Zu den Einrichtungen kritischer Infrastruktur zählen Eisenbahnen und Krankenhäuser.

Verwundbarkeit minimieren

Der Ausfall von Systemen und Diensten für die Daseinsvorsorge kann schwerwiegende Folgen nach sich ziehen. Deshalb liegt der Schutz dieser Einrichtungen im Interesse des Staates.

Staaten sind über ihre kritische Infrastruktur verwundbar. Der Ausfall eines Unternehmens, das kritische Infrastruktur betreibt, wie Strom-, Gas- oder Wasserkraftanlagen, kann für die Vorsorge der Gesellschaft und die innere Sicherheit schwerwiegende Folgen haben. Viele dieser Unternehmen sind mit dem Internet verbunden. Die Fernsteuerung von Kraftwerken oder Verkehrsleitsystemen, automatisierte Bestellsysteme für die Versorgung mit Lebensmitteln, Mobiltelefone und bargeldloser Zahlungsverkehr erleichtern die Abläufe im Wirtschaftsleben und im Alltag – doch ihre Vernetzung mit dem Internet bringt Gefahren und Risiken mit sich. Der Schutz kritischer Infrastruktur obliegt dem Bundeskanzleramt und dem Bundesministerium für Inneres – in operativer Hinsicht dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT). Das BVT gibt jährlich den Bericht zum Schutz kritischer Infrastruktur (SKI-Report) heraus. Im SKI-Report 2015 wird auf Gefahren und Risiken hingewiesen und über sicherheitsrelevante Vorfälle 2014/15 berichtet.

Gefahren für Unternehmen kritischer Infrastruktur gehen von politischen, ökonomischen und gesellschaftlichen Entwicklungen und Problemen aus. Die internationale Vernetzung und die Einbindung erneuerbarer Energie in Stromnetze führen zu einem höheren Risiko von Stromausfällen. Zur erneuerbaren Energie zählen Wasserkraft, Windenergie, Sonnenenergie, Erdwärme und die durch Gezeiten erzeugte Energie. Solche Anlagen können Ziele von Terroristen, Kriminellen oder Extremisten sein. Die Gefahr in Österreich besteht durch Anschläge von religiös motivierten Terroristen.

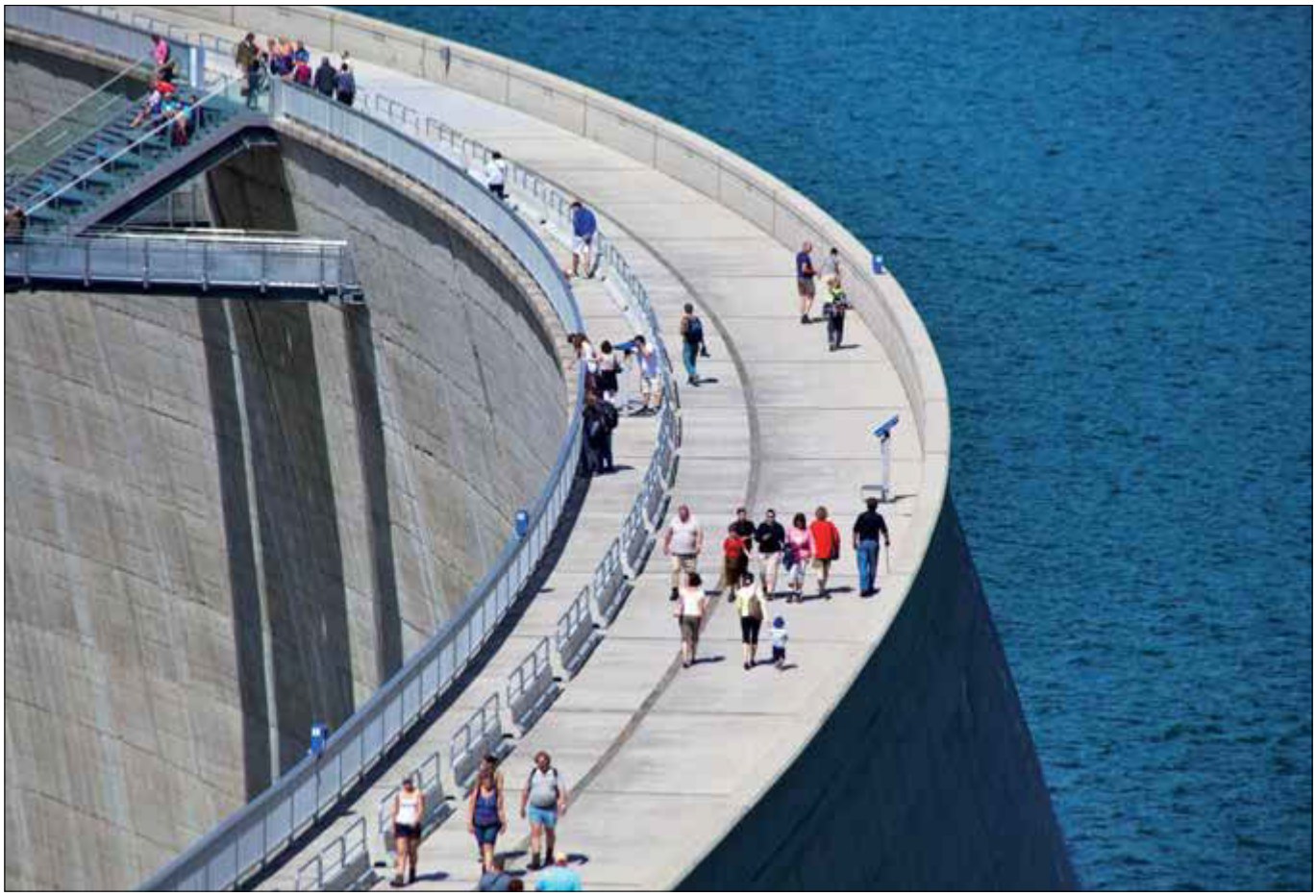
Die Handlungen extremistischer Gruppen reichen von gewalttätigen Protesten und militanten Störaktionen bis hin zu Beschädigungen, Brandstiftungen und Sprengstoffanschlägen an Unternehmenseinrichtungen. Vor allem im Internet und in sozialen Netzen veröffentlichte Daten – etwa die Eigendarstellung von Unternehmen oder die Selbstdarstellung von Mitarbeitern – ermöglicht Angriffe, die bis in die privaten Lebensbereiche von Unternehmensangehörigen eindringen.

