

Schutz kritischer Infrastrukturen in Deutschland - die Beiträge des BSI

Moderne Gesellschaften sind auf die (Dienst-) Leistungen Kritischer Infrastrukturen angewiesen. Der Schutz der dort eingesetzten Informationstechnik erfährt eine immer grössere Bedeutung.



Marit Blattner-Zimmermann

Fachbereichsleiterin im Bundesamt für Sicherheit in der Informationstechnik (BSI), Deutschland.
E-Mail: marit.blattner@bsi.bund.de

Marit Blattner-Zimmermann ist zuständig für den Fachbereich "Sicherheit in Kritischen Infrastrukturen und Internet". Sie war 1997 Gründungsmitglied der AG KRITIS und ist seitdem in leitender Position für den Schutz kritischer Infrastrukturen in Deutschland verantwortlich.

Mit der zunehmenden Durchdringung des alltäglichen Lebens mit Informations- und Kommunikationstechnik (ITK) ist unsere Gesellschaft mittlerweile zu grossen Teilen oder sogar vollständig abhängig von der Informationstechnik. Diese Abhängigkeit trifft insbesondere auch auf die nationalen Kritischen Infrastrukturen (KRITIS) zu. Dazu zählen die Sektoren Transport und Verkehr, Energie, Gefahrenstoffe, Informations- und Kommunikationstechnik, Finanz-, Geld- und Versicherungswesen, Verwaltung, der Bereich der Versorgung, zu dem auch das Gesundheits- sowie Notfall- und Rettungswesen gehören, aber z.B. auch Grossforschungseinrichtungen.

Neue Formen der Bedrohung entstehen

Damit Staat und Gesellschaft störungsfrei funktionieren, müssen die wesentlichen Dienstleistungen dieser Infrastruktur-Sektoren jederzeit verfügbar sein. In der Summe bilden die Kritischen

Infrastrukturen Organisationen und Einrichtungen, die für das staatliche Gemeinwesen von lebenswichtiger Bedeutung sind. Störungen könnten unter Umständen für grosse Bevölkerungsgruppen zu nachhaltig wirkenden Versorgungsengpässen führen oder sogar eine Gefährdung der öffentlichen Sicherheit zur Folge haben.

Durch den immer stärkeren Einsatz der Informationstechnik haben sich die Schutzanforderungen inzwischen deutlich verändert. Rein physische oder organisa-

Die Abhängigkeit Kritischer Infrastrukturen von der Informationstechnik wird weiter zunehmen.

torische Schutzmassnahmen, wie sie bis in die Achtzigerjahre zumeist die Regel darstellten, reichen nicht mehr aus. Durch ihre Verbindung mit den weltweiten Datennetzen sind Kritische Infrastrukturen auch IT-spezifischen Bedrohungen ausgesetzt. Die mit dieser Veränderung einhergehenden Gefahren sind jedoch noch nicht allen Infrastruktur-Betreibern bewusst. Die Verantwortlichen für IT-Sicherheit hier wissen zwar um die Bedeutung der eingesetzten Informationstechnik. Standard- IT-Sicherheit wie

Virens Scanner oder Firewalls wird weitläufig angewendet, auch das vom BSI entwickelte Grundschutzhandbuch spielt in diesem Zusammenhang eine entscheidende Rolle. Dagegen fehlt häufig noch das Bewusstsein für Bedrohung durch gezielte Angriffe. Das Wissen, dass z.B. Hacker, Innentäter, aber auch Nachrichtendienste Schwachstellen in den drei Grundsäulen der IT-Sicherheit Verfügbarkeit, Integrität und Vertraulichkeit nutzen, um IT-Systeme in Kritischen Infrastrukturen zu schädigen oder für eigene Zwecke zu missbrauchen, ist noch nicht sehr ausgeprägt. Hier bedarf es weiterer Sensibilisierung.

