Antiterrorübung „Vorsorge 05“: Der Schutz der Infrastruktur ist eine wichtige Aufgabe vorsorgender Sicherheitspolitik.

Schutz kritischer Infrastruktur

Infrastrukturen haben in der Gesellschaft die Funktion von Lebensadern. Die Gesellschaft ist darauf angewiesen, dass die gewohnte Versorgung, etwa mit Energie, Wasser und Kommunikationstechnologien, zuverlässig funktioniert und dass die Mobilität des Einzelnen jederzeit gewährleistet ist.

Fallen die Eckpfeiler der Versorgung aus, kann dies zu erheblichen Störungen der öffentlichen Sicherheit führen und weit reichende dramatische Folgen nach sich ziehen. Der Schutz der Infrastruktur ist daher eine wichtige Aufgabe vorsorgender Sicherheitspolitik. Die Anschläge in der Türkei (2003), Spanien (2004) und Großbritannien (2005) haben veranschaulicht, dass der internationale Terrorismus eine neue Dimension erreicht hat. Jeder Terroranschlag wird als „Bühne“ verwendet, um eine möglichst große mediale Breitenwirkung zu erreichen. Zusätzlich soll die Infrastruktur des betreffenden Staates massiv geschädigt und die Folgekosten in eine exorbitante Höhe getrieben werden. Speziell die komplexe und verwundbare Infrastruktur westlicher Industriegesellschaften dient dem Terrorismus sowohl als Angriffswaffe als auch als Angriffsziel, wie die Anschläge vom 11. September 2001 drastisch vor Augen geführt haben. Die Liste möglicher Angriffsziele ist dabei unbegrenzt.

Umfassende Antiterror-Strategie. Aufgrund dieser evidenten Bedrohung beauftragte der Europäische Rat im Juni 2004 die Kommission mit der Ausarbeitung einer umfassenden Strategie zur Terrorismusbekämpfung. Das Europäische Programm zum Schutz der kritischen Infrastruktur (EPCIP) ist ein Teilbereich dieser Strategie und hat zum Ziel, Störungen und Manipulationen kritischer Infrastrukturen zu vermeiden, um so das Leben und Eigentum der Bevölkerung vor Terroranschlägen, Naturkatastrophen und Unfällen zu schützen. Dies soll vor allem durch die Errichtung eines Warn- und Informationsnetzes (CIWIN), jährliche Fortschrittsberichte sowie die Analyse von Gefährdungen und gegenseitigen Abhängigkeiten erreicht werden. Das Warn- und Informationsnetz soll bei der Kommission installiert werden und als permanentes Forum dienen. Ziel des CIWIN ist die Unterstützung von Mitgliedstaaten sowie Eigentümern und Verantwortlichen kritischer Infrastrukturen beim Austausch von Informationen über terroristische Bedrohungen, Schwachstellenanalysen und die Erstellung geeigneter Maßnahmen und Strategien zur Risikoverminderung.

Im November 2005 erstellte die Kommission ein „Grünbuch“ zum Europäischen Programm zum Schutz der kritischen Infrastruktur. Die Vorlage eines ersten Vorschlags für EPCIP wird für das Ende der österreichischen Ratspräsidentschaft erwartet. In den

FOTO: E. WEISSHEIMER

Brüsseler Gremien wird das österreichische Bundesministerium für Inneres durch die Abteilung II/4 (Zivilschutz, Krisen- Katastrophenschutzmanagement) vertreten.

Kritische Infrastrukturen. Eine Infrastruktur gilt grundsätzlich dann als kritisch, wenn deren Ausfall oder Beeinträchtigung gravierende Folgen auf Staat und Gesellschaft haben können. Die Qualifizierung als kritisch erfolgt nach dem Grad ihrer Vernetzung, der wechselseitigen Abhängigkeit, Größe des Versorgungsgebiets und Bedeutung als Basis der Infrastruktur. In Österreich sind die als kritisch gewerteten zivilen Strukturen in fünf Schutzgruppen mit insgesamt ca. 180 Objekten eingeteilt. Sie umfassen die Organe der Gesetzgebung, oberste Organe der Vollziehung und der Gerichtsbarkeit, Anlagen der Energieversorgungsunternehmen, Informations- und Kommunikationseinrichtungen, Einrichtungen zur Versorgung der Bevölkerung mit lebensnotwendigen Gütern (z. B. Lebensmittelgroßlager, Wassergroßversorger) sowie Anlagen zur Aufrechterhaltung wesentlicher Verkehrsströme (z.B. Flughäfen, wichtige Donaubrücken, wesentliche Verkehrsknotenpunkte, ÖBB). Die Bewertung erfolgt aufgrund ihrer regionalen oder überregionalen Bedeutung, der Schwere, Reichweite und zeitlichen Auswirkung.

