen.
KONTINUITÄT	Kritische Leistungen auch unter Belastung aufrechterhalten.
VERTRAUEN	Entscheidungen transparent treffen und nachvollziehbar dokumentieren.

1. Entwicklung einer Krise

Wenn eine Störung eskaliert und Minuten entscheiden.

Angenommen, ein großflächiger Stromausfall betrifft mehrere öffentliche Standorte:
In den Krankenhäusern greifen Notfallpläne, die Verkehrssysteme melden Störungen und die Kommunikationsnetze brechen irgendwann zusammen. Der eingesetzte Krisenstab versucht die verfügbaren Kräfte zu koordinieren, doch noch sieht niemand das gesamte Lagebild, denn jedes System liefert unterschiedliche Informationen.

In solchen Situationen können sich Entscheidungszyklen drastisch verkürzen und Verantwortliche müssen innerhalb weniger Minuten wissen, welche Standorte betroffen sind, wer sich dort aufhält, welche Personen qualifiziert und einsatzbereit sind und welche Abhängigkeiten eine Störung auslösen kann. In komplexen Lagen stoßen herkömmliche Kommunikationswege und manuelle Tabellen schnell an Grenzen.

Die entscheidende Frage

Verfügt eine Organisation über Daten, aus denen sie im Krisenfall innerhalb weniger Minuten koordinierte Maßnahmen ableiten kann?

2. Strukturelle Herausforderung

Funktionierende Systeme brauchen ein vernetztes Zusammenspiel.

Wenn Informationen isoliert bleiben, entstehen operative Blindstellen, manuelle Abstimmungen verzögern die Reaktion und ein vollständiges Lagebild entsteht erst dann, wenn wertvolle Zeit verstrichen ist:

Im System für die **Zutrittskontrolle** sind die Berechtigungen hinterlegt. Diese liefern aber nicht automatisch Informationen über Qualifikation und aktuelle Verfügbarkeit.

Die **Videoüberwachung** und die **Sensorik** erkennen Ereignisse, können den personellen und betrieblichen Kontext jedoch nicht vollständig bewerten.

Das **Arbeitszeitmanagement** hat Informationen über verfügbare und qualifizierte Kräfte, aber nicht über die aktuelle Sicherheitslage.

Die **Krisenkommunikation** beginnt, nachdem Informationen aus unterschiedlichen Quellen manuell zusammengeführt wurden und damit vielleicht zu spät.

Jedes einzelne System liefert Daten für den jeweiligen Aufgabenbereich. Doch übergreifende Reaktionen geraten ins Stocken und kosten wertvolle Zeit. Öffentliche Sicherheit entsteht deshalb nicht allein durch leistungsfähige Technologien. Entscheidend ist die Verknüpfung zu einem gemeinsamen Lagebild, welches technische Ereignisse mit Personen, Rollen, Verantwortlichkeiten und definierten Maßnahmen in eine Beziehung stellt.

Ein zentrales Dashboard schafft Sichtbarkeit. Für eine koordinierte Reaktion müssen Ereignisse zusätzlich mit Rollen, Ressourcen und freigegebenen Abläufen verknüpft werden.

Grundsatz des Erfolgs: Vom Sehen zum Handeln

Eine Überwachung macht Ereignisse sichtbar. Orchestrierung geht einen Schritt weiter und sorgt dafür, dass die richtigen Personen die richtigen Maßnahmen einleiten und jede Entscheidung nachvollziehbar dokumentiert wird.

3. Unser Lösungsprinzip

Ein gemeinsames Lagebild schafft operative Klarheit.

Konvergente Sicherheit verbindet physische Sicherheit, digitale Sicherheit, Personalinformationen und operative Prozesse auf einer gemeinsamen Ebene.

Ein belastbares Lagebild muss mehr leisten als eine Karte mit Alarmen. Es bringt technische Signale mit dem organisatorischen Kontext zusammen und beantwortet sechs zentrale Fragen:

1
Was ist passiert?

2
Wo ist es passiert?

3
Wer ist betroffen?

4
Wer ist verfügbar?

5
Wer ist autorisiert?

6
Was muss jetzt geschehen?

Auf dieser Grundlage lassen sich vier Fähigkeiten aufbauen:

Echtzeittransparenz über Anwesenheit, Autorisierung, Dienststatus und Qualifikation.

Ein einheitliches Identitäts- und Berechtigungsmanagement für Mitarbeitende, Besucher und externe Kräfte.

Die Verbindung physischer, digitaler und operativer Umgebungen.

Vordefinierte Reaktionen mit automatisierter Benachrichtigung, Genehmigung und automatisierter Dokumentation in Echtzeit.

