

Securitas

Mehr als Regulierung: Echte Resilienz für kritische Infrastrukturen schaffen.

Sicherheit für das, was zählt

Die neuen Regeln für Sicherheit und Resilienz kritischer Infrastrukturen.



EINLEITUNG 4

GRENZENLOS UND VERNETZT – EIN NEUER HORIZONT SICH WANDELNDER BEDROHUNGEN 6
Fallbeispiel: Sicherheitsdienst vor Ort und Wärmebildkameratechnologie für Energieerzeuger 7

AUFBAU EINER RESILIENTEN SICHERHEITSARCHITEKTUR – VOM RISIKOVERSTÄNDNIS ZU MESSBAREN ERGEBNISSEN IN 5 SCHRITTEN 8

INTEGRIERTER PHYSISCHER UND DIGITALER SCHUTZ FÜR RESILIENTE 10 KRITISCHE INFRASTRUKTUREN 10
Fallbeispiel: Sicherheitsdienst und Remote Services helfen nordeuropäischen Energiebetreiber, auf das Risiko von Drohnenüberflügen zu reagieren 11

WICHTIGE SEKTOREN, DIE VON DER CRITICAL ENTITIES RESILIENCE DIRECTIVE BETROFFEN SIND 12
Fallbeispiel: Risk Intelligence unterstützt die Abläufe KRITIS-Unternehmens im Transportsektor

COMPLIANCE UND KONTROLLE ALS MANAGEMENT-AUFGABE – EINE AUFGABE FÜR DIE UNTERNEHMENSFÜHRUNG 14
Fallbeispiel: Mobile Videosicherheitslösung schützt eine Baustelle im Bereich kritischer Infrastruktur 14
Fallbeispiel: Echtzeit-Monitoring und Intelligence stärken ein globales Finanzinstitut 17

SICHERHEITSPRIORITÄTEN FÜR UNTERNEHMENS-VERANTWORTLICHE: VON COMPLIANCE ZU BUSINESS CONTINUITY UND RECOVERY 18

Inhalt

Einleitung

Kritische Infrastrukturen basieren auf enger Vernetzung und Interdependenz. Energie, Wasser, Verkehr, Bankwesen, digitale Plattformen, öffentliche Verwaltung und weitere Dienste sind inzwischen so eng miteinander verbunden, dass sich eine Störung in einem Bereich schnell auf viele andere auswirken kann. Diese Vernetzung sorgt für Effizienz, verstärkt aber zugleich Risiken. Ein lokaler Vandalismusakt an einem ungeschützten Knotenpunkt kann regionale Folgen auslösen. Der Brandanschlag auf das Berliner Stromnetz im Januar 2026 ist ein Beispiel dafür: ein Vorfall mit Tausenden Betroffenen und mehreren beeinträchtigten wesentlichen Einrichtungen und Diensten.

Vor dem Hintergrund zunehmender geopolitischer Spannungen haben sich Bedrohungsakteure diversifiziert und professionalisiert. Hybride Angriffe, die digitale und physische Vektoren kombinieren – von Sabotage vor Ort über Cyberangriffe bis hin zu Drohnenüberflügen – zielen zunehmend darauf ab, etablierte Erkennungs- und Reaktionsmechanismen zu überfordern.

Organisationen im Bereich kritischer Infrastrukturen stehen zudem vor einem neuen Kapitel der Sicherheit: Die Critical Entities Resilience Directive (CER) der Europäischen Union verpflichtet die Mitgliedstaaten, kritische Einrichtungen bis Juli 2026 zu identifizieren, und legt erhöhte Sicherheitsanforderungen fest. Analysen zufolge soll es in Europa bis 2027 mehr als 15.000[1] ausgewiesene kritische Einrichtungen geben, gegenüber nur 100 unter der früheren Richtlinie.

Mit zunehmenden regulatorischen Anforderungen und der Annäherung von Bedrohungen über physische und digitale Bereiche hinweg müssen Unternehmensverantwortliche einen stärker integrierten, intelligence-gestützten Sicherheitsansatz verfolgen. Dieser Wandel erfordert Verantwortung auf höchster Organisationsebene. Kritische Infrastruktur ist das Rückgrat gesellschaftlicher Resilienz und wirtschaftlicher Stabilität. Ihr Schutz ist daher nicht nur eine operative Aufgabe, sondern eine gemeinsame Verantwortung mit Auswirkungen, die weit über die einzelne Organisation hinausreichen.