Zusätzlich werden die zu schützenden Objekte in die Wertigkeitsstufe A bei überregionaler und B bei regionaler Bedeutung eingeteilt. A-wertige Objekte sind in einem Anlassfall unbedingt zu schützen. Die Einstufung der Objekte erfolgt über Vorschlag der zuständigen Sicherheitsdirektion im Einvernehmen mit dem zuständigen Amt der Landesregierung und der betroffenen Struktur beziehungsweise aufgrund einer generellen Bewertung durch das Bundesministerium für Inneres. Bei der Beurteilung wird darauf Bedacht genommen, ob eine Beschädigung, Zerstörung oder Besetzung des Objekts eine nur vorübergehende oder eine länger dauernde Beeinträchtigung nach sich zieht.

Ein absoluter Schutz kritischer Infrastrukturen ist allerdings nur schwer möglich. Folglich muss vorrangiges Ziel sein, eine Störung zu verhindern beziehungsweise die Auswirkungen lokal und zeitlich zu begrenzen, um eine schnelle Rückkehr zum Normalzustand zu gewährleisten.

In diesem Zusammenhang ist die Festlegung des Schutzniveaus für das jeweilige Element der Infrastruktur von grundlegender Bedeutung. Ausgangspunkt ist ein mehrstufiger Analyse- und Planungsprozess, der die Ermitt-

SICHERHEITSTECHNIK

Neue Technik – mehr Sicherheit

Um Bedrohungen schneller erkennen und gezielte Maßnahmen setzen zu können, bedarf es neuer Sicherheitseinrichtungen.

Notwendig wäre die Entwicklung intelligenter Überwachungssysteme, die Informationen aus Daten, Sprache und Bildern kombiniert auswerten und gegebenenfalls Alarm schlagen. Sicherheitsforschung soll dieser Entwicklung entsprechen und auf die Entwicklung eines nationalen und internationalen Frühwarn- und Monitoringsystems für elektronische Netze und von Sicherheitssystemen zur automatischen Erkennung terroristischer Bedrohungen auf kritische Infrastrukturen fokussieren.

Für eine effiziente Analyse und für konkrete Abwehrmaßnahmen bedarf es einer ganzheitlichen Betrachtung und Klassifizierung der Angriffsmittel. Für diese ganzheitliche Betrachtung müssen verschiedene Ereignisse verknüpft werden können, d. h. Verknüpfung von Gemeinsamkeiten mit den logisch zu erwartenden Entwicklungen. In diesem Zusammenhang wäre insbesondere die Entwicklung eines intelligenten Videoüberwachungssystems mit Bildauswertung und Mustererkennung, Zutrittkontrolle mittels biometrischer Verfahren und Alarmierungssystemen hilfreich. Die derzeitigen Videoüberwachungssysteme generieren zu viele Fehlalarme. Weiters werden Attacken nicht mit der erforderlichen Zuverlässigkeit erkannt.

Folgende Ziele sollten dabei insbesondere berücksichtigt werden:

- Die Netzwerke sollen Angriffe erkennen und abwehren können.
- Zusammenfassung der kritischen Infrastrukturnetzwerke zu nationalen und eventuell internationalen Clustern, um Dominoeffekte zu minimieren.
- Verifizierung der Gefährlichkeit von Angriffen auf einzelne Cluster durch Analyse der Angriffsmethoden, ihrer Folgen und erforderlichen Maßnahmen.
- Entwicklung eines Intrusion-Prevention-Systems.
- Weiterentwicklung der bestehenden Intrusion-Detection-Systeme, sodass sie auch die Gefährlichkeit eines Angriffs erkennen und bei Bedarf national und international vernetzt agieren können. Intrusion-Detection-Systeme überwachen Netzwerke, erkennen Anomalien und schlagen Alarm.
- Einrichtung eines Monitoringzentrums zwecks Erkennung und statistischer Erfassung von Angriffen auf kritische Infrastrukturen.
- Trennung der Zuständigkeit des Monitoringzentrums und IT-Systemen der Bedarfscluster,
- Anonymität der zur Analyse übermittelten Daten.
- Weiterentwicklung von Methoden und Verfahren zwecks Entwicklung neuer Technologien für eine zuverlässige Bildverarbeitung und Mustererkennung, die auf kriminelle und/oder terroristische Handlungen fokussiert.
- Entwicklung neuer Technologien zwecks Verknüpfung unterschiedlicher Sensoren (Audio und Video). Die Kombination von Sensoren reduziert Fehlalarme und erhöht die Treffsicherheit und folglich die Qualität von Videosystemen.
- Neue Methoden bei der Auswertung von Bildsequenzen. Die bestehenden Methoden unterscheiden nicht z. B. zwischen Touristen und Demonstranten.
- Weiterentwicklung der Methoden für den Vergleich von Bild- und Biometriedaten auf Ausweisdokumenten mit jenen, die in den internationalen Datenbanken gespeichert sind.

