AMSTEIN+WALTHERT

zB

No. 67 11.2015

Schutz kritischer Infrastrukturen

Kritische Infrastrukturen (KI) stellen in unserem Land die Verfügbarkeit von essenziellen Gütern und Dienstleistungen, wie etwa Energie, Kommunikation oder Verkehr, sicher. Sie leisten damit einen Beitrag zum Wohle der Bevölkerung und einer funktionierenden Wirtschaft. Strategien zum Schutz kritischer Infrastrukturen sind auf Stufe des Bundes in Umsetzung; auch viele Unternehmen beschäftigen sich mit dem Thema. In welchem Masse ist ihr Unternehmen von kritischen Infrastrukturen abhängig? Welche Risikofaktoren sind in der Planung von kritischen Infrastrukturen zu beachten, welche im Betrieb? Welcher Schutz ist angemessen und was versteht man unter dem Begriff «Integrale Sicherheit»? Diese Fragen beleuchten wir in diesem zB.

In der Schweiz erfreuen wir uns einer konstanten Versorgung mit wichtigen Gütern wie Wasser, Lebensmittel, Energie und Information. Die Verfügbarkeit dieser Güter wird als selbstverständlich erachtet und oft wird vergessen, welche Infrastrukturen zu deren Bereitstellung notwendig sind. Gleichzeitig sind Unternehmen wie auch Privatpersonen zunehmend von der hohen Verfügbarkeit dieser Güter und somit auch von den kritischen Infrastrukturen abhängig.
Aus Sicht der Unternehmen wie auch der Bevölkerung ist es essenziell, die gegenseitigen Abhängigkeiten zu erkennen und Ausfallrisiken zu minimieren.

Auf Bundesebene existiert dazu eine breit abgestützte Strategie, aber auch private Unternehmen müssen sich mit Fragen zu Risiken und angemessenen Massnahmen vertieft befassen.

Nationale Strategie zum Schutz kritischer Infrastrukturen

Im Jahr 2012 wurde die nationale SKI-Strategie durch den Bundesrat verabschiedet. Diese hat zum Ziel, die Widerstandsfähigkeit der Schweiz in Bezug auf kritische Infrastrukturen zu stärken und somit die Ausfallrisiken zu mindern. Die SKI-Strategie teilt die Infrastruktur in 10 Sektoren und 28 Teilsektoren ein und ordnet diesen jeweils eine Kritikalität (Wichtigkeit) zu.

Behörden	**Gesundheit**
Industrie	**Information und Kommunikation**
Energie	**Nahrung/Wasser**
Entsorgung	**Öffentliche Sicherheit**
Finanzen	**Verkehr**

1 Die 10 Sektoren gemäss SKI-Strategie

Die SKI-Strategie definiert zur Zielerreichung insgesamt 15 Massnahmen, welche von übergeordneten behördlichen Massnahmen bis hin zu objektspezifischen Analysen durch die Betreiber reichen. Beispielsweise wurden die Abhängigkeiten der KI untereinander vertieft untersucht und ein objektspezifisches Inventar der KI erstellt. Die durch das Programm SKI geleisteten Vorarbeiten können für einzelne Unternehmen interessante Hinweise auf die eigenen Abhängigkeiten und Risiken liefern.

Integrale Sicherheit herstellen

Was hat ein Data Center, ein Spital, und eine Verkehrsleitzentrale gemeinsam? Aus unserer Sicht sind es die hohen Anforderungen an die Verfügbarkeit. Daraus ergeben sich Anforderungen an die Konzeption von Systemen, an die Schutz- und Überwachungsmassnahmen und natürlich an die involvierten Organisationen. Eine auf die Kernaufgabe abgestimmte Massnahmenstrategie, die sämtliche Risiken adäquat berücksichtigt, ist erforderlich. Wir reden in diesem Fall von integraler Sicherheit.