Mitwirkende

Mike Evans
Director, Risk Intelligence Center
Securitas

Benedikt Meyer
Public Affairs
Securitas Deutschland

Claus Fibiger
Country President
Securitas Dänemark

Morten Krohn Sommer Mikkelsen
VP Solutions Offering
Securitas Europe

Gaspard Fierens
Head of Security Advisory
Securitas Europe

Marc Moris
Group Prevention & Protection Lead
Proximus

1 Umsetzung der europäischen Richtlinie zur Resilienz kritischer Einrichtungen (CER Directive): Status, Herausforderungen und internationaler Kontext - EU-CIP



Grenzenlos und vernetzt – ein neuer Horizont sich wandelnder Bedrohungen

Globale geopolitische Konfrontationen, einschließlich des ersten großen europäischen Konflikts seit über 70 Jahren, haben die Bedrohungslage für Betreiber kritischer Infrastrukturen verschärft. NATO[2] stuft Sabotage an **kritischen Infrastrukturen** inzwischen als eine der größten Sicherheitsbedrohungen ein. Hybride oder „Blended"-Angriffe mit dem Ziel, kritische Infrastrukturen zu stören, sind Teil einer sich schnell entwickelnden Bedrohungslage.

Hybride Angriffe überschreiten Grenzen so schnell wie Daten- und Medienströme. Die Digitalisierung hat die Angriffsfläche erweitert. Zugleich sind auch physische Risiken komplexer geworden, von Perimeterverletzungen bis hin zu unbemannten Flugsystemen, die auf Umspannwerke und abgelegene Anlagen abzielen. Abhängigkeiten zu erfassen, Lieferketten zu diversifizieren und Redundanzen aufzubauen, ist wesentlich. Diese Maßnahmen wirken jedoch nur dann, wenn sie mit einem integrierten Sicherheits- und Risikomanagement verbunden sind, das Risiken in Echtzeit erkennen, verifizieren und eine Reaktion einleiten kann.

„Bedrohungen für kritische Infrastrukturen respektieren keine geografischen Grenzen."

Mike Evans
Director, Risk Intelligence Center
Securitas

Mike Evans, Director, Risk Intelligence Center, Securitas, sagt: „Heute ist jede einzelne Art von Bedrohungsakteur motiviert, kritische Infrastrukturen ins Visier zu nehmen. Selbst einfache Sabotage- und Diebstahlakte können schwerwiegende Ausfälle verursachen. Einige Bedrohungen sind aufgrund der gegenseitigen Abhängigkeit moderner Infrastrukturen heute tatsächlich grenzenlos. Bedrohungen für kritische Infrastrukturen respektieren keine geografischen Grenzen. Die Geschwindigkeit, mit der sich Probleme ausbreiten, ist ein Risikofaktor an sich. Unsere Empfehlung an Unternehmensverantwortliche lautet, das Echtzeit-Monitoring regionaler Risiken zu einer zentralen Priorität zu machen."

Marc Moris, Group Prevention & Protection Lead beim ICT- und digitalen Dienstleistungsunternehmen Proximus, warnt davor, dass Organisationen proaktiv und agil handeln müssen. Er sagt: „Die Vorbereitungen zur Prävention und zum Schutz vor sich wandelnden Risiken sind in vielen Fällen noch unzureichend. Unternehmen im Bereich kritischer Infrastrukturen müssen umfassende Risikobewertungen durchführen, um angemessene präventive und schützende Maßnahmen umzusetzen und Risiken dynamischer zu bewerten."

Abhängigkeiten zu erfassen und Lieferketten zu diversifizieren, gehört zu den Prioritäten von Organisationen, die Störungen minimieren und Ausfallzeiten vermeiden wollen. Gleiches gilt für den Aufbau von Redundanzen in kritischen Systemen. Dies muss jedoch mit einem integrierten Sicherheits- und Risikomanagement verbunden werden, um vielschichtige Bedrohungen wirksam zu bewältigen.

