Grundsatzpapier Kritis

Infrastrukturen sind wichtige Versorgungssysteme einer Gesellschaft. Die Gewährleistung der ständigen Verfügbarkeit kritischer Infrastrukturen ist eine Voraussetzung für das Funktionieren moderner, vernetzter Gesellschaften. Die Verfügbarkeit von Infrastrukturen ist jedoch nicht nur durch alltägliche Störungen und Gefahren bedroht, sondern auch durch Extremereignisse wie Naturgefahren, menschliches und technisches Versagen sowie vorsätzliche Handlungen staatlicher und nichtstaatlicher Akteure.

Die Gefahren werden zu einer Bedrohung für Kritische Infrastrukturen, wenn diese den hybriden Angriffen keine gestärkte physische und digitale Resilienz entgegenstellen.

Die Identifizierung kritischer Infrastrukturen wurde in bisherigen gesetzlichen Regelungen auf europäischer und nationaler Ebene geregelt. In diesem Zusammenhang wurden Vorgaben für IT-Systeme mit Bezug zu kritischen Infrastrukturen erlassen.

Mit dem **KRITIS-Dachgesetz** sollen die Vorgaben für das sichere Betreiben von kritischen Infrastrukturen für die Betreiber auf alle dafür relevanten Bereiche ausgeweitet werden. Ziel ist es, den **Betreibern organisatorische, personelle und baulich-technische (physische) Vorgaben für den Betrieb der von ihnen zu verantwortenden Kritischen Infrastrukturen** an die Hand zu geben.

Unsere Positionen

Aufgrund der Vielfalt der zu betrachtenden Situationen ist eine standortbezogene Einzelfallbetrachtung für jede Kritische Infrastruktur notwendig und unumgänglich. Im Rahmen einer Sicherheitsanalyse sind die Bedrohungen unter Berücksichtigung der konkreten Prozesse und Gefahren zu ermitteln. Durch eine systematische Bewertung der sich aus den Bedrohungen ergebenden möglichen Schadensausmaße und deren Eintrittswahrscheinlichkeiten sind die konkreten Risiken zu bewerten. In einem standortbezogenen Sicherheitskonzept werden für die identifizierten Risiken **organisatorische, personelle und baulich-technische Maßnahmen** abgeleitet. Hieraus ist ein Maßnahmenplan zur Risikobehandlung zu entwickeln, der die zeitliche Abfolge der Einzelmaßnahmen festlegt und das Ergebnis in Bezug auf die Stärkung der Resilienz definiert.

Die **baulich-technischen Maßnahmen umfassen** hier typischerweise:

1. **Bauliche Maßnahmen**
   - Perimeterschutz: Die Gestaltung der Perimetersicherung z.B. durch Zaunanlagen muss unter Berücksichtigung des angenommenen Täterprofils, der beschriebenen Hilfsmittel und notwendigen Überwindungszeit erfolgen. Die zu betrachtenden Anforderungen wie Durchbruch, Übersteigen, Untergraben, Überfliegen, usw. sind durch technische Maßnahmen zu sichern.
   - Zufahrtsschutz: Die Anforderungen an den Schutz von Zufahrten gegen Kfz-Durchfahrten sind zu formulieren. Hieraus ergeben sich Anforderungen an die Gestaltung der Zufahrten und an dafür benötigte Durchfahrtsschutzeinrichtungen.
   - Pforten und Schleusen: Zugänge und Zufahrten zu kritischen Infrastrukturen müssen bedarfsweise so gestaltet werden, dass eine Kontrolle des Personen- und Warenverkehrs sicher und anforderungsgerecht möglich ist. Vorgaben der Strukturierung und der erforderlichen Widerstandsklassen sind notwendig.
   - Gebäude: Die Anforderungen an Gebäudeaußenhüllen einschließlich Fenster und Türen sind zu formulieren.

2. **Technische Maßnahmen**
   Die Sicherung kritischer Infrastrukturen erfordert den Einsatz technischer Systeme für die Detektion von unerwünschten Ereignissen, deren Bewertung und Auslösung von Reaktionen. Hier ist der Einsatz von Sicherheitssystemen wie etwa Perimeterdetektionssystemen, Einbruchmeldeanlagen, Videosicherheitssystemen, Zutrittssteuerungssystemen und Gefahrenmanagementsystemen usw. festzulegen.

