FOCUS
— Investigations & Consulting —

Whitepaper
HYBRIDE RISIKEN BEWÄLTIGEN

Konvergenz von Cybersicherheit und physischer Sicherheit in modernen Organisationen

Abhängigkeiten verstehen
Sicherheitsfunktionen besser vernetzen
Resilienz stärken



Vorwort

Grenzen, die sich immer schwerer ziehen lassen

Die digitale Transformation hat die Funktionsweise von Organisationen grundlegend verändert. Informationssysteme, Betriebstechnologien, intelligente Gebäude, Zutrittskontrollen, Videoüberwachung, vernetzte Geräte und technische Infrastrukturen sind heute zunehmend miteinander verbunden.

Diese Entwicklung bringt erhebliche Vorteile hinsichtlich Effizienz, Überwachung und Automatisierung. Gleichzeitig entstehen neue Abhängigkeiten.

Ein Cyberangriff hat nicht mehr zwangsläufig ausschliesslich digitale Auswirkungen. Er kann Betriebsabläufe stören, den Zugang zu Anlagen verhindern, Geräte beeinträchtigen oder die Kontinuität einer Tätigkeit gefährden.

Umgekehrt kann ein physisches Eindringen den Zugang zu einem Computerarbeitsplatz, einer Netzwerkkomponente, einem technischen System oder zu Informationen ermöglichen, die anschliessend eine digitale Kompromittierung erleichtern.

Die herkömmliche Trennung zwischen Cybersicherheit und physischer Sicherheit wird somit weniger eindeutig, wenn die geschützten Werte, Technologien und Prozesse selbst voneinander abhängig sind.

Aus diesen Wechselwirkungen entstehen hybride Risiken: Risiken, deren Ursprung, Ausbreitung oder Auswirkungen mehrere Sicherheitsbereiche betreffen.

Dennoch werden diese Bereiche in vielen Organisationen weiterhin von unterschiedlichen Funktionen mit eigenen Zuständigkeiten, Instrumenten, Prozessen und Berufskulturen geführt.

Es geht nicht darum, diese Spezialisierung infrage zu stellen. Entscheidend ist vielmehr, ob die verschiedenen Funktionen ausreichend koordiniert sind, wenn ein Risiko ihre jeweiligen Zuständigkeitsgrenzen überschreitet.

Diesem Thema widmet sich das vorliegende Whitepaper.

Inhaltsverzeichnis

1. Warum sprechen wir heute von hybriden Risiken? **1**

2. Hybride Risiken verstehen **2**

3. Das Problem der organisatorischen Silos **3**

4. Vier zentrale Herausforderungen **5**

5. Sechs Dimensionen zum Verständnis der Konvergenz **7**

01 — Governance & Führung 7
02 — Organisation & Zusammenarbeit 8
03 — Management hybrider Risiken 8
04 — Technologien & Integration 9
05 — Erkennung & Reaktion 9
06 — Sicherheitskultur, Kompetenzen & kontinuierliche Verbesserung 9

6. Den eigenen Reifegrad beurteilen **10**

7. Von der Diagnose zur Verbesserung **11**

8. Zehn bewährte Praktiken **12**

9. Ist Ihre Organisation auf hybride Risiken vorbereitet? **13**

10. Was Konvergenz nicht werden darf **14**

11. Sicherheit als dynamischer Prozess **15**

Schlussfolgerung **15**

Das FOCUS-Modell zur Beurteilung des Reifegrads **16**

Über diese Publikation **16**

Über FOCUS **17**

Wichtigste Referenzen **17**

1. Warum sprechen wir heute von hybriden Risiken?

Organisationen sind zunehmend cyber-physisch vernetzt

Physische Sicherheit und Cybersicherheit haben sich historisch aus unterschiedlichen Problemstellungen heraus entwickelt.

Die physische Sicherheit schützt in erster Linie Menschen, Sachwerte, Anlagen und Infrastrukturen. Die Cybersicherheit hat sich auf den Schutz von Informationssystemen, Netzwerken und Daten ausgerichtet.

Diese Unterscheidung bleibt sinnvoll. Die erforderlichen Kompetenzen sind nicht dieselben, und Konvergenz bedeutet nicht, dass diese Berufsfelder zusammengelegt werden müssen.

Verändert hat sich das Umfeld, in dem sie tätig sind.

Gebäude verfügen heute über digitale Systeme. Zutrittskontrollsysteme sind vernetzt. Kameras arbeiten über IP-Netzwerke. Technische Anlagen werden aus der Ferne überwacht. Industrielle Umgebungen verbinden Informatiksysteme mit Betriebstechnologien. Mitarbeitende greifen von unterschiedlichen Orten und Geräten auf digitale Ressourcen zu.

Die physische Welt ist somit stärker vom Digitalen abhängig, während das Digitale weiterhin auf sehr physische Elemente angewiesen ist: Gebäude, Stromversorgung, Geräte, Netzwerke, Menschen und Zutrittsmöglichkeiten.

Eine moderne Organisation bildet damit ein **System wechselseitiger Abhängigkeiten**.

Eine Schwachstelle in einem Bereich kann sich auf einen anderen auswirken.

Genau an diesen Schnittstellen entstehen hybride Risiken.

Risiken halten sich nicht an Organigramme

Eine Organisation kann über ein ausgezeichnetes Cybersicherheitsteam und ein wirksames physisches Sicherheitsdispositiv verfügen und dennoch Schwachstellen an der Schnittstelle zwischen diesen beiden Bereichen aufweisen.

Warum?

Weil sich ein Angreifer, ein Vorfall oder eine Störung nicht zwangsläufig an die interne Zuständigkeitsverteilung hält.