Morten Krohn Sommer Mikkelsen, VP Solutions Offering, Securitas Europe, betont die Bedeutung der Bewertung von Lieferketten und sagt: „Kritische Infrastruktur ist Teil wesentlicher und stark vernetzter Wertschöpfungsketten. Jeder Lieferant, Subunternehmer und Dienstleister wird Teil der Resilienzfrage. Wenn ein Glied in dieser Kette fragil ist, bleibt die Wirkung nicht begrenzt, sondern breitet sich aus. Deshalb ist die Auswahl von Lieferanten heute nicht mehr nur eine kommerzielle oder beschaffungsbezogene Entscheidung. Sie ist eine Resilienzentscheidung."

Evans sagt: „Situationsbewusstsein ist für kritische Infrastrukturen wichtiger denn je. Doch die Fähigkeit, ein fundiertes Verständnis vernetzter Bedrohungen in Echtzeit zu gewinnen, wird Organisationen auszeichnen und sie in die Lage versetzen, einen Schritt voraus zu bleiben."

Situationsbewusstsein ist daher eine entscheidende Fähigkeit. Organisationen, die physische Daten wie Videoüberwachung, Zutrittsprotokolle oder Streifendaten mit Cybersignalen und externer Threat Intelligence zusammenführen, können Vorfälle schneller verifizieren und eskalieren. Dadurch lassen sich operative und gesellschaftliche

2 https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence



FALLBEISPIEL

Sicherheitsdienst vor Ort und Technologie mit Wärmebildkameras für Energieerzeuger

Ein führender privater Energieerzeuger, spezialisiert auf Wärme-, Wasser-, Solar- und Windkraftanlagen, benötigte eine Aktualisierung seiner Sicherheitsarchitektur. Ziel war es, den Perimeterschutz zu stärken, die vorhandene Sicherheitstechnik zu modernisieren und eine skalierbare Lösung über mehrere Standorte hinweg zu etablieren.

Dazu wurde eine integrierte Sicherheitslösung umgesetzt, die Bewachung vor Ort mit Remote-Video und Videoanalytik, Wärmebildkameras, Lautsprechersystemen und Bodycams kombiniert. Ergänzend wurden Brand- und weitere Sicherheitsdienste in das maßgeschneiderte Konzept eingebunden. So konnten Sicherheitsniveau, Effizienz und Skalierbarkeit des Schutzes der Anlagen messbar erhöht werden.

Aufbau einer resilienten Sicherheitsarchitektur

Die meisten Betriebsprozesse und Anlagen in KRITIS-Umgebungen sind sicherheitskritisch, was sie deutlich von anderen Betreiberlandschaften unterscheidet.

Vom Risikoverständnis zu messbaren Ergebnissen in 5 Schritten

1. VERSTEHEN
ERKENNEN, WAS ZÄHLT

Erfassen Sie kritische Werte wie Menschen, Standorte, Ausrüstung und Prozesse. Bewerten Sie mögliche Auswirkungen, um zu verstehen, wie sich Vorfälle auf die Sicherheit von Menschen, die Kontinuität, finanzielle Verluste oder die Reputation auswirken können. Schaffen Sie ein gemeinsames Verständnis von Prioritäten und Risikoakzeptanz.

2. BEWERTEN
BEDROHUNGEN UND SCHWACHSTELLEN BESTIMMEN

Nutzen Sie Open-Source-Intelligence, proprietäre Daten und lokale Erkenntnisse, um relevante Bedrohungen zu identifizieren und zu bestimmen, wie sich deren Wahrscheinlichkeit je nach Region unterscheidet. Bewerten Sie bestehende Kontrollen in den Bereichen Menschen, Prozesse und Technologie.

3. MINIMIEREN
DIE RICHTIGEN KONTROLLEN ANWENDEN

Kombinieren Sie schnelle Maßnahmen mit längerfristigen Verbesserungen in drei Bereichen: Menschen, Prozesse und Technologie.

4. STEUERN
VERBESSERUNGEN VERANKERN

Governance sollte regelmäßige Überprüfungen und die Nachverfolgung von KPIs umfassen, etwa Vorfallarten, Reaktionszeiten, Systemverfügbarkeit und Schulungscompliance.

5. WEITERENTWICKELN
MIT VERÄNDERUNGEN SCHRITT HALTEN

Bedrohungen und Schwachstellen verändern sich, wenn Organisationen wachsen und sich ihr Umfeld weiterentwickelt. Beobachten Sie neue Entwicklungen, aktualisieren Sie Verfahren, integrieren Sie gewonnene Erkenntnisse und überarbeiten Sie Risikoroadmaps zweimal jährlich.