3. **IT-Sicherheit und Cybersecurity**
   Die IT ist in allen Bereichen von Unternehmen nicht mehr wegzudenken, d.h., ohne IT-Systeme mit der dazugehörigen Software kann kein Unternehmen mehr überleben. Auch die Vernetzung der

unterschiedlichsten Systeme und deren Software ist dabei elementarer Bestandteil. D.h., die Systeme sind i.d.R. über das öffentliche Internet weltweit zumindest temporär miteinander verbunden. Bereits die Betriebssysteme dieser Systeme umfassen mehrere Millionen programmierte Quellcodes. Diese komplexen Strukturen bieten - oftmals auch bis dato - unbekannte Möglichkeiten der Manipulation und des unerlaubten Eindringens. Dieses zu vermindern, erfordert das sogenannte „Härten der IT-Systeme“ durch zusätzliche Sicherungsmaßnahmen wie ständig aktualisierte, zuverlässige Firewalls, System-Updates und Redundanzen.

4. **Kommunikationssysteme**
   Die Kommunikation im Sicherheitsumfeld ist zu bewerten. Neben drahtgebundenen Kommunikationsmitteln ist auch der Einsatz von Funksystemen und/oder weiterer Redundanzen zu bewerten

5. **Betriebssicherheit**
   Auch die Sicherheitstechnik, die die Verfügbarkeit kritischer Infrastrukturen erhöhen soll, benötigt für die Funktion eine technische Infrastruktur. Die Anforderungen an diese Infrastruktur hinsichtlich Aufstellung, Stromversorgung, Umgebungsbedingungen sowie Instandhaltung müssen der Bedeutung der zu schützenden Infrastruktur entsprechen.

6. **Bedienkonzepte**
   Technische Systeme für den Schutz kritischer Infrastrukturen müssen in ein personelles Bedien- und Schutzkonzept eingebunden sein. Es bedarf daher neben den „proaktiven“, technischen Maßnahmen auch ein verstärktes Augenmerk auf den Ablauf von organisatorischen Maßnahmen, um im Fall der Fälle auch im organisatorischen Ablauf – durch geeignete Maßnahmen und vorgehaltene Mitarbeiterstrukturen vorbereitet zu sein.

Ziel aller technischen Maßnahmen ist es, die Vulnerabilität der Infrastrukturen in Bezug auf Bedrohungen auf ein tragbares Maß zu verringern. Mit den genannten baulich-technischen, den IT- und Cyber-, sowie den sicherheitstechnischen und organisatorischen Maßnahmen wird die Resilienz des betrachteten Systems in der Nutzungsphase erhöht, so dass die Funktion kritische Infrastrukturen und Anlagen auch während und nach dem Einfluss von Gefahren und Stressoren aufrechterhalten werden kann (Robustheit), bzw. diese schnell wiederhergestellt werden kann (Resilienz). **Der Nachweis der Resilienz einer kritischen Anlage muss durch eine Wirksamkeitsprüfung alle 4 Jahre neu erbracht werden.** Die Nachverfolgung der Wirksamkeitsprüfung obliegt dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).

Kontakt

BHE Bundesverband Sicherheitstechnik e.V.
Carl Becker-Christian • Geschäftsführer
Feldstraße 28 • 66904 Brücken
Telefon: +49 6386 9214-0 • E-Mail: info@bhe.de
www.bhe.de

VfS Verband für Sicherheitstechnik e. V.
Prof. Dr. Clemens Gause • Geschäftsführer
Eulenkrugstraße 7 • 22359 Hamburg
Telefon: +49 40 2197 0010 • E-Mail: info@vfs-hh.de
Lobbyregisternr.: R005814 • www.vfs-hh.de

ZVEI e. V. • Verband der Elektro- und Digitalindustrie
Peter Krapp • Geschäftsführer • Fachverband Sicherheit •
Lyoner Straße 9 • 60528 Frankfurt am Main
Telefon: +49 69 6302-272 • E-Mail: Peter.Krapp@zvei.org
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org