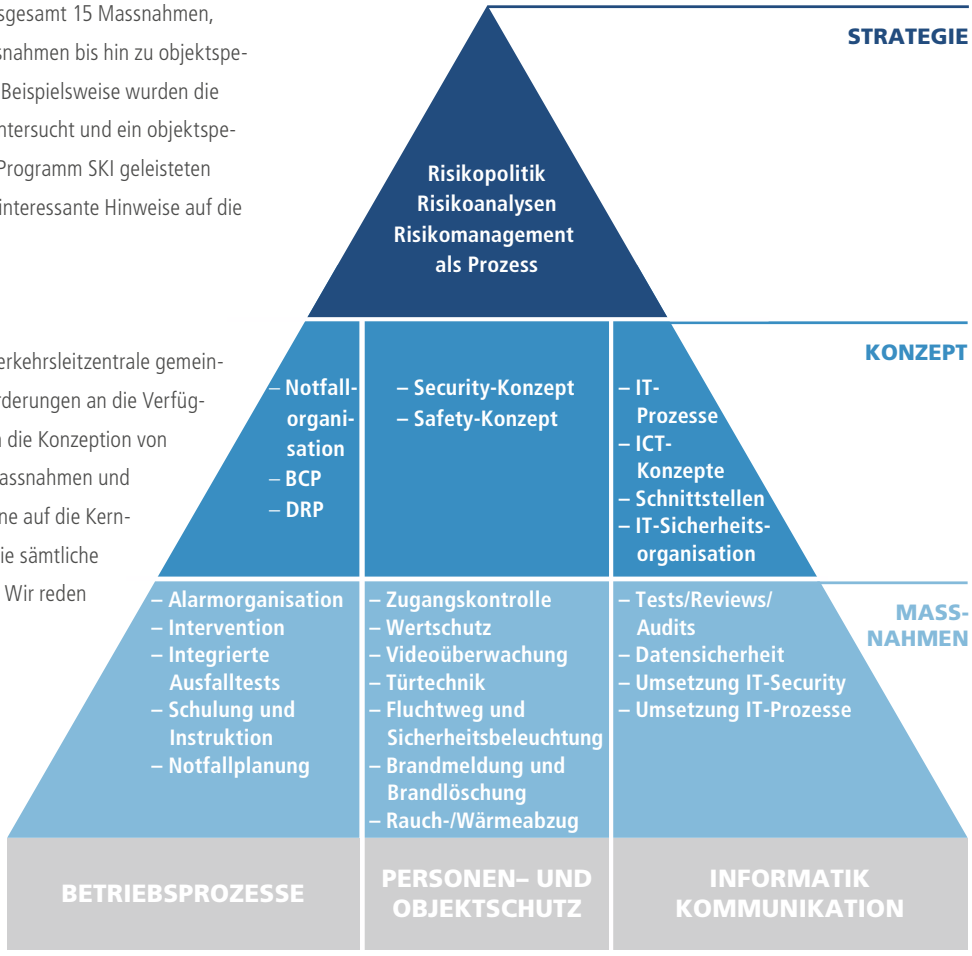
Individuelles Risikoprofil

Die Risiken bezüglich Infrastruktur sind in jedem Unternehmen je nach Standort, Geschäftsfeld, Markt, Personen, Prozessen und Abhängigkeiten unterschiedlich. Dabei können aktive Risiken wie zum Beispiel Sabotage oder gezielter Diebstahl von Informationen ebenso bedeutend sein wie standortspezifische Naturgefahren oder interne Risiken wie technische Ausfälle oder Brände. Um einen angemessenen Schutz zu entwickeln, ist eine Auslotung der Risiken unerlässlich, sei dies für bestehende Infrastrukturen oder im Rahmen von Projekten.

Strategie, Konzept, Massnahmen

Integrale Sicherheit muss top-down von der Strategie über die Konzepte zu den Massnahmen entwickelt werden. Grössere Unternehmen besitzen ein Risikomanagement-System, welches auf strategischer Ebene verankert ist. Daraus werden die verschiedenen Konzepte abgeleitet. Auf der Massnahmenebene befinden sich detaillierte Arbeitsanweisungen, Prozesse und Hilfsmittel für die operativ tätigen Personen. Werden diese Systeme und Konzepte implementiert, die Prozesse gelebt und die nötigen Massnahmen umgesetzt, so kann integrale Sicherheit erzeugt und langfristig erhalten bleiben.