Quelle: Securitas Global Clients Europe – Security Advisory



Integrierter physischer und digitaler Schutz für resiliente kritische Infrastrukturen

Während Digitalisierung und Vernetzung einerseits die Angriffsflächen vergrößert haben, **sind zugleich auch physische Bedrohungen komplexer geworden.** Organisationen suchen daher nach Möglichkeiten, diese Risiken zu minimieren. Kritische Einrichtungen in zentralen Sektoren müssen formale Risikobewertungen durchführen, Resilienzpläne entwickeln und technische Maßnahmen umsetzen, um Störungen zu reduzieren. Die CER-Richtlinie betont die Bedeutung physischer Sicherheit, von Zutrittskontrollen und Standortschutz bis hin zu Redundanzen und Notfallverfahren.

Benedikt Meyer, Public Affairs, Securitas Deutschland, sagt: „Was wir derzeit sehen, ist ein abgestimmter, integrierter Vorstoß hin zu ganzheitlichen physischen und Cyber-Sicherheitsarchitekturen. Investitionen in Bereiche wie robusten Perimeterschutz, Videoüberwachung und Risikobewertung werden zunehmend zu einem erwarteten, überprüfbaren Mindeststandard."

Auch Sicherheitstechnologie entwickelt sich weiter und bietet innovative Lösungen zum Schutz von Organisationen. Claus Fibiger, Country President, Securitas Denmark, sagt: „Das Interesse an Technologien zur Minimierung von Risiken für Organisationen im Bereich kritischer Infrastrukturen hat zugenommen. Wir sehen in Dänemark und in ganz Europa ein wachsendes Interesse an Drohnendetektion. Gleichzeitig nimmt auch das Interesse an robotergestützten Sicherheitsstreifen für abgelegene Anlagen zu."
Bedrohungen für kritische Infrastrukturen lassen sich heute nicht mehr klar in getrennte Kategorien einordnen. Mikkelsen sagt:

„Physische Risiken und digitale Bedrohungen sind zunehmend miteinander verbunden. Sicherheit verliert an Wirkung, wenn sie weiterhin in Silos organisiert wird. Echte Einsatzbereitschaft entsteht durch Integration: durch die Verbindung von physischem Schutz, Technologie und Intelligence sowie durch die Fähigkeit, in Echtzeit zu handeln. Der menschliche Faktor bleibt in dieser Kette entscheidend, um Reaktionen zu mobilisieren und auf Vorfälle zu reagieren."

FALLBEISPIEL

Sicherheitsdienst und Remote Services helfen nordischem Energiebetreiber, auf das Risiko von Drohnenüberflügen zu reagieren

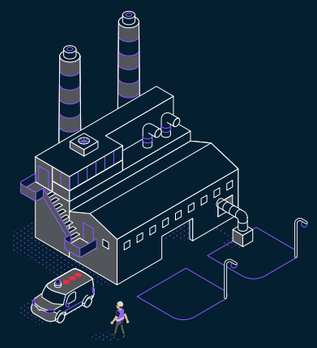
Ein großer Energieübertragungsbetreiber in Nordeuropa war an großen Umspannwerken mit Perimeterschutz dem Risiko von Drohnenüberflügen ausgesetzt.

Eine Bewertung der Bedrohung ergab, dass eine Sicherheitslösung aus stationärem Sicherheitsdienst und mobilen Interventionsteams zur Bearbeitung von Eskalationen die Sicherheit an diesen Standorten erhöhen würde. Ergänzt wurde dies durch Intelligence und Koordination über ein Securitas Operations Center (SOC).

Diese integrierte Lösung führte bei diesem wichtigen Betreiber zu einer deutlich schnelleren Verifizierung von Bedrohungen und verbesserte zugleich die Compliance-Ausrichtung der Organisation im Hinblick auf künftige Anforderungen der CER-Richtlinie sowie der Network and Information Security Directive (NIS2).

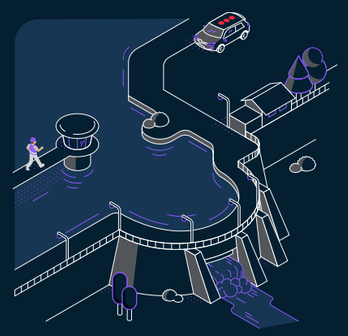
Hauptsektoren im Fokus der Critical Entities Resilience Directive

Die Critical Entities Resilience Directive (CER) ist ein EUweiter Rahmen, der 11 Sektoren adressiert: Energie, Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung, Weltraum und Lebensmittel.



