**Wasserkraftwerke: Rund 400 Unternehmen und Anlagen in Österreich gelten als kritische Infrastruktur.**

# Schutz kritischer Infrastruktur

**Die Gesellschaft ist zunehmend von sensiblen Unternehmen und Prozessen abhängig – und damit verletzlich. Das erfordert einen speziellen Schutz.**

Sie sichern unsere Energie- und Wasserversorgung, gewährleisten unsere Gesundheit und ermöglichen uns uneingeschränkte Kommunikation. Kritische Infrastrukturanlagen sind die „Lebensadern" unserer Gesellschaft. „Vereinfacht gesagt versteht man darunter alle Unternehmen, die für die Versorgung der Bevölkerung mit lebenswichtigen Gütern verantwortlich sind", erklärt Mag. Sylvia Mayer, Leiterin des Referates „Schutz kritischer Infrastrukturen" (SKI) in der Abteilung 3 (Personen- und Objektschutz) im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT). „Das sind beispielsweise Elektrizitäts- und Ölunternehmen, Banken, Mobilfunk- und Internetbetreiber, Krankenhäuser, große Medikamentenhersteller, große Lebensmittelhändler, Schienen- und Luftfahrtsunternehmen aber auch etwa Hilfs- und Einsatzkräfte."

**Rund 400 Unternehmen** in Österreich gelten als kritische Infrastruktur. Identifiziert wurden sie unter anderem nach den Kriterien Zeit, Art der Auswirkung, Ausmaß der Auswirkung und Redundanzen. „Diese Unternehmen bilden nun die Grundlage unserer Arbeit", erläutert Mayer. „Momentan erfolgt die Identifizierung der kritischen Objekte innerhalb dieser Unternehmen, also beispielsweise von Umspann- und Kraftwerken, von großen Rechenzentren, Lebensmittelgroßlagern oder Sendemasten." 80 Prozent der kritischen Infrastrukturanlagen werden von privaten oder privatisierten Unternehmen betrieben.

Zumindest einmal pro Jahr erfolgen vom jeweiligen Landesamt Verfassungsschutz (LV) Erhebungen über Ansprechpersonen, Sicherheitsvorkehrungen und Kernelementen des Objektes", sagt Mayer. Potenzielle Bedrohungen sind etwa terroristische Anschläge, Katastrophen jeglicher Art, technisches und/oder menschliches Versagen, organisierte Kriminalität sowie Cyber-Angriffe. „Die größte Bedrohung dieser Unternehmen geht sicher von Hacker-Angriffen aus – mit Auswirkungen bis hin zu einem längerfristigen, großflächigen Stromausfall in Österreich, da alle Bereiche der kritischen Infrastruktur immer mehr von IT-Systemen abhängig und untereinander stark vernetzt sind," erklärt Mayer.

Diese Vernetzung – und damit verbunden die Gefahr großflächiger Auswirkungen im Ernstfall – macht den Schutz kritischer Infrastruktur zu einer wichtigen Aufgabe des Staates. „Unsere Gesellschaft ist stark abhängig von bestimmten Unternehmen und Prozessen – und dadurch auch verletzlich", erklärt die Referatsleiterin. Kommt es zu Störungen oder gar Ausfällen kriti-

Foto: Egon Weissheimer

scher Infrastrukturanlagen, ist mit erheblichen Belastungen für Staat, Wirtschaft und große Teile der Bevölkerung zu rechnen. „Unsere Aufgabe ist es daher, diese kritischen Unternehmen und Prozesse als sensibel zu erkennen und besonders zu schützen. Diese Aufgabe besteht für das Innenministerium, da bei einem Ausfall dieser Unternehmen sicherheitspolizeiliche Auswirkungen zu befürchten sind bzw. auch eine erhöhte Gefährdung dieser Unternehmen besteht“, betont Mayer.

**Raffinerie als kritische Infrastruktur: Im Objektschutz gibt es eine Kooperation mit dem Bundesheer.**

Seit 1. Juli 2014 erfasst § 22 SPG (Vorbeugender Schutz von Rechtsgütern) auch den vorbeugenden Schutz kritischer Infrastruktur (Z. 6). Die Hauptaufgabe besteht somit in der Kontakthaltung, Beratung sowie Informationsanalyse und -weiterleitung an Unternehmen.

**Aufgaben.** Das Referat deckt zwei Tätigkeitsbereiche ab: Im Bereich „Kontaktgespräche und Beratung zu sicherheitsrelevanten Themen“ führen die Mitarbeiter und Kollegen der Landesämter Verfassungsschutz (LV) Gespräche mit Betreibern kritischer Infrastruktur in ganz Österreich und bieten Beratungen an. Im Bereich „Lagebild und Risikoanalyse“ erfolgt täglich eine Recherche in öffentlich zugänglichen Quellen hinsichtlich aktueller Vorfälle rund um kritische Infrastruktur. Zudem werden Meldungen und Informationen anderer Behörden und Dienste ausgewertet, analysiert und bei Bedarf an Betreiber kritischer Infrastrukturanlagen weitergeleitet. Die Darstellung der Informationen erfolgt in Lagebildern und Risikoanalysen. Dazu kommen Berichte, Stellungnahmen und Vorträge in der öffentlichen Verwaltung und in der Wirtschaft.