Ein Ereignis kann in der physischen Welt beginnen und sich im digitalen Bereich fortsetzen. Es kann auch den umgekehrten Weg nehmen oder mehrere Vorgehensweisen gleichzeitig kombinieren.

Die entscheidende Frage lautet daher weniger:

«Erfüllt jede Sicherheitsfunktion ihre Aufgaben korrekt?»

Sondern vielmehr:

«Was geschieht, wenn ein Risiko mehrere Funktionen betrifft?»

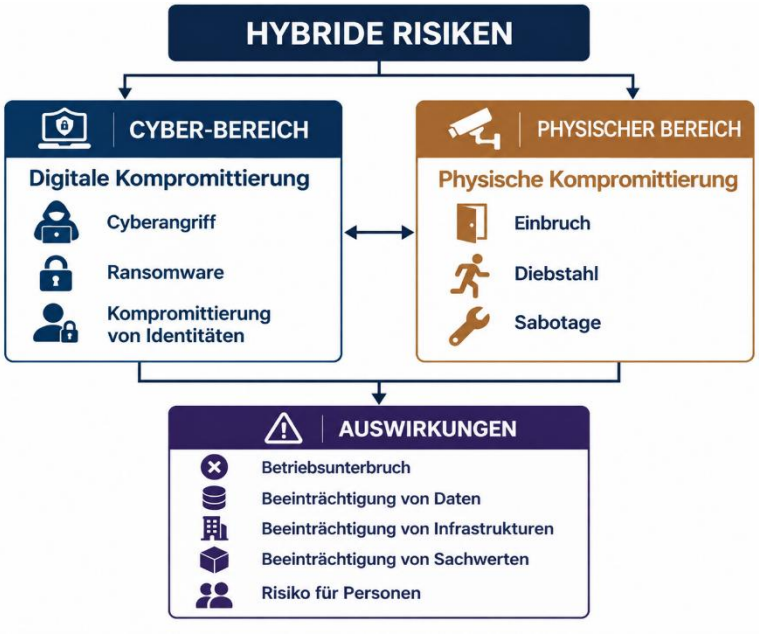
Diese Entwicklung rechtfertigt einen stärker bereichsübergreifenden Sicherheitsansatz.

2. Hybride Risiken verstehen

Wechselwirkungen zwischen digitalen und physischen Dimensionen

Im Rahmen dieses Whitepapers bezeichnet ein **hybrides Risiko** ein Risiko, das aus dem Zusammenwirken der digitalen und physischen Dimensionen einer Organisation entsteht und bereichsübergreifende Auswirkungen auf Menschen, Sachwerte, Prozesse, Systeme oder Infrastrukturen haben kann.

Drei grundlegende Dynamiken verdeutlichen diese Zusammenhänge.



Vom Cyberbereich in die physische Welt

Eine digitale Kompromittierung kann die Funktionsweise eines Systems stören oder verändern und Auswirkungen in der physischen Welt verursachen.

Dies kann beispielsweise bei einem Angriff auf ein industrielles System, eine technische Anlage, eine Steuerungseinrichtung oder auf die Verfügbarkeit einer für den Betrieb unverzichtbaren Dienstleistung der Fall sein.

Der Vorfall beginnt im digitalen Umfeld, seine Folgen reichen jedoch darüber hinaus.

Von der physischen Welt in den Cyberbereich

Auch der umgekehrte Weg ist möglich.

Der physische Zugang zu einem Gebäude, einem Technikraum, einem Arbeitsplatz oder einem Gerät kann es ermöglichen, digitale Ressourcen zu erreichen, die normalerweise durch mehrere Ebenen logischer Sicherheitsmassnahmen geschützt sind.

Ein physisches Eindringen kann ausserdem ermöglichen, Informationen auszuspähen, ein Gerät zu entwenden, eine noch aktive Sitzung auszunutzen oder ein Gerät mit einer Infrastruktur zu verbinden.

Die Kontrolle physischer Zugänge wird damit zu einem Bestandteil des Schutzes von Informationssystemen.

Kombinierte Handlungen

Manche Szenarien beruhen schliesslich auf einer Kombination mehrerer Dimensionen: digitale Handlungen, physisches Eindringen, Social Engineering, die Nutzung öffentlich zugänglicher Informationen oder menschliche Manipulation.

Die Wirksamkeit eines solchen Szenarios ergibt sich nicht unbedingt aus der Raffinesse eines einzelnen Angriffs, sondern aus der **Verkettung mehrerer Schwachstellen aus unterschiedlichen Bereichen.**

3. Das Problem der organisatorischen Silos

Ausgeprägte Fachkompetenzen können unzureichend koordiniert bleiben

Spezialisierung ist notwendig. Eine komplexe Organisation benötigt Kompetenzen in den Bereichen Cyber, IT, OT, physische Sicherheit, Business Continuity, Krisenmanagement, Risikomanagement, Compliance und Fachbereiche.

Problematisch wird es, wenn aus dieser Spezialisierung eine **Abschottung** entsteht.

Unterschiedliche Führungslinien, getrennte Budgets, funktionsspezifische Instrumente oder fehlende gemeinsame Prozesse können den Informationsfluss einschränken.

Ein Team kann dadurch über Informationen verfügen, die für eine andere Funktion wichtig wären, ohne deren Bedeutung zu erkennen.

Auch ein Ereignis, das in einem Bereich als geringfügig gilt, kann in Verbindung mit einem anderen Ereignis zu einem wichtigen Hinweis werden.