Mit der wachsenden Zahl gesetzlicher Vorgaben – darunter NIS-2, der Cybersecurity Act und arbeitsrechtliche Anforderungen – steigt auch die Komplexität der Dokumentation und der notwendigen Prüfpfade. Primion automatisiert diese Compliance Prozesse und erstellt revisionssichere Nachweise für die behördliche Aufsicht. Das kann dazu beitragen, Regelverstöße frühzeitig zu erkennen und den Dokumentationsaufwand zu reduzieren. Bereits installierte Systeme müssen dafür nicht ersetzt werden. Diese behalten ihre Aufgaben und werden über offene Schnittstellen in eine gemeinsame Sicht eingebunden. Das schützt Investitionen und ermöglicht eine schrittweise Modernisierung.

Ereignisebenen und Handlungsfähigkeit

EBENE	BEITRAG ZUR HANDLUNGSFÄHIGKEIT
1. Ereignisebene	Daten aus der kritischen Infrastruktur, Leitstellen, Telekommunikation, Gesundheitswesen und weiteren Quellen werden korreliert und zu einem gemeinsamen Lagebild verdichtet. Bestehende Systeme bleiben bestehen.
2. Planungs- und Simulationsebene	Mögliche Kaskaden werden berechnet und Handlungsoptionen mit Wahrscheinlichkeiten, Vertrauensbereichen und wesentlichen Einflussfaktoren dargestellt. Unsicherheit muss sichtbar bleiben.
3. Ausführungsebene	Qualifizierte, vorab registrierte Kräfte können abhängig von Standort, Verfügbarkeit und Aufgabe mobilisiert werden. Jeder operative Plan unterliegt einer menschlichen Freigabe.

Der besondere Wert dieses Modells liegt in der Verbindung von Erkennen, Vorausschauen und Handeln. Es macht nicht nur sichtbar, was gerade geschieht, sondern unterstützt die Frage, wie sich eine Lage entwickeln könnte und welche Ressourcen für eine wirksame Reaktion benötigt werden.

Erfolgsfaktor Mensch

Der Mensch ist in einer Krise gleichzeitig Betroffener, Helfer, Entscheider und Teil der Gemeinschaft. Sein Verhalten kann entscheidend dafür sein, wie gut eine Gesellschaft eine Krise übersteht.

Technologie kann Informationen bündeln, Entwicklungen analysieren und mögliche Maßnahmen vorschlagen. Die Einordnung einer komplexen Lage, die Abwägung unterschiedlicher Interessen und die Verantwortung für Entscheidungen bleiben jedoch menschliche Aufgaben. Damit Menschen unter hohem Zeitdruck und in hoher Verantwortung sicher handeln können, benötigen sie ein verlässliches Lagebild, klar definierte Verantwortlichkeiten und verständliche Handlungsempfehlungen. Wichtig sind regelmäßige Übungen um Routinen zu schaffen. Vertrauen in Prozesse entsteht nicht erst in der Krise, sondern durch kontinuierliche Vorbereitung.

Gleichzeitig sind Menschen nicht nur Teil der offiziellen Krisenorganisation. Qualifizierte Personen aus der Bevölkerung – wie zum Beispiel medizinisches Fachpersonal oder das THW – können Einsatzkräfte unterstützen, Informationen weitergeben, vulnerable Gruppen erreichen oder wichtige Aufgaben in Versorgung und Logistik übernehmen. Voraussetzung dafür ist, dass ihre Fähigkeiten bekannt sind und sie gezielt, sicher und entsprechend ihrer Qualifikation eingebunden werden können.

Eine resiliente Sicherheitsarchitektur stärkt deshalb nicht nur technische Systeme. Sie befähigt Menschen, auch unter außergewöhnlicher Belastung fundiert zu entscheiden, koordiniert zu handeln und Verantwortung zu übernehmen. **Erst das Zusammenspiel aus menschlicher Urteilskraft, gesellschaftlichem Engagement und vernetzter Technologie schafft die Handlungsfähigkeit, die eine Krise erfordert.**

Grundsatz des Erfolgs: Das System schlägt vor – aber der Mensch entscheidet

Verpflichtende Freigaben müssen an den kritischen Übergängen eingebaut sein: bei der Einstufung einer Lage, bei der Bewertung einer Empfehlung und vor der operativen Ausführung. Manuelle Übersteuerung und ein klares Vetorecht bleiben jederzeit möglich.

4. Wirkung Konvergenter Sicherheit in der Praxis

Ein Prinzip, unterschiedliche Lagen

Die Architektur bleibt bestehen. Datenquellen, Szenarien und notwendige Qualifikationen ändern sich je nach Lage.

Pandemie und Hitzewelle

Frühwarnsignale aus Gesundheitswesen, Versorgung und Umwelt werden verbunden. Verfügbare Pflegekräfte, Sozialarbeit und Sprachmittlung können gezielt eingeplant werden.

Cyberangriff auf kritische Infrastruktur

Digitale Angriffssignale werden mit betrieblichen und physischen Auswirkungen verknüpft. So wird sichtbar, welche Leistungen, Standorte und Ressourcen betroffen sind.