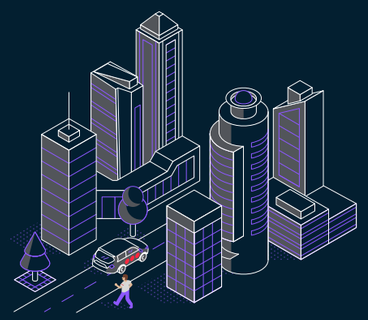
ENERGIESEKTOR

Stromerzeugung und Energiespeicherung.



WASSERSEKTOR

Trinkwasserversorgung, Trinkwasserverteilung sowie Sammlung, Behandlung und Entsorgung von Abwasser.



FINANZMARKT UND BANKWESEN

Dienstleistungen wie der Betrieb von Handelsplätzen und Clearingsystemen sowie Bankdienstleistungen mit wesentlichen Leistungen wie Einlagengeschäft und Kreditvergabe.

FALLBEISPIEL

Risk Intelligence unterstützt die Betriebsabläufe einer Organisation im Transportsektor

Ein Unternehmen aus dem Transportsektor betreibt mehrere Standorte und ist auf verlässliche Lageeinschätzungen angewiesen, um seine Sicherheitsstrategie fundiert auszurichten. Der Betreiber erhält regelmäßig Risk Intelligence Informationen zu relevanten Entwicklungen im Umfeld seiner Standorte, etwa zu Protesten, Störungen oder anderen potenziellen Risiken.

Die Informationen haben dazu beigetragen, potenzielle Bedrohungen frühzeitig zu erkennen und Sicherheitsmaßnahmen entsprechend anzupassen. Dadurch konnten die Einsatzbereitschaft verbessert und die Resilienz gestärkt werden.

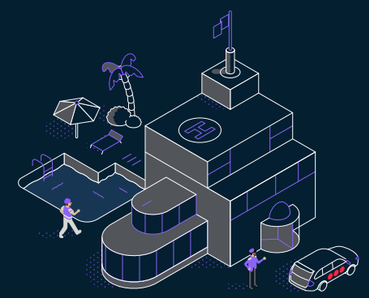
Die EU Mitgliedstaaten sind verpflichtet, bis Juli 2026 eine nationale Risikobewertung durchzuführen, um alle kritischen Einrichtungen zu bestimmen. Danach haben Organisationen unter Umständen nur 10 Monate Zeit, um die Einhaltung der Resilienzanforderungen nachzuweisen.

Zu den wesentlichen Anforderungen zählen die Durchführung von Risikobewertungen, die Umsetzung technischer und organisatorischer Resilienzmaßnahmen sowie die Meldung von Sicherheitsvorfällen. Die Richtlinie soll sicherstellen, dass Betreiber in der Lage sind, verschiedene Störungen zu verhindern, ihnen standzuhalten, darauf zu reagieren und sich davon zu erholen.



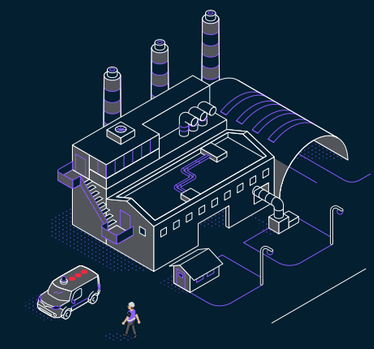
DIGITALE INFRASTRUKTUR

Dienstleistungen wie die Bereitstellung und der Betrieb von Internetknoten, Domain Name Systemen, Top Level Domains, Cloud Computing und Rechenzentren.



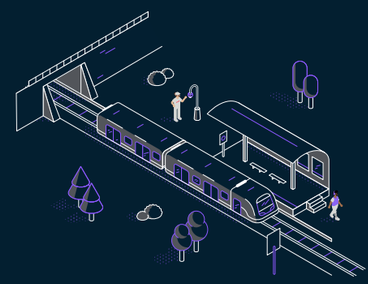
GESUNDHEITSWESEN

Verteilung, Herstellung und Bereitstellung von Gesundheitsleistungen und medizinischen Dienstleistungen.