Unser Ansatz unterstreicht deshalb die Bedeutung einer bereichsübergreifenden Governance, geeigneter Koordinationsmechanismen und eines wirksamen Informationsaustauschs**, ohne zwingend eine Zusammenlegung der Cyber- und physischen Sicherheitsfunktionen zu empfehlen.**

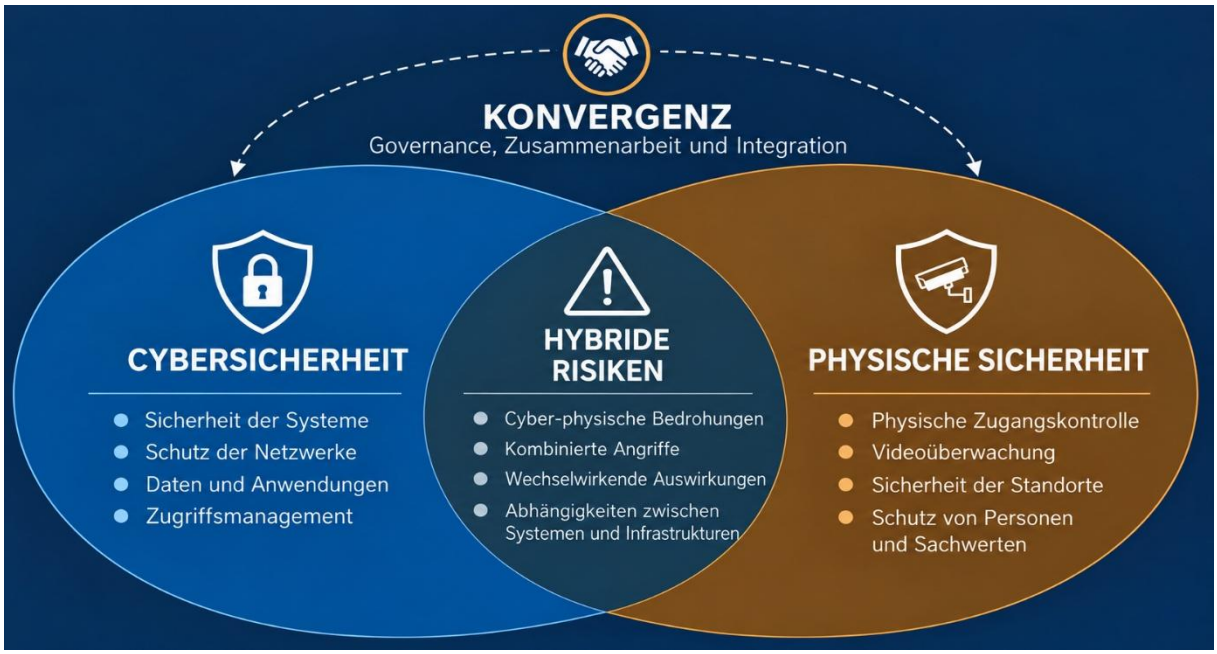
Konvergenz bedeutet nicht Fusion

Dies ist ein wesentlicher Punkt.

Cyber-physische Konvergenz bedeutet weder, Fachpersonen für physische Sicherheit zu Cyberexperten zu machen, noch Cyberfachleute zu Verantwortlichen für physische Sicherheit.

Ebenso wenig müssen sämtliche Sicherheitsfunktionen grundsätzlich einer einzigen Leitung unterstellt werden.

Konvergenz bedeutet vielmehr, Voraussetzungen zu schaffen, **damit die verschiedenen Fachdisziplinen ihre gegenseitigen Abhängigkeiten verstehen und bei Bedarf zusammenarbeiten können.**



Sie kann insbesondere folgende Aspekte betreffen:

Governance · Zuständigkeiten · Informationsaustausch · Risikobeurteilung · Verfahren · Technologien · Erkennung · Reaktion auf Sicherheitsvorfälle · Krisenmanagement · Schulung und Sicherheitskultur.

Der angemessene Konvergenzgrad hängt somit von der jeweiligen Organisation ab.

> **Konvergenz ist kein Selbstzweck. Sie ist ein Mittel, um die Fähigkeit einer Organisation zu verbessern, Risiken zu verstehen, ihnen vorzubeugen, sie zu erkennen und zu bewältigen, wenn sie mehrere Sicherheitsbereiche betreffen.**

4. Vier zentrale Herausforderungen

Die Arbeiten, die zur Entwicklung des FOCUS-Ansatzes geführt haben, lassen vier grosse Kategorien von Herausforderungen erkennen: **organisatorische, technische, menschliche und regulatorische.**
Diese Herausforderungen sind voneinander abhängig: Eine Schwäche in einer Kategorie kann Auswirkungen auf andere haben.



01 —Organisatorische Herausforderungen

Eine erste Herausforderung liegt häufig in der Governance.

Wer verfügt über einen Gesamtüberblick über hybride Risiken? Wer entscheidet, wenn ein Ereignis mehrere Bereiche betrifft? Gibt es dauerhafte Mechanismen, über die verschiedene Funktionen ihre Informationen austauschen können?

Eine Organisation kann über ausgezeichnete spezialisierte Fähigkeiten verfügen und dennoch kein **gemeinsames Lagebild** haben.

Konvergenz beginnt daher mit der Klärung von Zuständigkeiten und Schnittstellen.

02 —Technische Herausforderungen

Die Vernetzung der Technologien stellt eine zweite Herausforderung dar.

Zutrittskontrollsysteme, Videoüberwachung, Gebäudeleittechnik, IT-Netzwerke, Betriebstechnologien und vernetzte Geräte können Infrastrukturen, Identitäten oder Daten gemeinsam nutzen.

Die Sicherheit eines Systems lässt sich daher nicht mehr in jedem Fall unabhängig von seiner Umgebung beurteilen.

Es geht nicht zwingend darum, noch mehr Sicherheitssysteme miteinander zu verbinden, sondern ihre **Abhängigkeiten zu verstehen und ihre Schnittstellen zu beherrschen.**

03 —Menschliche Herausforderungen

Konvergenz hängt ebenso von den Menschen ab.