Hochwasser und Sturm

Pegel, Wetter, Verkehr und Bauhofdaten fließen in eine aktuelle Risikosicht ein. Evakuierung, Logistik und qualifizierte Hilfe lassen sich standortbezogen koordinieren.

Versorgungsausfall

Energie, Wasser, Kommunikation und Transport werden als voneinander abhängige Systeme betrachtet. Prioritäten richten sich an gesellschaftlich kritischen Leistungen aus.

Großbrand und Industrieunfall

Einsatzdaten, Wetter, Klinikkapazitäten und Verkehr werden gemeinsam bewertet. Aufnahme, Evakuierung und Versorgung können abgestimmt werden.

Öffentliche Verwaltung

Verteilte Standorte, Krisenstäbe und sensible Bereiche erhalten eine gemeinsame Sicht auf Anwesenheit, Berechtigungen, Verantwortlichkeiten und Entscheidungen.

Je stärker Systeme voneinander abhängen, desto wichtiger werden ein gemeinsames Lagebild, abgestimmte Prozesse und die gezielte Aktivierung verfügbarer Ressourcen.

5. Rahmenbedingungen Konvergenter Sicherheit

KI, Compliance und Datensouveränität

Geschwindigkeit ist wichtig. Aber in sicherheitskritischen Umgebungen zählen ebenso Transparenz, Kontrolle und rechtliche Belastbarkeit. Die Anforderungen gemäß der NIS-2 Richtlinie, der Cybersecurity Act und arbeitsrechtliche Vorschriften erhöhen die Komplexität.

Künstliche Intelligenz kann Ereignisse priorisieren, Muster erkennen, große Datenmengen analysieren und mögliche Entwicklungen simulieren. Sie dient nicht dazu, Verantwortung zu verlagern. Vielmehr gelten klare Grundsätze:

- ein klar definierter Zweck und Verhältnismäßigkeit
- Datensparsamkeit und hohe Datenqualität
- nachvollziehbare und verständliche Empfehlungen
- sichtbare Vertrauensgrenzen und regelmäßige Validierung
- menschliche Aufsicht, Korrektur und übergreifende Steuerung
- vollständige Protokollierung von Ereignissen, Freigaben und Maßnahmen

Operative Resilienz

Aufrechterhaltung des Betriebes, dezentrale Funktionsfähigkeit und schnelle Wiederherstellung.

Compliance by Design

Audit Trails, Genehmigungen und Nachweise entstehen direkt im Prozess.

Compliance by Design

Verarbeitung, Rechtsraum, Zugriffe und Abhängigkeiten sind transparent geregelt.

Für Behörden und Betreiber kritischer Infrastrukturen ist Datenhoheit eine strategische Frage. Entscheidend ist nicht allein, ob Daten verschlüsselt sind, sondern auch, wo sie verarbeitet werden, wer zugreifen kann und welchem Rechtsraum die Verarbeitung unterliegt.

Rechtliche Prüfung gehört in die Architektur

Datenschutz, Informationssicherheit, Haftung, Versicherung und mögliche Vergütung freiwilliger Kräfte müssen bereits im Vorfeld verbindlich geklärt werden. Im besten Fall erfolgt vorab eine juristische Einzelfallprüfung.

6. Empfehlung zur Umsetzung konvergenter Sicherheit

Resilienz schrittweise aufbauen

Modernisierung beginnt nicht mit einem Komplettaustausch, sondern mit den kritischsten Prozessen und Informationslücken.

1.Verstehen
Kritische Leistungen, Abhängigkeiten, Rollen, Datenquellen und manuelle Übergaben erfassen.

2.Verbinden
Bestehende Systeme über eine gemeinsame Identitäts-, Daten- und Prozessebene integrieren.

3. Orchestrieren
Eskalationen, Freigaben, Kommunikation und Ressourcenzuweisung als Playbooks definieren.

4. Erproben
Szenarien in Übungen testen, Zeitziele messen und Empfehlungen validieren.

Lernen
Auditdaten auswerten, Modelle anpassen und Prozesse kontinuierlich verbessern.

Für den schrittweisen Einstieg eignen sich Bereiche, in denen vernetzte Systeme und eine schnellere Koordination den größten Mehrwert schaffen. Entscheidend sind die gesellschaftliche Bedeutung der betroffenen Leistungen, die Anzahl manueller Schnittstellen, die Qualität der vorhandenen Daten und die Bereitschaft der beteiligten Organisationen, Informationen und Prozesse gemeinsam weiterzuentwickeln.

Strategische Empfehlung

Öffentliche Sicherheit ist keine einmalige Aufgabe, sondern ein fortlaufender Prozess. Technik, Organisation, rechtliche Rahmenbedingungen und Krisenübungen müssen deshalb konsequent aufeinander abgestimmt und kontinuierlich weiterentwickelt werden.

primion

Primion Technology
info@primion.eu
primion.io