DuD
Datenschutz und Datensicherheit

# Kritische IT-Infrastrukturen

Volker Hammer

*Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.*

Informations- und Kommunikations-Systeme nehmen eine immer wichtigere Rolle für die Produktion und den Handel mit Gütern, die Bereitstellung von Dienstleistungen und die öffentliche Verwaltung ein. Oft können im Falle einer IT-Störung die eigentlichen sozialen Funktionen nicht mehr aufrecht erhalten werden. Als *kritische IT-Infrastruktur* werden solche IT-Infrastrukturen bezeichnet, deren Störung zu schweren Schäden für Unternehmen oder die Gesellschaft führen kann. Unter Infrastruktur wird dabei die Gesamtheit der technischen und baulichen Einrichtungen, des Personals und der organisatorischen und rechtlichen Regeln verstanden, die erforderlich sind, um die notwendigen Informations- und Kommunikationsdienste zu erbringen.

## Kritikalität

Ob eine IT-Infrastruktur als kritisch eingestuft werden sollte, hängt insbesondere von der Höhe des möglichen Schadens ab. Immer dann, wenn bereits sehr wenige oder sogar nur ein einziger Störfall die Existenz des betroffenen sozialen Systems bedroht, handelt es sich um eine kritische IT-Infrastruktur. Dabei sind die Schäden an der Technik in der Regel vernachlässigbar. Die relevanten Schadenspotentiale ergeben sich beispielsweise aus dem Verlust von Kunden, zusätzlicher Arbeitszeit, monetären Verlusten oder Umweltschäden.

Ob Handlungsbedarf zur Verminderung der Kritikalität gesehen wird, hängt in der Regel aber auch von der Wahrscheinlichkeit des Eintretens einer solchen schweren Störung ab. Dabei sind Fehler oder Naturereignisse und Angriffsmöglichkeiten zu unterscheiden. Eine hohe Kritikalität ist immer dann anzunehmen, wenn ein Störfall mit hohem Schadenspotential im Verlauf einiger Jahre auftreten kann oder ein Angriff möglich erscheint. Angriffe dürften dabei um so unwahrscheinlicher werden, je mehr Koordinationsaufwand und Ressourceneinsatz getrieben werden muss, je mehr Störbedingungen gleichzeitig vorliegen müssen, um den Störfall auszulösen, und – im Fall terroristischer Anschläge – je geringer die Öffentlichkeitswirkung ist.

Für die Analyse der Kritikalität von IT-Infrastrukturen müssen zwei Ebenen unterschieden werden: die der einzelnen Organisation und die der Gesellschaft.

## Unternehmenssicht

Aus der Sicht eines Unternehmens sind die IT-Infrastrukturen kritisch, deren Störungen seine Existenz wesentlich beeinträchtigen oder direkt bedrohen können. Im Vordergrund werden dabei insbesondere IuK-Systeme stehen, mit deren Hilfe Leistungen für Kunden erbracht werden. Je nach Grad der IuK-Abhängigkeit können dies z. B. die Produktionssteuerung, das Auftragsabwicklungssystem, der Web-Auftritt oder das Unternehmensnetzwerk sein. Auch Systeme zur Abwicklung interner Prozesse, wie für die Buchhaltung und Finanzverwaltung oder die Personalverwaltung können kritisch sein. Allerdings bestehen hier häufig größere zeitliche Spielräume zur Störfallbeherrschung als für Kundenprozesse.

Der Schutz kritischer IT-Infrastruktur muss von Unternehmen im Rahmen der Risikovorsorge und einem IT-Sicherheitsmanagement geleistet werden. Die Maßnahmen sind häufig anwendungsspezifisch, Backup-Konzepte und Katastrophenpläne sind aber typische Bestandteile.

## Gesellschaftliche Perspektive

Aus gesellschaftlicher Perspektive steht die Funktionsfähigkeit des Gemeinwesens im Mittelpunkt. Dazu gehören neben einer normalen Versorgung der Bevölkerung mit notwendigen Gütern des täglichen Bedarfs auch das Funktionieren von Produktion, Handel und Wirtschaft sowie eine geordnete öffentliche Verwaltung. Vom BSI[1] wurden sieben Infrastruktursektoren mit (lebens-)wichtiger Bedeutung für das staatliche Gemeinwesen identifiziert: Telekommunikation, Energieversorgung, Bank-, Finanz- und Versicherungswesen, Transport und Verkehr, Gesundheitswesen (inkl. Lebensmittel- und Trinkwasserversorgung), Notfall- und Rettungsdienste sowie Regierung und öffentliche Verwaltung (inkl. Polizei, Zoll und Bundeswehr).

Schwere Störungen in jedem dieser Infrastruktursektor können weitreichende Folgen für die Gesellschaft oder zumindest für große Teile davon haben. Jeder dieser Infrastruktursektoren setzt Informations- und Kommunikationstechnik ein, allerdings sind sie in unterschiedlicher Weise davon abhängig.

Für die Kritikalitätsbewertung aus gesellschaftlicher Perspektive müssen zwei wesentliche Unterschiede zur Unternehmenssicht berücksichtigt werden. Günstig wirkt sich aus, dass die Leistungen in den genannten Infrastruktursektoren in der Regel nicht alleine von einem Unternehmen erbracht werden, sondern oft viele Akteure konkurrierend am Markt anbieten. Kritische IT-Infrastrukturen können daher auftreten, wenn der Markt durch ein oder wenige Unternehmen dominiert wird, deren Leistungen im Störfall nicht substituiert werden können und die selbst keine ausreichende Störfallvorsorge vorbereitet haben. Ungünstig wirkt sich aus, dass es innerhalb und zwischen den Infrastruktursektoren Abhängigkeiten gibt. So benötigen alle Infrastruktursektoren in mehr oder weniger großem Umfang Finanzdienstleistungen oder Energie. Für die Bewertung der Kritikalität von IT-Infrastrukturen muss deshalb auch geprüft werden, ob sich IT-Störungen innerhalb des Sektors oder aus einem Infrastruktursektor in andere ausbreiten kann.

[1] Zusätzliche Informationen und Links finden sich unter http://www.bsi.de/fachthem/kritis/