Berufskulturen unterscheiden sich. Fachbegriffe, Analysemethoden, Prioritäten und selbst die Risikowahrnehmung können zwischen Teams stark variieren.

Ein gemeinsames Verständnis zu schaffen bedeutet nicht, Kompetenzen zu vereinheitlichen. Vielmehr soll jede Funktion die Anliegen der anderen ausreichend verstehen, **um relevante Informationen zu erkennen, an die richtigen Stellen weiterzugeben und koordiniert zu handeln.**

04 —Regulatorische Herausforderungen

Organisationen bewegen sich schliesslich in einem zunehmend anspruchsvollen regulatorischen und normativen Umfeld.

Datenschutz, Cybersicherheit, Geschäftskontinuität, Resilienz von Infrastrukturen und Risikogovernance greifen zunehmend ineinander.

Die wichtigsten in den zugrunde liegenden Arbeiten untersuchten Referenzwerke – darunter ISO/IEC 27001, ISO 31000, ISO 22301, NIST CSF 2.0 sowie Schweizer Rahmenwerke zur Cybersicherheit und Resilienz – betonen die Bedeutung von Governance, Risikomanagement und kontinuierlicher Verbesserung, auch wenn nicht alle unmittelbar auf die cyber-physische Konvergenz eingehen.

Die Einhaltung von Vorschriften bleibt eine Grundlage, aber keine absolute Sicherheitsgarantie.

> **Die vier Herausforderungen sind miteinander verbunden. Bei der Konvergenz geht es nicht darum, sie isoliert zu behandeln, sondern ihre Wechselwirkungen zu verstehen.**

5. Sechs Dimensionen zum Verständnis der Konvergenz

Ein von FOCUS entwickeltes Modell

Um diese Herausforderungen in einen strukturierten Ansatz zu überführen, hat FOCUS ein **Modell zur Diagnose des Reifegrads der cyber-physischen Konvergenz entwickelt.**

Das Modell dient weder der Zertifizierung einer Organisation noch der Überprüfung ihrer Normenkonformität.

Ziel ist es vielmehr, den Reifegrad der cyber-physischen Konvergenz zu beurteilen, Unterschiede zwischen den einzelnen Dimensionen zu erkennen und einen auf den jeweiligen organisatorischen Kontext abgestimmten Verbesserungsprozess zu unterstützen.

Das vollständige Modell basiert auf sechs miteinander verbundenen Dimensionen.

DIMENSION	ROLLE IN DER KONVERGENZ
01 Governance & Führung	Gibt die strategische Ausrichtung vor, definiert die Verantwortlichkeiten und schafft die Voraussetzungen für eine wirksame Koordination.
02 Organisation & Zusammenarbeit	Fördert die Koordination zwischen den Funktionen, den Informationsfluss und den Abbau von Silos.
03 Management hybrider Risiken	Ermöglicht die Identifikation, Bewertung und Behandlung von Risiken, die mit den Abhängigkeiten zwischen physischen und digitalen Bereichen verbunden sind.
04 Technologien & Integration	Stellt die technischen Fähigkeiten bereit, die für die Konvergenz erforderlich sind, und gewährleistet gleichzeitig die Sicherheit und Resilienz der vernetzten Systeme.
05 Erkennung & Reaktion	Ermöglicht die frühzeitige Erkennung von Ereignissen, eine gemeinsame Lageanalyse und eine koordinierte Reaktion.
06 Sicherheitskultur, Kompetenzen & kontinuierliche Verbesserung	Fördert ein gemeinsames Verständnis, stärkt die Kompetenzen und unterstützt eine kontinuierliche Verbesserung, die auf die Herausforderungen der Organisation abgestimmt ist.

01 — Governance & Führung

Eine gemeinsame Richtung vorgeben

Konvergenz beginnt auf der Ebene der Governance.

Eine Organisation muss festlegen können, wie hybride Risiken in ihre Entscheidungen einbezogen werden und wie die Zuständigkeiten auf die verschiedenen Funktionen verteilt sind.

Der Geschäftsleitung kommt dabei eine zentrale Rolle zu.

Sie muss sich nicht zwangsläufig mit technischen Einzelheiten befassen, soll jedoch ein gemeinsames Verständnis ermöglichen, Zuständigkeiten klären und Prioritäten festlegen.

Zentrale Fragen:

Ist die Steuerung der Konvergenz klar zugeordnet?

Sind die Zuständigkeiten eindeutig geregelt?

Werden hybride Risiken auf der angemessenen Entscheidungsebene behandelt?

Verfolgen die verschiedenen Funktionen miteinander vereinbare Ziele?

Wird die Konvergenz ausschliesslich von operativen Teams getragen, besteht die Gefahr, dass sie punktuell bleibt. Damit sie dauerhaft verankert wird, braucht sie die Unterstützung der Governance.

02 — Organisation & Zusammenarbeit

Silos überwinden, ohne Fachkompetenzen aufzugeben

Eine gemeinsame Governance genügt nicht, wenn den Teams die Mechanismen fehlen, um im Alltag zusammenzuarbeiten.

Diese Dimension befasst sich mit bereichsübergreifenden Prozessen, dem Informationsaustausch, Schnittstellen zwischen Teams und Koordinationsmechanismen.

Das Ziel ist nicht, mehr Sitzungen durchzuführen.

Entscheidend ist, dass die **richtigen Informationen zur richtigen Zeit bei der zuständigen Funktion ankommen.**

Dazu können regelmässige Austausche, gemeinsame Verfahren, klar bezeichnete Ansprechpersonen oder abgestimmte Eskalationsmechanismen beitragen.