Linksradikale Aktionen richten sich vor allem gegen die Errichtung von Tunnels, Wasser- und Windkraftwerken sowie Hochspannungsleitungen. Unternehmen, die sich im Asylbereich einsetzen, können in den Fokus rechtsradikaler und fremdenfeindlicher Gruppen kommen.

Militante Tierrechtsgruppen setzen auf Aktionen gegen Unternehmen am Gesundheitssektor (Pharmaindustrie – Forschung mit Tierversuchen) sowie Banken und Versicherungen, die mit den angegriffenen Unternehmen verbunden sind. Kritische Infrastruktur kann ein Ziel für politisch motivierte Einzeltäter sein. Auch Angriffe durch Innentäter sind nicht auszuschließen. Hier kann vorwiegend auf präventive Maßnahmen wie Schulung und Sensibilisierung von Mitarbeitern, verstärkte Überwachung von sensiblen Bereichen, die Einführung von Unternehmensstandards und Verhaltenskodizes sowie auf Sicherheitsüberprüfungen durch das BVT zurückgegriffen werden.

Die Verwundbarkeit kritischer Infrastruktur hängt von den Kontrollsystemen ab. *SCADA (System Supervisory Control and Data Aquisition)* ist eines der am meisten genutzten Systeme. Es ist mit den Maschinen vernetzt und nutzt für die Kommunikation zwischen Maschinen und verschiedenen *SCADA*-Systemen zumeist das TCP-Protokoll, das auch die Kommunikation im Internet steuert. Eingesetzt wird *SCADA* in vielen Unternehmen der kritischen Infrastruktur, unter anderem in Kraftwerken, Pipelines und Pumpwerken.

Fotos: Franz Gruber/Picturedesk.com, Egon Weissheimer



Schutz kritischer Infrastruktur: Auch Staukraftwerke können Ziele von Terroristen sein.

Ein weiteres Problem sind Schwachstellen in Netzwerkkomponenten. Diese Geräte sind die Herzstücke eines jeden Computernetzwerks. Zu den spektakulärsten Angriffen auf Sicherheitslücken zählten die „SYNful Knock"-Lücke im September 2015 und die „Juniper-Hintertüre" im Dezember 2015.

Hacking. Im Mai 2014 wurden Speicherkarten der Leittechnik eines Kohlekraftwerks in Österreich gestohlen. Durch die Entfernung der Karten kam es zu einer Störung des Kraftwerks, das 40.000 Haushalte versorgt – die Leistung konnte durch redundante Systeme ersetzt werden.

Im Juni 2014 wurde bekannt, dass die internationale Energiewirtschaft durch die Hacker-Gruppe „Dragonfly" mittels Schadsoftware attackiert worden ware. Angriffsziele waren Betreiber von Energienetzen und Pipelines, Stromerzeuger und Anbieter von Technik für die Energiebranche.

Im Dezember 2014 wurde bekannt, dass Hacker in das Netzwerk eines Stahlwerks in Deutschland eingedrungen waren, die Steuerung des Hochofens übernommen und die Anlage massiv beschädigt hatten. Die Systeme waren nicht mehr kontrollierbar und der Hochofen nicht mehr abschaltbar.

Stromausfälle. 2015 kam es in Österreich zu einzelnen Stromausfällen, die nicht durch strafbare Handlungen herbeigeführt worden waren. Beispielsweise waren im Dezember 2015 nach einem technischen Defekt rund 12.000 Innsbrucker Haushalte zeitweise ohne Strom. In Österreich liegt die durchschnittliche statistische Ausfallszeit pro Jahr pro Haushalt bei rund 50 Minuten. Im März 2015 kam es zu mehrstündigen Stromausfällen in Amsterdam und großen Teilen der Türkei, wobei der anfängliche Verdacht von terroristischen Hintergründen bzw. Hacker-Angriffen von den Betreibern nicht bestätigt wurde.