PRODUKTION, VERARBEITUNG UND VERTEILUNG VON LEBENSMITTELN

Groß angelegte industrielle Lebensmittelproduktion und Lebensmittelverarbeitung, Dienstleistungen entlang der Lebensmittelversorgungskette sowie Großhandelsvertrieb von Lebensmitteln.



TRANSPORTSEKTOR

Dienstleistungen wie das Management und die Instandhaltung von Flughafeninfrastruktur oder Schieneninfrastruktur.



ÖFFENTLICHE VERWALTUNG

Behörden und öffentliche Einrichtungen, die zentrale staatliche und gesellschaftliche Funktionen sicherstellen.

Compliance und Kontrolle als Management-Aufgabe

Die CER-Richtlinie und weitere regulatorische Rahmenwerke spielen eine wichtige Rolle bei der Weiterentwicklung der Sicherheit kritischer Infrastrukturen. Sie machen Resilienz von einer freiwilligen Best Practice zu einer gesetzlich verankerten Führungs- und Governance-Aufgabe. Vor diesem Hintergrund hat sich Resilienz von einer technischen Maßnahme zu einer strategischen Priorität auf Vorstandsebene entwickelt.

Fibiger sagt: „Es ist wichtig, CER nicht nur als Compliance-Thema zu betrachten. Richtlinien sind nicht nur regulatorische Belastungen. Sie sind strategische Treiber, die Entscheidungen und Investitionen auf Vorstandsebene prägen. Es geht um Führung, Risikobewusstsein und langfristige Wettbewerbsfähigkeit. Organisationen, die ihre Rolle innerhalb der Wertschöpfungsketten verstehen, in denen sie tätig sind, können Resilienz als Stärke nutzen und sie nicht nur als regulatorische Anforderung betrachten. Wenn Resilienz in Managementpraktiken und operatives Denken integriert wird, wird sie zu einem strategischen Vorteil.“

Während ein hohes Maß an Resilienz in Sektoren wie Energie häufiger anzutreffen ist, können robuste Sicherheit und die Umsetzung von Sicherheitskontrollen je nach Sektor sehr unterschiedlich ausgeprägt sein. Auch die Vorbereitung auf Sicherheitsvorfälle ist nicht überall ausreichend. In ganz Europa rückt das regulatorische Umfeld stärker in den Fokus. Nationale Umsetzungen der CER-Richtlinie treten in Kraft. Ein Beispiel dafür ist das deutsche KRITIS Dachgesetz[3].

FALLBEISPIEL

Mobile Videosicherheitslösung schützt Baustelle kritischer Infrastruktur

Bei der Planung eines großen Modernisierungsprojekts für die Schieneninfrastruktur wurden zwei große Gasleitungen entdeckt, die den geplanten Bau beeinträchtigten. Diese unerwartete Herausforderung musste kurzfristig gelöst werden, damit das Projekt im Zeitplan bleiben konnte. Die bestehenden Gasleitungen mussten durch den nationalen Gasversorger umgeleitet werden. Gleichzeitig war zusätzliche Sicherheitstechnik erforderlich, um die Baustelle während des gesamten Prozesses zu schützen.

Zum Einsatz kam eine mobile Videolösung mit integrierter Videoanalyse. Zusätzlich wurde eine Fernanbindung an das lokale Securitas Operations Center eingerichtet. So konnten Wärmeentwicklung und Perimeter kontinuierlich überwacht werden.

SOC-Mitarbeitende standen rund um die Uhr bereit, um in Echtzeit auf Alarme zu reagieren.

Im Falle eines Vorfalls koordinierten die Mitarbeitenden die geeigneten Einsatzkräfte und konnten über mit dem SOC verbundene Lautsprecher Durchsagen vor Ort machen.