Der Reifegrad bemisst sich weniger an der Zahl geschaffener Strukturen als an ihrer tatsächlichen Funktionsfähigkeit, wenn es darauf ankommt.

03 — Management hybrider Risiken

Szenarien ganzheitlich betrachten

Eine getrennte Erfassung von Cyberrisiken und physischen Risiken kann blinde Flecken hinterlassen.

Diese dritte Dimension soll daher feststellen, ob die Organisation ihre kritischen Werte, deren Abhängigkeiten und Szenarien mit bereichsübergreifenden Auswirkungen erkennt.

Ein hybrides Risiko muss als Ereigniskette und nicht nur als isolierter Vorfall analysiert werden.

Beispielsweise:

Unbefugtes physisches Eindringen → Zugang zu einem Gerät → digitale Kompromittierung → Betriebsstörung.

Oder in umgekehrter Richtung:

Digitale Kompromittierung → Verlust der Überwachung → Störung eines physischen Prozesses → Auswirkungen auf den Betrieb.

Ziel ist es, mögliche Ausbreitungswege eines Risikos zu erkennen.

04 — Technologien & Integration

Technologische Abhängigkeiten verstehen

Technologien unterstützen heute sowohl betriebliche Abläufe als auch Schutzmassnahmen.

Diese Dimension untersucht insbesondere die Wechselwirkungen zwischen vernetzten Systemen, Betriebstechnologien, Zutrittskontrollen, Identitäten und Überwachungseinrichtungen.

Eine stärkere Integration bedeutet nicht automatisch mehr Sicherheit.

Eine zusätzliche Technologie kann auch eine neue Abhängigkeit schaffen.

Die entscheidende Frage lautet daher:

Sind unsere Sicherheitstechnologien nur einzeln leistungsfähig, oder wird auch ihr Zusammenwirken verstanden und beherrscht?

Eine Organisation mit einem hohen Reifegrad sollte insbesondere die wichtigsten Abhängigkeiten zwischen ihren kritischen Systemen kennen und wissen, wie sich ein Vorfall in einem System auf andere auswirken kann.

05 — Erkennung & Reaktion

Ein gemeinsames Lagebild des Vorfalls schaffen

Ein Ereignis zu erkennen, genügt nicht.

Man muss auch verstehen, was es bedeutet.

Ein physisches Ereignis kann der erste Hinweis auf einen digitalen Angriff sein. Ein Cybereereignis kann eine physische Handlung ankündigen oder begleiten.

Bleiben Informationen voneinander getrennt, besteht die Gefahr, dass Teams nur einen Teil des Szenarios wahrnehmen.

Diese Dimension untersucht daher die Fähigkeit der Organisation, **Ereignisse zu erkennen, Informationen auszutauschen, Zusammenhänge herzustellen und Vorfälle zu bearbeiten, die mehrere Funktionen betreffen können.**

Sie umfasst auch die Reaktion auf Sicherheitsvorfälle und Eskalationsmechanismen.

Bei einem hybriden Vorfall kann die Qualität der Koordination ebenso wichtig werden wie die Qualität der Erkennungsinstrumente.

06 — Sicherheitskultur, Kompetenzen & kontinuierliche Verbesserung

Konvergenz dauerhaft in der Praxis verankern

Technologien und Verfahren funktionieren nur, wenn die Menschen sie verstehen und anwenden.

Die letzte Dimension umfasst daher die Sicherheitskultur, Sensibilisierung, bereichsübergreifende Kompetenzen, die Einbindung des Managements und die kontinuierliche Verbesserung.

Die Teams müssen nicht alle Disziplinen beherrschen.

Sie sollten jedoch die angrenzenden Fachgebiete ausreichend verstehen, um ungewöhnliche Situationen zu erkennen und rasch die richtigen Kompetenzen beizuziehen.

Konvergenz erreicht einen hohen Reifegrad, wenn sie nicht länger ein punktuelles Projekt ist, sondern zu **einem selbstverständlichen Bestandteil des Sicherheitsdenkens wird.**

6. Den eigenen Reifegrad beurteilen

Den Reifegrad beurteilen statt die Normenkonformität prüfen

Das FOCUS-Modell basiert auf einem Reifegradansatz.

Damit lässt sich die Entwicklung einer Organisation beurteilen: von einer weitgehend getrennten Arbeitsweise hin zu einer stärker integrierten Koordination, die in einem kontinuierlichen Verbesserungsprozess verankert ist.

Die Diagnose umfasst **mehrere Fragen zu den sechs Dimensionen**, die anhand einer fünfstufigen Reifegradskala beurteilt werden. Die Ergebnisse ermöglichen insbesondere, Unterschiede zwischen den Dimensionen sichtbar zu machen und Prioritäten festzulegen.



Ein Punkt bleibt jedoch grundlegend:

> **Nicht nur der Gesamtreifegrad ist entscheidend. Auch das Gleichgewicht zwischen den verschiedenen Dimensionen spielt eine wichtige Rolle.**

Eine Organisation kann beispielsweise über fortschrittliche Technologien verfügen, während ihre Governance unzureichend strukturiert ist. Eine andere kann eine ausgezeichnete Zusammenarbeit zwischen den Teams entwickelt haben, hybride Risiken jedoch noch kaum in ihre Prozesse einbeziehen.

Die Konvergenz muss daher **gesamthaft und unter Berücksichtigung des jeweiligen organisatorischen Kontexts beurteilt werden.**

7. Von der Diagnose zur Verbesserung

Wichtigste Elemente der Ergebnisdarstellung



Ein Vorgehen in vier Schritten

Eine Diagnose ist nur dann wertvoll, wenn daraus nützliche Entscheidungen entstehen. Sie ermöglicht es, die Reifegradbeurteilung in eine strukturierte Übersicht über Stärken, Lücken und Verbesserungsprioritäten zu überführen.