Kooperationen ausbauen - Wissen vermitteln

Das BSI untersucht als die zuständige Behörde für IT-Sicherheit in Deutschland Schwachstellen und Bedrohungen der IT-Sicherheit und entwickelt Konzepte zur Minimierung der Folgen möglicher Vorfälle. Der Schutz Kritischer Infrastrukturen umfasst aber weit mehr als rein technische Lösungen. Es gilt alle Aspekte des Infrastrukturschutzes in integrativen Sicherheitslösungen zu vereinen. Auch der physische Schutz oder Möglichkeiten der Strafverfolgung bei relevanten Vorfällen sind von zentraler Bedeutung. Die Erarbeitung solcher Lösungen ist Aufgabe der Ressortübergreifenden Projektgruppe KRITIS (PG KRITIS) des Bundesministeriums des Innern (BMI). In dieser sind neben dem BMI und dem BSI u.a. auch das Bundesamt für Bevölkerungs-

schutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA) sowie das Technische Hilfswerk (THW) vertreten.

Doch der Staat kann seine nationalen Infrastrukturen nicht allein schützen. Zwischen 85 und 90 Prozent der Kritischen Infrastrukturen in Deutschland liegen in der Hand der Wirtschaft. Eine enge Kooperation zwischen Staat und dem privaten Sektor ist daher unbedingt notwendig. Das BSI hält gute Kontakte zu KRITIS-Betreibern, die es weiter ausbaut und intensiviert. Neben regelmässigen Treffen umfasst die Zusammenarbeit auch gemeinsame Projekte zur strategischen Verbesserung der IT-Sicherheit.

Um die Probleme und Bedürfnisse der Wirtschaft möglichst konkret erfassen zu können, hat das BSI die „Wissensbasis KRITIS“ entwickelt und eine „Vorfalldatenbank“ eingerichtet. Die Wissensbasis ermöglicht es, nach bestimmten Auswahlkriterien Unternehmen oder Behörden in kritischen Infrastruktur-Sektoren sowie die dortigen Ansprechpartner zu bestimmen. Die Vorfalldatenbank speichert Open-Source-Quellen über weltweite Vorfälle in Kritischen Infrastrukturen, die Mitarbeiter des BSI analysieren und bewerten.

Eines des grossen Anliegen des BSI bleibt die Erzeugung eines wachsenden Bewusstseins für die Notwendigkeit des Schutzes Kritischer Infrastrukturen in Deutschland. Dies soll auf allen Ebenen geschehen: beim Staat, in der Wirtschaft und in der Gesellschaft. Um das eigene Wissen bestmöglich zu ver-

mitteln, halten Mitarbeiter des BSI Vorträge z.B. bei Branchenverbänden und in Bildungseinrichtungen. Zusätzlich bietet die KRITIS-Homepage (www.bsi.bund.de/fachthem/kritis/index.htm) umfangreiche Informationen zum Schutz Kritischer IT-Infrastrukturen in Deutschland aber auch weltweit.

Die Abhängigkeit wächst – weltweit

Die Bedeutung des Schutzes der Informationstechnik in Kritischen Infrastrukturen ist erkannt – die deutsche Regierung setzt sich aktiv mit dieser Problematik auseinander und stellt dazu weitere Ressourcen zur Verfügung. Denn der Auf- und Ausbau von Fachkräften und Know-how wird auch in Zukunft eine der zentralen Aufgaben sein.

Die Abhängigkeit Kritischer Infrastrukturen von zuverlässiger Informationstechnik wird aber nicht nur in Deutschland, sondern weltweit zunehmen. Damit bleibt der Schutz der IT in Kritischen Infrastrukturen eine Herausforderung, die nicht an den Landesgrenzen aufhören darf. Je weiter die globale Vernetzung fortschreitet, desto stärker müssen die KRITIS-Verantwortlichen auf bi- und multilateraler Ebene zusammenarbeiten. Das BSI kooperiert mit Experten z.B. aus den USA, der Schweiz oder Schweden. Ferner organisiert das BSI im nationalen wie auch internationalen Rahmen fachspezifische Konferenzen sowie Workshops und ist in internationalen Fachgruppen und Gremien der EU, G-8 und Nato vertreten.