3 https://www.bundesregierung.de/breg-en/news/cabinet-kritis-umbrella-law-2404992



„Wer Compliance nur als Abhaken von Vorgaben versteht, ist dadurch nicht automatisch sicher.“

Mike Evans
Director, Risk Intelligence Center
Securitas



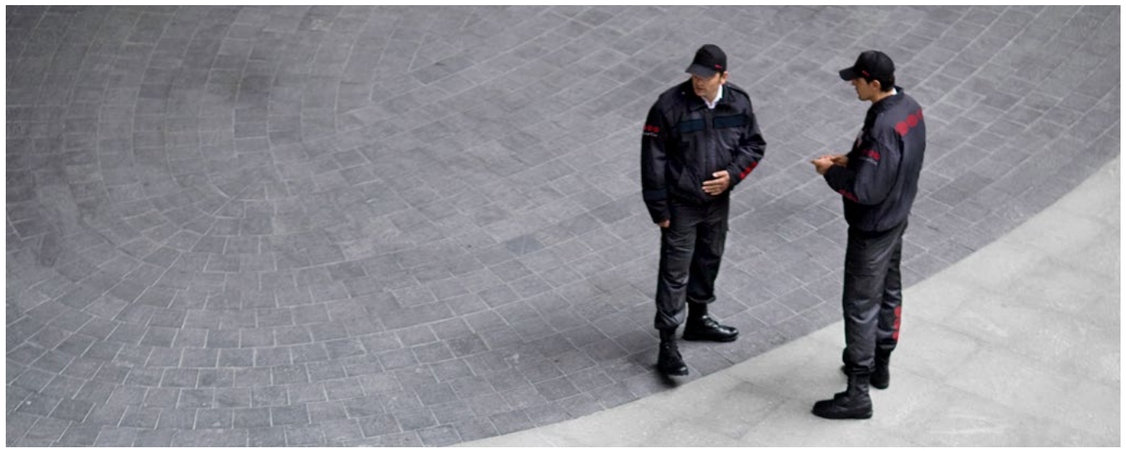
Der regulatorische Rahmen soll in erster Linie kritische Einrichtungen identifizieren. Organisationen, die mehr als 500.000 Menschen versorgen, werden als KRITIS eingestuft. Akteure in dieser Kategorie müssen Sicherheitsvorfälle innerhalb von 24 Stunden melden. Bei Verstößen können Bußgelder von bis zu 1 Million Euro drohen.

Physische Sicherheit ist ein zentraler Bestandteil der Einhaltung von Vorgaben wie der CER-Richtlinie und dem KRITIS Dachgesetz. Diese Rahmenwerke betonen die Bedeutung eines angemessenen Perimeterschutzes, einer wirksamen Zutrittskontrolle, von Überwachung und Monitoring, Sicherheitsdiensten sowie Alarmanlagen.

Meyer sagt: „Die Gesetzgebung schreibt verpflichtende Risikobewertungen, Meldepflichten und Anforderungen an die physische Sicherheit vor. Wichtig ist aber auch: Compliance markiert einen großen Schritt hin zu einem umfassenden, sektorübergreifenden Schutz kritischer Infrastrukturen.“

Moris sagt: „Europa hat bei der Entwicklung neuer Gesetzgebung viel erreicht. Compliance darf für Organisationen im Bereich kritischer Infrastrukturen jedoch nicht zum Selbstzweck werden. Unternehmensleitungen müssen berücksichtigen, dass Kriminelle außerhalb gesetzlicher Rahmenbedingungen agieren und Risiken kontinuierlich bewertet werden sollten.“

Evans ergänzt: „Compliance ist unverzichtbar. Die sich weiterentwickelnden Rahmenwerke tragen dazu bei, das Sicherheitsniveau insgesamt zu erhöhen. Compliance wie eine reine Pflichtübung zu behandeln, macht Sie jedoch nicht sicher. Sie sollte beim Schutz kritischer Infrastrukturen als Ausgangspunkt verstanden werden, nicht als Endziel.“



FALLBEISPIEL

Echtzeit Monitoring und Intelligence unterstützen ein globales Finanzinstitut

Eine weltweit tätige Organisation an der Spitze der Finanzdienstleistungsbranche sah sich mit einer zunehmenden Zahl von Vorfällen konfrontiert. Bedrohungen wirkten sich auf Mitarbeitende, Ressourcen und zentrale Geschäftsabläufe aus.

Im bestehenden Berichtssystem zur Erfassung von Bedrohungen wurden Schwachstellen identifiziert. Diese schränkten sowohl die Resilienz als auch die künftige Compliance ein.

Daraufhin wurde ein individuell zugeschnittener Intelligence Service eingerichtet, der auf Echtzeit Monitoring basiert. Er umfasst Alarmierung rund um die Uhr, Frühwarnungen und Krisenunterstützung. Dadurch wurde ein vorausschauender Umgang mit Bedrohungen und eine robuste Reaktion ermöglicht.