Das vorgeschlagene Vorgehen umfasst deshalb vier Schritte.

Beurteilen

Die Ausgangssituation, die bestehenden Praktiken und die Wechselwirkungen zwischen den Funktionen einschätzen.

Lücken erkennen

Bereiche aufzeigen, in denen die Koordination unzureichend, informell oder zu stark von einzelnen Personen abhängig ist.

Priorisieren

Verbesserungen nach Kontext, Herausforderungen, Abhängigkeiten und Reifegrad gewichten.

Die Roadmap festlegen

Prioritäten in realistische und schrittweise umsetzbare Verbesserungsansätze überführen.

Technologie ist nicht immer die erste Lösung

Wenn ein neues Risiko auftritt, besteht die naheliegende Reaktion manchmal darin, nach einer neuen technischen Lösung zu suchen.

Die Arbeiten, die diesem Whitepaper zugrunde liegen, zeigen jedoch, dass die Bewältigung hybrider Risiken auch – und häufig in erheblichem Mass – **von Governance, Koordination, Prozessen und Kompetenzen** abhängt.

Bevor in ein neues Instrument investiert wird, können mehrere Fragen gestellt werden:
Sind die Zuständigkeiten klar?
Kommunizieren die Teams miteinander?
Sind hybride Szenarien identifiziert?
Werden vorhandene Informationen angemessen ausgetauscht?
Sind die Verfahren zur Reaktion auf Vorfälle aufeinander abgestimmt?

Mitunter lässt sich die Resilienz bereits deutlich verbessern, indem bestehende Fähigkeiten besser zusammenwirken.

8. Zehn bewährte Praktiken

Konkrete Schritte für weitere Fortschritte

01 — Kritische Abhängigkeiten erkennen

Nicht nur die Werte erfassen, sondern auch die Beziehungen zwischen Systemen, Menschen, Infrastrukturen, Lieferanten und Prozessen identifizieren.

02 — Zuständigkeiten klären

Festlegen, wer die Führung übernimmt und wer eingreift, wenn ein Ereignis mehrere Sicherheitsbereiche betrifft.

03 — Informationsaustausch organisieren

Definieren, welche Informationen zwischen welchen Funktionen und unter welchen Umständen ausgetauscht werden müssen.

04 — Hybride Szenarien entwickeln

Bei Übungen und Überlegungen Ereignisse berücksichtigen, die herkömmliche Grenzen überschreiten: vom Cyberbereich in die physische Welt, von der physischen Welt in den Cyberbereich oder durch kombinierte Handlungen.

05 — Fachbereiche einbeziehen

Sicherheit betrifft nicht nur Spezialisten. Die Fachbereiche kennen die betrieblichen Abhängigkeiten und die tatsächlichen Folgen eines Unterbruchs.

06 — Schnittstellen zwischen IT, OT und physischer Sicherheit berücksichtigen

In den betreffenden Umgebungen müssen die Wechselwirkungen zwischen diesen Bereichen bekannt sein und bei Entscheidungen berücksichtigt werden.

07 — Erkennung und Reaktion koordinieren

Sicherstellen, dass ein in einem Bereich erkanntes Ereignis rasch an die anderen betroffenen Funktionen weitergeleitet und dort richtig eingeordnet werden kann.

08 — Koordination überprüfen

Theoretische Verfahren allein genügen nicht. Übungen, Simulationen und Tests ermöglichen es, ihre tatsächliche Funktionsfähigkeit zu überprüfen.

09 — Eine gemeinsame Kultur entwickeln

Fachpersonen für die Schnittstellen zu anderen Disziplinen sensibilisieren und schulen, statt jede Person zur Expertin oder zum Experten für sämtliche Bereiche machen zu wollen.

10 — Konvergenz in die kontinuierliche Verbesserung integrieren

Technologien, Bedrohungen und Organisationen verändern sich. Der heute angemessene Konvergenzgrad wird morgen nicht zwangsläufig ausreichen.

9. Ist Ihre Organisation auf hybride Risiken vorbereitet?

Sechs Fragen als Einstieg

Eine Organisation kann über leistungsfähige Massnahmen in der Cyber- und physischen Sicherheit verfügen, ohne vollständig auf Ereignisse vorbereitet zu sein, die beide Dimensionen gleichzeitig betreffen.

Die folgenden Fragen stellen keine Diagnose dar, ermöglichen jedoch eine erste Auseinandersetzung mit dem Thema.

1 — Governance

Sind bei einem Vorfall, der sowohl das physische als auch das digitale Umfeld betrifft, die **Zuständigkeiten, die Führung und die Entscheidungsmechanismen klar geregelt?**

☐ Ja ☐ Teilweise ☐ Nein ☐ Weiss nicht

2 — Zusammenarbeit

Tauschen sich die Funktionen Cybersicherheit und physische Sicherheit sowie gegebenenfalls IT, OT, Business Continuity und Fachbereiche **regelmässig über ihre jeweiligen Bedrohungen, Schwachstellen und Vorfälle** aus?

☐ Ja ☐ Teilweise ☐ Nein ☐ Weiss nicht

3 — Hybride Risiken

Berücksichtigen Ihre Risikobeurteilungen ausdrücklich Szenarien, bei denen **eine physische Kompromittierung digitale Auswirkungen hat – oder umgekehrt?**

☐ Ja ☐ Teilweise ☐ Nein ☐ Weiss nicht

4 — Technologien

Sind die Abhängigkeiten zwischen **Zutrittskontrollen, Videoüberwachung, vernetzten Systemen, Netzwerken, Informationssystemen und betrieblichen Umgebungen** bekannt und werden sie von den betroffenen Funktionen verstanden?