Umgekehrt, sprich bottom-up, funktioniert es nicht. Eine sicherheitstechnische Pflästerchenpolitik, bei welcher immer nur punktuell und losgelöst von übergeordneten Zielen investiert wird, ist unbedingt zu vermeiden.



2 Pyramiden-Modell integrale Sicherheit

AMSTEIN + WALTHERT

Physische Sicherheit

Die physische Sicherheit von Personen, Gütern und Informationen ist eine wichtige Komponente der integralen Sicherheit. Um ein stimmiges Sicherheitskonzept zu erzeugen, müssen aus der übergeordneten Risikoanalyse die massgebenden Szenarien abgeleitet und die entsprechenden Schutzziele definiert werden. Nur durch den konsequenten top-down Ansatz entstehen optimale Lösungen. Ein Beispiel: Was nützen starke Türen und Fenster wenn die Überwachung der Bauteile lückenhaft und die Intervention schlecht organisiert ist? Das Zusammenwirken von baulichen, technischen und organisatorischen Faktoren ist in der physischen Sicherheit entscheidend.

Strom und Kälte

Längere Stromausfälle sind in der Schweiz selten, dennoch müssen Betreiber von kritischen Infrastrukturen entsprechende Massnahmen vorsehen. Spitäler, Banken, Rechenzentren, Kommunikationsdienstleiter aber auch die Verwaltung müssen sich mit dem Szenario Stromausfall befassen und risikogerechte Konzepte realisieren. Durch USV-Anlagen und Notstromgeneratoren kann das Risiko minimiert werden. Aber Vorsicht: Auch im Bereich der Kälteversorgung braucht es vermehrt Abklärungen in Bezug auf Verfügbarkeit. Eine hochverfügbare Stromversorgung allein bringt wenig, wenn die Schwachstelle (Single Point of Failure) in der Kälteversorgung steckt. Auch hier sind ganzheitliche Betrachtungen sämtlicher kritischen Systeme notwendig, um die übergeordneten Ziele zu erreichen.

Je früher desto besser

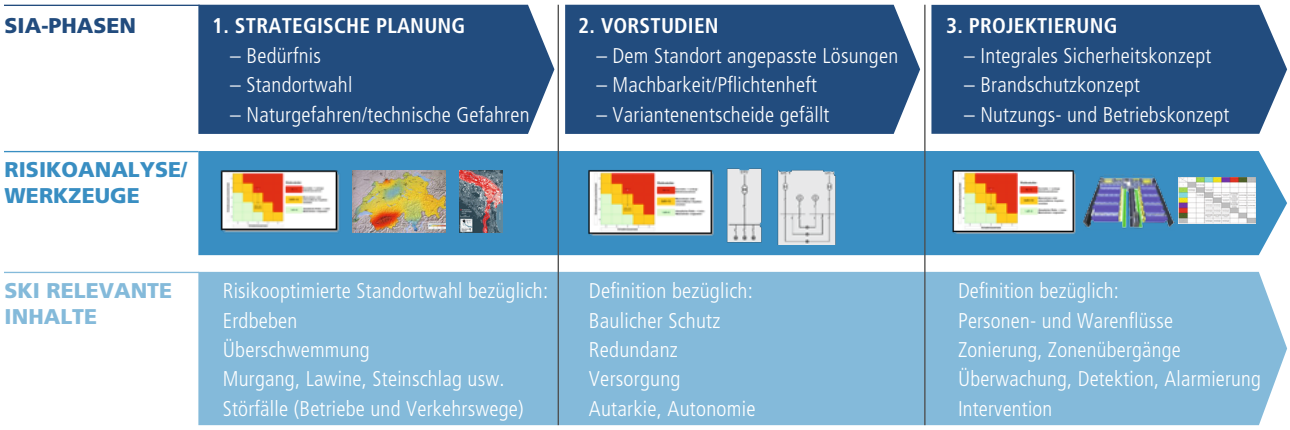
Grundsätzlich sollen Risiken und daraus abgeleitete bauliche und technische Sicherheitsmassnahmen möglichst früh in einem Projekt analysiert werden. Beispielsweise kann ein falscher Standortentscheid für eine kritische Infrastruktur später in der Betriebsphase zu unverhältnismässigen Kosten führen, wenn Schäden auftreten oder Risiken durch teure bauliche Massnahmen minimiert werden müssen. Die Standortwahl ist in Bezug auf viele Umweltrisiken relevant. Auch sind grundsätzliche Fragen der Erschliessung, Erreichbarkeit, physischer Schutz und Redundanz entscheidend. Wenn die Risiken für die Betriebsphase bereits frühzeitig im Projekt analysiert werden, so können die nötigen Massnahmen in der Planung effizient definiert und integriert werden: je früher, desto besser.