Regelmäßige Intelligence Updates wurden eingeführt, um fortlaufend Transparenz über die Bedrohungslage zu schaffen. Zudem wurde ein Executive Protection Screening eingerichtet, um Personen zu schützen, die gezielten Bedrohungen ausgesetzt sind. Ergänzend wurde ein Dedicated Request for Intelligence Service aufgebaut. Über diesen können Fachleute gezielt Informationen zu spezifischen Bedrohungen bereitstellen.

Diese individuell angepassten und integrierten Services haben dazu beigetragen, Sachschäden, Bedrohungen gegen Mitarbeitende und potenziell störende Proteste zu reduzieren. Durch mehr Kontrolle und klarere Entscheidungsgrundlagen berichtete die Organisation aus dem Finanzdienstleistungssektor von Verbesserungen im globalen Betrieb.

Sicherheit als Führungsaufgabe: von Compliance zu Business Continuity und Recovery

Der Umgang mit der zunehmenden Verbindung physischer und digitaler Bedrohungen hat für Verantwortliche kritischer Infrastrukturen höchste Priorität. Überwachung, Intelligence und Reaktionsfähigkeit müssen im Rahmen eines abgestimmten Sicherheitsansatzes zusammengeführt werden. Jeden Sabotageakt, jede Insider-Bedrohung und jeden Systemausfall vollständig zu verhindern, ist nicht mehr realistisch. Umso wichtiger sind mehrschichtige Resilienz und wirksame Reaktionsmaßnahmen.

Evans sagt: „In einer Welt, in der hybride Bedrohungen gezielt darauf ausgelegt sind, größtmögliche gesellschaftliche Auswirkungen zu erzielen, war integrierte Sicherheit über physische und digitale Ebenen hinweg noch nie so wichtig."

Auch Zusammenarbeit und Abstimmung zwischen den beteiligten Akteuren sind entscheidend. Moris sagt: „Zusammenarbeit muss über die Trennung zwischen öffentlichem und privatem Sektor hinausgehen und auch Partnerschaften innerhalb der Privatwirtschaft einschließen. So lassen sich Fachwissen, Ressourcen, Innovation und Allianzen zwischen Unternehmen nutzen. Die Abstimmung zwischen Betreibern kritischer Infrastrukturen, Dienstleistern und öffentlichen Behörden bleibt wesentlich. Sicherheitsdienstleister spielen eine zentrale Rolle dabei, größere Vorfälle einzudämmen und zu bewältigen."

Regulatorische Vorgaben und Rahmenwerke wie die CER-Richtlinie sollten nicht nur als Compliance-Verpflichtungen verstanden werden, sondern als **strategische Chancen, um Vorbereitung, Widerstandsfähigkeit und langfristige Wettbewerbsfähigkeit zu stärken.**

Fibiger fasst zusammen: „Wer bei der Vorbereitung frühzeitig handelt, kann wirksamer reagieren, wenn die Anforderungen steigen. Die am besten vorbereiteten Organisationen gehen gestärkt daraus hervor. Sie sind glaubwürdiger im Kundendialog und verlässlicher in der operativen Umsetzung."

Organisationen, die diese Haltung übernehmen, Sicherheit integrieren, wirksam mit Partnern zusammenarbeiten und Regulierung als Hebel für Resilienz nutzen, sind in einer zunehmend volatilen Risikolandschaft am besten aufgestellt.

Securitas gestaltet die Zukunft der Sicherheitsbranche aktiv mit. Wir verbinden unsere Expertise in einzelnen Leistungen wie Remote Services, mobilen Sicherheitsdiensten und Sicherheitsdiensten vor Ort, Fire & Safety sowie Sicherheitstechnik zu innovativen Sicherheitslösungen, die auf die vielfältigen Anforderungen unserer Kunden zugeschnitten sind. Unterstützt durch Risk Intelligence bleiben wir neuen Bedrohungen einen Schritt voraus.

Genau wie Ihr Unternehmen sind auch unsere Sicherheitslösungen darauf ausgelegt, sich anzupassen und mitzuwachsen. Mit unserer globalen Präsenz sind wir stolz darauf, für Unternehmen weltweit ein vertrauensvoller Sicherheitspartner zu sein.