☐ Ja ☐ Teilweise ☐ Nein ☐ Weiss nicht

5 — Erkennung & Reaktion

Ermöglichen Ihre Verfahren, ein Ereignis, das die Grenze zwischen Cyberbereich und physischer Welt überschreitet, gemeinsam **zu erkennen, einzuordnen, Informationen dazu auszutauschen und es zu bearbeiten?**

☐ Ja ☐ Teilweise ☐ Nein ☐ Weiss nicht

6 — Sicherheitskultur & Kompetenzen

Verfügen die betroffenen Mitarbeitenden über ein ausreichendes Verständnis der cyber-physischen Wechselwirkungen, **um schwache Signale zu erkennen, die für eine andere Sicherheitsfunktion** relevant sein könnten?

☐ Ja ☐ Teilweise ☐ Nein ☐ Weiss nicht

Wie sind Ihre Antworten zu interpretieren?

Diese Fragen ergeben bewusst **weder eine Punktzahl noch ein Audit oder eine formelle Reifegradbeurteilung**.

Eine Antwort mit «Nein», «Teilweise» oder «Weiss nicht» bedeutet nicht zwangsläufig, dass Ihre Organisation unzureichend geschützt ist.

Mehrere solche Antworten können jedoch auf Bereiche hinweisen, **in denen die Konvergenz näher betrachtet werden sollte:** fragmentierte Zuständigkeiten, unzureichend strukturierter Austausch, unbekannte Abhängigkeiten, zu wenig berücksichtigte hybride Szenarien oder weiterhin getrennte Reaktionsverfahren.

Es geht dann nicht unbedingt darum, zusätzliche Sicherheitsmassnahmen einzuführen. Zunächst sollte geklärt werden, **ob die bereits vorhandenen Massnahmen, Informationen, Kompetenzen und Funktionen ausreichend koordiniert sind.**

10. Was Konvergenz nicht werden darf

Vier Fallstricke vermeiden

Auch die Konvergenz birgt Risiken, wenn sie falsch verstanden wird.

01 —Alles zentralisieren wollen

Eine koordinierte Governance setzt nicht zwingend eine zentralisierte Organisation voraus.
Die spezialisierten Fachbereiche müssen ihre fachliche Tiefe und operative Handlungsfähigkeit bewahren.

02 — Technische Integration ohne tatsächlichen Bedarf schaffen

Die Vernetzung weiterer Systeme kann die Übersicht verbessern, aber auch die Komplexität erhöhen und neue Abhängigkeiten schaffen.

Die Integration muss einem klar erkannten Bedarf entsprechen.

03 — Konvergenz auf ein IT-Projekt reduzieren

Die Herausforderungen sind ebenso organisatorischer und menschlicher wie technischer Natur.

Ein ausschliesslich technologieorientiertes Projekt wird Probleme der Governance oder Zusammenarbeit nicht lösen.

04 —Einen maximalen Konvergenzgrad anstreben

Es gibt nicht zwingend einen idealen Reifegrad, der für alle Organisationen gleichermassen gilt.

Ein KMU, eine Gesundheitseinrichtung, ein Industriebetrieb oder eine grosse Organisation haben weder dieselben Abhängigkeiten noch dieselben Bedürfnisse.

Das Ziel ist daher eine **verhältnismässige und bedarfsgerechte** Konvergenz, nicht eine maximale Integration.

11. Sicherheit als dynamischer Prozess

Resilienz als fortlaufender Prozess

Bedrohungen verändern sich. Organisationen ebenfalls.

Neue Systeme werden eingeführt, Infrastrukturen verändern sich, Lieferanten wechseln, neue Abhängigkeiten entstehen und die Vorgehensweisen von Angreifern passen sich an.

Sicherheit kann daher nicht als ein für alle Mal erreichter Zustand betrachtet werden.

> Eine resiliente Organisation muss in der Lage sein, **vorauszuschauen · zu erkennen · zu verstehen · zu koordinieren · zu reagieren · zu lernen · sich anzupassen.**

Die cyber-physische Konvergenz ist Teil dieses Ansatzes.

Sie ersetzt weder die Cybersicherheit noch die physische Sicherheit, das Risikomanagement oder die Business Continuity.

Sie zielt darauf ab, **diese Fähigkeiten miteinander zu verbinden, wenn ihre Wechselwirkungen entscheidend werden.**

Schlussfolgerung

Besser koordinieren statt lediglich mehr schützen

Die digitale Transformation hat einen Teil der Grenzen zwischen physischen und digitalen Umgebungen schrittweise aufgelöst. Dadurch sind neue Möglichkeiten, aber auch neue Abhängigkeiten entstanden.

Ein Angriff, ein Fehler oder eine Störung kann sich heute von einem Bereich auf einen anderen ausbreiten und gleichzeitig Informationen, Betriebsabläufe, Infrastrukturen und Menschen betreffen.

Angesichts dieser Realität genügt es nicht immer, spezialisierte Schutzmassnahmen einfach zu erweitern. Die Fähigkeit einer Organisation, hybride Risiken zu bewältigen, hängt auch davon ab, ob sie ihre **Abhängigkeiten versteht, ihre Sicherheitsfunktionen koordiniert, Informationen austauscht und ein gemeinsames Risikoverständnis entwickelt.**

Konvergenz bedeutet nicht, Berufsfelder zusammenzulegen, sondern die Voraussetzungen dafür zu schaffen, dass ihre jeweiligen Fachkompetenzen zusammenwirken, wenn ein Risiko dies erfordert.

