

newsletter

zum Thema **Kritische Informations-Infrastrukturen (CII)**

Die Abhängigkeit Kritischer Infrastrukturen von Informations- und Kommunikationstechnologien nimmt kontinuierlich zu. Als Folge dieser Entwicklung ergeben sich für viele essentielle Strukturen des Staates, der Gesellschaft und der Wirtschaft neue Bedrohungen und Verwundbarkeiten, die sich auch auf die Risikolandschaft für die Assekuranz auswirken.

Begriffs- erklärung

Gemäß der Definition des BSI (Bundesamt für Sicherheit in der Informationstechnik) sind Kritische Infrastrukturen Organisationen und Einrichtungen mit hoher Bedeutung für das Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Auswirkungen zur Folge hätten. Zu den Kritischen Infrastrukturen gehören u.a. die Sektoren Energieversorgung (Anlagen und Netze), Wasserversorgung, Verkehr sowie die medizinische Versorgung.

Unter Kritischen Informations- Infrastrukturen (engl. Critical Information Infrastructure CII) versteht man, den auf Informations- und Kommunikationstechnologien (IKT) basierenden Teil der Kritischen Infrastrukturen, d. h. die Telekommunikationseinrichtungen, Netzwerke, Computer und die dazugehörige Software.

Rahmen- bedingungen

Mit der zunehmenden Durchdringung aller Lebensbereiche mit Informations- und Kommunikationstechnik (IKT) ist unsere Gesellschaft inzwischen in vielen Bereichen von diesen Technologien abhängig geworden. Diese Abhängigkeit besteht vor allem in den Segmenten der Kritischen Infrastrukturen, in denen in zunehmendem Maße Informationstechnologien auf Basis des Internets und der Funkkommunikation eingesetzt werden. Eine Reihe weiterer Rahmenbedingungen führen zu weiteren Gefährdungsdimensionen und einer hohen Komplexität der Risiken von Kritischen Infrastrukturen:

- Unternehmensübergreifende Vernetzung
- Unternehmensfusionen
- Rationalisierung
- Länderübergreifende Verbindung
- Globalisierung der Wertschöpfungsketten
- Verschärfter Wettbewerb (Kostendruck!)

Auf Grund dieser Abhängigkeiten können lokale Störungen unvorhergesehene Kettenreaktionen mit massiven, weitreichenden Ausfällen auslösen. (Beispiele hierfür sind die weitreichenden Stromausfälle im europäischen Übertragungsnetz im Jahre 2003 in Italien und 2006 in großen Teilen Europas).

Szenarien und Gefährdungen

Kritische Infrastrukturen sind gegenüber einer Vielzahl von Gefährdungen exponiert, die Palette möglicher Szenarien reicht von Naturgefahren, technischem Versagen, Unfällen bis hin zu zielgerichteten Angriffen mit kriminellen oder terroristischem Hintergrund. Vor dem Hintergrund der Diskussionen über den Klimawandel erwarten Experten zunehmende Wetterextreme (schwere Stürme, hohe Niederschlagsmengen, lange Hitzeperioden), wovon Kritische Infrastrukturen in besonderem Maße betroffen wären.

Neben diesen Gefährdungen sind „man made hazards“ ein weiteres Bedrohungspotential: Neben Sabotage und kriminellen Handlungen können vor allem System- und Netzfehler die Verfügbarkeit von Infrastrukturen gefährden und große Schadenereignisse zur Folge haben. Dabei spielt vornehmlich die Vernetzung in und zwischen den Infrastruktursektoren durch Informationstechnologien eine entscheidende Rolle. Durch die zunehmende Komplexität der weltweit vernetzten IT-Systeme in Verbindung mit industriespezifischen kurzen Innovationszyklen und den Trend zur Standardisierung von IT-Lösungen stellt der Einzug der Informationstechnologie im Bereich der Kritischen Infrastrukturen einen besonderen Risikofaktor dar.