BILD: BVT

lung der Risiken und eine daran anknüpfende Überprüfung sowie gegebenenfalls Anpassung von Schutzmaßnahmen umfasst. Darüber hinaus muss darauf Bedacht genommen werden, dass etwa 85 Prozent der kritischen Infrastrukturen im privatwirtschaftlichen Bereich liegen. Daraus resultiert, dass ihr Schutz weder durch den Staat noch durch ihre Betreiber alleine gewährleistet werden kann. In diesem Bereich bedürfen umfassende Schutzmaßnahmen einer engen und vertrauensvollen Zusammenarbeit zwischen Staat und Wirtschaft.

Bereits im Vorfeld möglicher Krisen sollte ein Kommunikationskonzept erstellt werden, das unter anderem sichere Kommunikationsformen wie E-Mail, Webseiten, klassische und Mobiltelefonie sowie Funk enthält, um im Ereignisfall die Medien und die Bevölkerung zu informieren und zu sensibilisieren.

Objektschutzblätter. In Österreich werden im Rahmen des derzeitigen Schutzkonzepts für Strukturen, deren Schutz vorgesehen ist, von den Sicherheitsdirektionen Objektschutzblätter angelegt. Dabei wird unter anderem untersucht, ob und durch welche baulichen Maßnahmen und technischen Vorsorgen die Sicherheit verbessert werden kann. Die einzelnen Objektschutzblätter werden vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) im „Objektschutzkatalog“ gesammelt. Weiters werden Risiko- und Gefährdungsanalysen erstellt, um festzustellen, welche Objekte einem erhöhten Risiko ausgesetzt sind, um die Prioritätsstufen festzulegen und um gezielte Schutzkonzepte zu erstellen.

Das BVT erarbeitet neben präventiven Schutzplänen, mit deren Hilfe Sicherheitsrisiken durch die Sensibilisierung von Verantwortungsträgern, Aufzeigen von Bedrohungsszenarien und Entwicklung von Abwehr- und Sicherheitsmaßnahmen reduziert werden sollen, auch konkrete Schutzpläne, um einer speziellen Bedrohungslage wirkungsvoll zu begegnen.

Ohne die praktische Erprobung und Einübung lassen sich aber nur ungenaue Aussagen über die Effizienz der Schutzpläne machen. Vorrangiges Ziel wird es daher immer sein, bereits im Vorfeld alle staatlichen, privaten und freiwilligen Kräfte koordiniert zu bündeln sowie die dringlichsten Notmaßnahmen (Recovery-Maßnahmen) zu vereinbaren, die nach dem Eintritt einer Katastrophe erforderlich sind.

Präventive Schutzpläne: Gezielte Schutzkonzepte für Kraftwerke und andere kritische Infrastrukturen.

Foto: Alexander Tuma

Ansprech- und Koordinierungsstellen für Personen- und Objektschutzangelegenheiten sind die Sicherheitsbeauftragten in den Zentralstellen des Bundes. Als Verbindungsstelle fungiert das BVT.

Zuständigkeitsbereich des Bundesministeriums für Inneres. Bei überregionalen Anlassfällen fällt die Gesamtkoordination des staatlichen Katastrophenschutzmanagements, des Krisenmanagements und der internationalen Katastrophenhilfe in den Zuständigkeitsbereich des Bundesministeriums für Inneres.

Zu diesem Zweck wurde ein interministerielles Lagezentrum und das Einsatz- und Krisenkoordinationscenter (EKC) eingerichtet. Das Lagezentrum unterstützt insbesondere die Zusammenarbeit von Bund und Ländern im polizeilichen Bereich der Sicherheitsvorsorge.

Im EKC werden permanente und anlassbezogene Aufgaben, wie unter anderem das Sammeln, Bewerten und die interne Weitergabe von für das Ressort relevanten Informationen wahrgenommen – 24 Stunden am Tag, 365 Tage im Jahr. Darüber hinaus dient es im Anlassfall, wie zum Beispiel bei Krisen und Katastrophen, als Einsatzzentrale für Großeinsätze der Polizei und als nationale Kontaktstelle für das CIWIN. Das staatliche Krisen- und Katastrophenschutzmanagement (SKKM) wird von hier aus unterstützt

RECHT

Gesetzliche Grundlagen des Personen- und Objektschutzes in Österreich sind:

- Art. 10/1/7 BVG: Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit.
- §§ 3 und 22 SPG: Aufgaben der Sicherheitspolizei, vorbeugender Schutz von Rechtsgütern.
- § 48 SPG: Bewachung von Menschen und Sachen.