Dieser Ansatz muss dem Kontext, den Herausforderungen und dem Reifegrad jeder Organisation angemessen sein. Konvergenz sollte daher weniger als Endzustand, sondern vielmehr als **schrittweiser Prozess zur Verbesserung der Resilienz verstanden werden.**

> **Möglicherweise haben Sie bereits in Cybersicherheit und physische Sicherheit investiert. Entscheidend ist nun die Frage, ob all diese Komponenten tatsächlich zusammenwirken.**

Das FOCUS-Modell zur Beurteilung des Reifegrads

Von der ersten Reflexion zur strukturierten Beurteilung

Die sechs Fragen dieses Whitepapers dienen als erstes Instrument zur Sensibilisierung. Sie ermöglichen keine Bestimmung des Reifegrads einer Organisation.

FOCUS hat ein **Modell zur Beurteilung des Reifegrads der cyber-physischen Konvergenz** entwickelt, das auf sechs miteinander verbundenen Dimensionen beruht:
Governance & Führung
Organisation & Zusammenarbeit
Management hybrider Risiken
Technologien & Integration
Erkennung & Reaktion
Sicherheitskultur, Kompetenzen & kontinuierliche Verbesserung

Die Reifegradanalyse dient dazu, **wesentliche Lücken in der Konvergenz zu identifizieren, den Reifegrad zu beurteilen und Prioritäten für Verbesserungsmassnahmen abzuleiten.**

Sie ersetzt weder ein technisches Cybersicherheitsaudit noch eine detaillierte Risikoanalyse. Vielmehr bietet sie eine **bereichsübergreifende Sicht auf die Koordination zwischen den verschiedenen Sicherheitsfunktionen.**

BEURTEILEN SIE DEN GRAD IHRER CYBER-PHYSISCHEN KONVERGENZ

FOCUS

Ermittlungen · Sicherheit · Beratung

Über diese Publikation

Ursprung des Ansatzes

Die in diesem Whitepaper vorgestellten Arbeiten bauen auf einer **wissenschaftlichen Arbeit zum Management hybrider Risiken und zur Konvergenz zwischen Cybersicherheit und physischer Sicherheit** auf, die im Rahmen des **Certificate of Advanced Studies HES-SO *en Sécurité et sûreté (CAS SEC)* an der HEIG-VD** durchgeführt wurde.

Diese Forschungsarbeit führte insbesondere zur Entwicklung eines **Modells zur Bewertung des Reifegrads der cyber-physischen Konvergenz**.

Das Modell und die daraus gewonnenen Erkenntnisse wurden anschliessend von FOCUS im Hinblick auf die **angewandte Forschung und den professionellen Einsatz** angepasst und weiterentwickelt. Die wissenschaftliche Arbeit, auf der dieser Ansatz beruht, stützte sich insbesondere auf eine Auswertung wissenschaftlicher und praxisorientierter Fachliteratur, die Untersuchung anerkannter Standards und Referenzwerke sowie den Austausch mit Fachpersonen aus dem Sicherheitsbereich.

Das vorliegende Whitepaper ist eine eigenständige Publikation von FOCUS. Es verfolgt das Ziel, die Thematik verständlich aufzubereiten, **bewährte Praktiken** aufzuzeigen und einen Beitrag zur Auseinandersetzung mit den Herausforderungen zu leisten, denen Organisationen angesichts zunehmend voneinander abhängiger physischer und digitaler Umgebungen gegenüberstehen.

Über FOCUS

Ermittlungen · Sicherheit · Beratung

FOCUS unterstützt Unternehmen und Institutionen bei der Analyse sensibler Situationen, der Beurteilung ihrer physischen Sicherheitsvorkehrungen und beim Umgang mit Risiken.

Die Tätigkeiten gliedern sich in drei sich ergänzende Bereiche:

Ermittlungen — Sachverhalte klären und Situationen verstehen.

Audits & Tests — Schwachstellen erkennen und Schutzmassnahmen beurteilen.

Beratung — Organisationen bei Fragen der physischen Sicherheit begleiten und zu einem besseren Risikomanagement beitragen.

FOCUS entwickelt zudem eigene Methoden, Beurteilungsinstrumente und praxisorientierte Ansätze, die durch praktische Erfahrungen, angewandte Forschung und kontinuierliche Verbesserung weiterentwickelt werden.

Die Arbeiten zu hybriden Risiken und zur cyber-physischen Konvergenz sind Teil dieser Entwicklung.

Wichtigste Referenzen

ISO/IEC 27001:2022 — Internationale Organisation für Normung (ISO) und Internationale Elektrotechnische Kommission (IEC). Informationssicherheit, Cybersicherheit und Datenschutz — Informationssicherheitsmanagementsysteme — Anforderungen, 2022.

ISO 31000:2018 — Internationale Organisation für Normung (ISO). Risikomanagement — Leitlinien, 2018.

ISO 22301:2019 — Internationale Organisation für Normung (ISO). Sicherheit und Resilienz — Managementsysteme für die Kontinuität von Geschäftsprozessen — Anforderungen, 2019.

NIST CSF 2.0 — National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 2024.

IKT-Minimalstandard (2023) — Bundesamt für wirtschaftliche Landesversorgung (BWL). Minimalstandard zur Verbesserung der IKT-Resilienz, 2023.

CSRM (2025) — Bundesamt für Cybersicherheit (BACS). *Cybersicherheits- und Resilienzmethode (CSRM) — Eine strukturierte Vorgehensweise zur Stärkung der Cybersicherheit und Resilienz*, 2025.

Cybersecurity and Physical Security Convergence — Cybersecurity and Infrastructure Security Agency (CISA). Cybersecurity and Physical Security Convergence Action Guide, 2021.

Richtlinie (EU) 2022/2555 (NIS2) — Europäisches Parlament und Rat der Europäischen Union. Richtlinie vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, 2022.

Richtlinie (EU) 2022/2557 (CER) — Europäisches Parlament und Rat der Europäischen Union. Richtlinie vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen, 2022.