Zusätzliche Anforderungen an KI-Betreiber?

Im Moment besteht keine gesetzliche Grundlage, um KI-Betreiber zu zusätzlichen Sicherheitsmassnahmen zu verpflichten. Das Stichwort lautet Eigenverantwortung. Im Rahmen des Programms SKI sind die Betreiber von kritischen Infrastrukturen jedoch aufgefordert, die Resilienz (Widerstandsfähigkeit) ihrer im SKI-Inventar eingetragenen Objekte zu überprüfen, integrale Schutzkonzepte zu erstellten und die Massnahmen daraus umzusetzen. Gemäss dem Zeitplan in der nationalen SKI-Strategie, sollten integrale Schutzkonzepte für Objekte im SKI-Inventar ab 2015 vorliegen.

Fazit

In einer hochtechnisierten und vernetzten Welt mit vielen gegenseitigen Abhängigkeiten können Ausfälle von kritischen Infrastrukturen grosse Folgen für Bevölkerung und Wirtschaft haben. Es stellt sich daher für Unternehmen die Frage nach einer angemessenen Risikostrategie beim Erstellen und Betreiben von kritischen Infrastrukturen. Eine Überprüfung der Risikosituation im Gesamtkontext ist sinnvoll, denn meist fehlt eine übergeordnete, prozess- und ressourcenorientierte Risikobetrachtung und daraus abgeleitet Massnahmen zur integralen Sicherheit. Die durch das Programm SKI erarbeiteten Grundlagen können dabei eine Hilfestellung leisten.
Eine risikobasierte Standortwahl, frühzeitige Abklärungen bezüglich Redundanzen sowie Definition der Ziele in der physischen Sicherheit sind wichtige Faktoren in der Planung von kritischen Infrastrukturen. Durch zeitgerechte Abklärungen kann die Hebelwirkung der frühen Planungsphasen genutzt und kostspielige Massnahmen in der Bewirtschaftung vermieden werden.



3 Planung kritische Infrastrukturen

AMSTEIN + WALTHERT

DIENSTLEISTUNGSANGEBOT

- Risikomanagement, Risikoanalysen und integrale Sicherheitskonzepte für Spitäler, Banken, Data Center, Leitstellen, Infrastrukturanlagen, usw.
- Gesamtplanungen für Spitäler, Data Center, usw.
- Sicherheitsberatung, Sicherheitsplanung
- Brandschutzberatung, Brandschutzplanung
- Planung hochverfügbarer Energie- und Kälteversorgungsanlagen
- Planung hochverfügbarer ICT-Anlagen
- Zuverlässigkeits- und Verfügbarkeitsanalysen
- Projektbezogenes Qualitätsmanagement (PQM)
- Standortanalysen und Technikstandards für Data Center
- Risikoanalysen und Testkonzepte Verkehrsbetriebe
- Risikoanalysen und Sicherheitsprüfungen für Strassentunnel
- Planung Betriebs- und Sicherheitsausrüstung Strassentunnel und offene Strecken
- Risikobasiertes Instandhaltungsmanagement
- RAMS-Analysen, PQM und Validierung Bahntechnik
- Facility Management Beratung
- Integrale Tests
- Reviews und Audits von Sicherheitsorganisationen

KONTAKT

Robert Schneider
Dipl. El. Ing. ETH
robert.schneider@amstein-walthert.ch

Stephen Lingwood
Dipl. El. Ing. ETH
stephen.lingwood@amstein-walthert.ch

Urs Welte
Dipl. El. Ing. ETH
urs.welte@amstein-walthert.ch

Amstein + Walthert AG
Andreasstrasse 11
Postfach
CH-8050 Zürich
Tel. +41 44 305 91 11
Fax +41 44 305 92 14

www.amstein-walthert.ch