Angriffe auf CII Beispiele

In der Vergangenheit kam es bereits vereinzelt zu Angriffen auf IT-Systeme Kritischer Infrastrukturen:

- *Attacke auf die Wasserversorgung (Queensland/Australien, April 2000): Ein entlassener Angestellter der Stadtwerke einer Gemeinde wollte sich rächen und drang mit Hilfe seines Laptops über eine drahtlose Verbindung in das Wasserkontrollsystem seines ehemaligen Arbeitgebers ein. Er öffnete Schleusentore, woraufhin sich große Mengen Abwasser in das örtliche Flusssystem ergossen.*
- *Der Computerwurm Slammer gelangte Anfang 2003 in das Kontrollnetzwerk des Atomkraftwerkes Davis-Besse (Ohio), blockierte das digitale Kontrollsystem und setzte es für fast 5 Stunden außer Betrieb. Ein Schaden konnte verhindert werden, da es ein analoges Backup-System gab.*

Fazit

Kritische Infrastrukturen waren bis vor kurzer Zeit noch relativ unabhängig voneinander, da sie meist auf Grundlage von proprietären Systemen geplant und erstellt wurden. Dieser Status ist im Wandel begriffen, hin zu immer mehr auf Informations- und Kommunikationstechnologien aufbauenden Systemen. Von entscheidender Bedeutung ist hierbei der Einsatz von Internettechnologien, da diese die bis dato relativ abgeschotteten Infrastrukturen gegenüber den weltweiten Datennetzen und damit neuen Risikopotentialen wie Computerviren, Denial of Service- oder Hackerattacken verwundbar machen. Die Abhängigkeit Kritischer Infrastrukturen von Informationstechnologien wird weiter zunehmen. Telekommunikation und Stromversorgung bilden dabei die Kern-Infrastrukturen. Daher kann eine Kritische Infrastruktur ohne adäquat geschützte IT-Systeme heute wie in der Zukunft ihre Funktion nicht mehr erfüllen.

Im Global Risk Report des World Economic Forums von 2008 wird ein Angriff oder ein Systemversagen im Bereich der Kritischen Informations- Infrastrukturen zu den größten aktuellen globalen Risiken gezählt. Insbesondere das Versagen von IT-abhängigen Infrastrukturen und ein dadurch ausgelöster Dominoeffekt kann zu weitreichenden Ausfällen in verschiedenen Infrastruktur-Sektoren führen. Entsprechend hoch ist das Schadenpotenzial, das sich auf Grund von Ausfällen und Störungen Kritischer Informations-Infrastrukturen ergibt.

Hinweise für das Underwriting

Die gegenseitigen Abhängigkeiten, insbesondere von Energieversorgung und Informationstechnologien, können sich in Form von Kaskaden- oder Dominoeffekten potenzieren und damit ein besonders hohes unternehmens- und länderübergreifendes Schadenpotential entwickeln.

Es ist daher notwendig, bei der Risikoerfassung Kritische Infrastrukturen zunehmend aus der Perspektive der eingesetzten IKT-Systeme, d.h. deren Zuverlässigkeit und Verfügbarkeit zu beurteilen.

Die zunehmende IT-Durchdringung und Vernetzung im Bereich der Kritischen Infrastrukturen lassen großflächige Störungen und Ausfälle zukünftig wahrscheinlicher werden, die sich auf Grund von Wechselwirkungen auf nahezu alle anderen Infrastrukturen auswirken. Oftmals sind die durch ein Ausfallereignis im Infrastrukturbereich hervorgerufenen Folge- oder Sekundärschäden um ein Vielfaches höher als der Schaden innerhalb der betroffenen Infrastruktur selbst.

Versicherungsseitig können sich Störungen und Ausfälle in Infrastrukturen sowohl auf Haftpflicht- als auch auf Sachversicherungs-Deckungen in vielen Versicherungsprodukten auswirken. Beispielhaft zu nennen sind Haftungen aus „failure to supply“ oder Betriebsunterbrechungen auf Grund eines Ausfalls externer Netze. Die Schadenszenarien haben bei entsprechend großen Ausfalldimensionen ein erhebliches Kumulpotential. Derartige Kumulschadenszenarien können auf Grund der Abhängigkeiten und der Komplexität der Systeme nur bedingt erfasst und bewertet werden. Hierin liegt eine besondere Herausforderung für Risk Engineering und Produktentwicklung. Als Folge der dynamischen Entwicklung der Informationstechnologien sind CII-Strukturen heute einem stetigen und beschleunigten Veränderungsprozess unterworfen. Technische Neuerungen und regulatorische Entwicklungen haben vor diesem Hintergrund einen erheblichen Einfluss auf Sicherheitsaspekte bei CII und bedürfen aus Versicherersicht einer stetigen Beobachtung.

Kontakt

AssTech GmbH
Postfach 1211
85766 Unterföhring bei München
Telefon + 49 89 3844-1585
Telefax + 49 89 3844-1586
info@asstech.com
www.asstech.com