**Das Referat SKI** besteht seit 2013 und hat derzeit sieben Mitarbeiterinnen und Mitarbeiter. „Der rasche Aufbau des Know-hows und der Struktur ist an sich eine Erfolgsgeschichte“, sagt Mayer. Die Schutzaufgaben und Kompetenzen sind zwischen der BMI-Zentralstelle und den Landespolizeidirektionen aufgeteilt. „Wir im BVT sind für die Kommunikation mit den kritischen Infrastrukturunternehmen Österreichs zuständig und als Informationsdrehscheibe eingerichtet. Die Kollegen in den Landesämtern sind für den Objektschutz vor Ort zuständig – inklusive der regelmäßigen Erhebung wichtiger Informationen über die Objekte hinsichtlich der Einsatzvorbereitung.“

Eine Herausforderung ist es, Hintergrundwissen über die kritische Infrastruktur zu bekommen. „Nur so können wir auf Augenhöhe mit den Unternehmensvertretern sprechen“, betont Mayer. „Es ist daher notwendig, dass unsere Mitarbeiter je nach Zuständigkeit wissen, wie etwa die Elektrizität in Österreich funktioniert und welche Anlagen und Prozesse dafür eine Bedeutung haben, über welche Strecken das Öl nach Österreich kommt, wie die Versorgung in Österreich mit Medikamenten funktioniert und wie sich die Mobilfunkbetreiber vor Ausfällen schützen.“

Zu den Kooperationspartnern gehören das Bundeskanzleramt und das Büro für Sicherheitspolitik im BMI, die für die Umsetzung auf der strategischen Ebene zuständig sind. „Unser wichtigstes strategisches Ziel ist es, die Kommunikation, Koordination und Kooperation zwischen der Wirtschaft und den Behörden zu verbessern und ein Vertrauensverhältnis zu schaffen, das einen intensiven Informationsaustausch zu Vorfällen, Gefährdungen und Bedrohungen zulässt“, erklärt Mayer. „Zudem geht es uns darum, die Sicherheitsarchitektur innerhalb der Unternehmen durch Beratungen und Sensibilisierung unsererseits zu verbessern. Wir investieren in die Bereiche Objektschutz, Sicherheit der IT-Systeme und Informationssicherheit.“

Im Objektschutz wird auch mit dem Bundesheer kooperiert. „Da in Krisenfällen das Bundesheer im Assistenzeinsatz für Agenden des Objektschutzes zuständig werden könnte, erfolgt ein regelmäßiger Informationsaustausch, um den Einsatz im Krisenfall gewährleisten zu können“, erläutert Mayer. Trainiert wurde der Ernstfall etwa im Rahmen der Großübung „Schutz 2014“. „Ziel war unter anderem eine Verbesserung der Zusammenarbeit und Abstimmung zwischen Polizei und Bundesheer.“ In Abstimmung mit dem Referat SKI führt das Bundesheer regelmäßig Übungen an ausgewählten Objekten durch, um für den Ernstfall gerüstet zu sein. Zumindest alle zwei Jahre findet ein Treffen mit Behördenvertretern aus Deutschland und der Schweiz statt. „Dadurch können wir viele neue Ideen für unser Referat und unsere Tätigkeit gewinnen“, sagt Mayer. Auch auf europäischer und internationaler Ebene finden regelmäßig Veranstaltungen mit dem Ziel der besseren Vernetzung statt. Mitarbeiter des Referats nahmen vom 7. bis 10. Juli 2014 an einem Symposium des FBI und der Interpol teil. „Eine Vernetzung ist gerade im Bereich SKI deshalb so wichtig, weil Bedrohungen oft im Ausland ihren Ursprung nehmen und wir uns in Österreich aufgrund rascher Information durch die ausländischen Behörden vorbereiten können“, sagt die Referatsleiterin.

**Zukünftige Gefahren.** „Wir alle sind abhängig von Strom, Mobiltelefon, Internet und Onlinebanking“, betont Sylvia Mayer. „Wir verlassen uns sehr stark auf das Funktionieren dieser Bereiche, da wir bislang kaum von Ausfällen betroffen sind. Zudem besteht in vielen Sektoren eine sehr große Abhängigkeit von IT-Systemen, was eine zusätzliche Vernetzung verschiedener kritischer Infrastrukturen untereinander bedeutet – und damit ein weiteres Gefährdungspotenzial darstellt.“ Welche Auswirkungen ein Störfall in sensiblen Bereichen tatsächlich haben kann, zeigte etwa im März 2014 der Stillstand dreier Wiener U-Bahn-Linien während der Stoßzeit: Der Grund war lediglich der Ausfall eines „Switches“, eines Verteilungsknotens für Daten – mit weitreichenden Folgen, nämlich dem bisher großflächigsten U-Bahn-Ausfall der Geschichte, von dem über 100.000 Menschen betroffen waren.

*Julia Riegler/Herbert Zwickl*

FOTO: EGON WEISSHEIMER