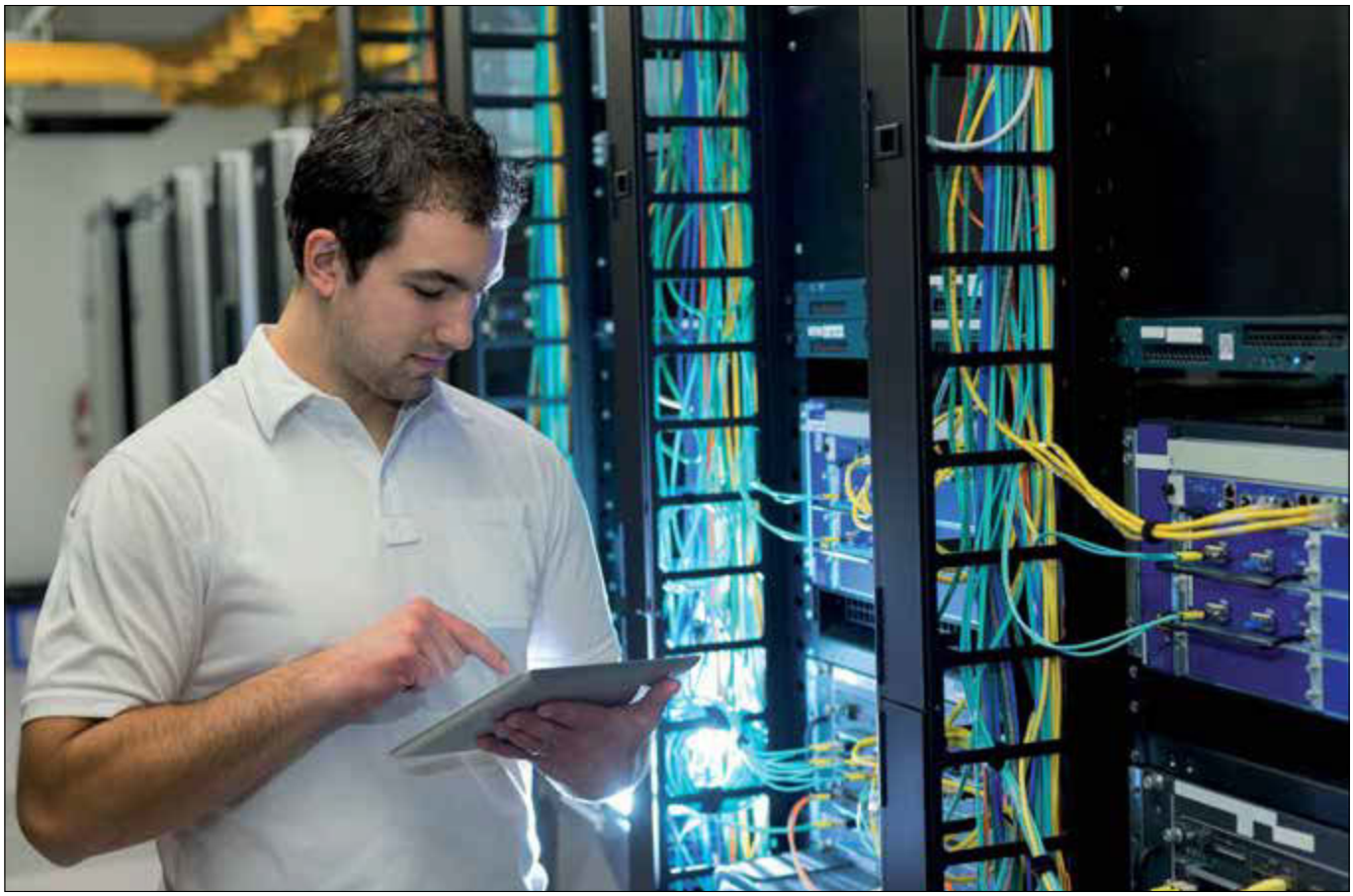
Im November 2015 wurde in der Ukraine die Stromversorgung unterbrochen und auf der Halbinsel Krim der Notstand ausgerufen, nachdem Strommasten gesprengt worden waren. In Österreich wurden wesentliche Komponenten aus Kraft- und Umspannwerken gestohlen, was jedoch keine Ausfälle verursachte. Beispielsweise wurde im April 2015 ein 325 Kilogramm schwerer Bestandteil einer zu diesem Zeitpunkt nicht in Betrieb stehenden Turbine aus einem Kraftwerk gestohlen.

Zwischen August und Oktober 2015 ereigneten sich in Niederösterreich mehrere Kupfer- und Buntmetalldiebstähle in Umspannwerken.

Öffentliche Verkehrsmittel. Terroristen geht es darum, Objekte mit einem hohen Symbolwert zu treffen und damit eine breite Aufmerksamkeit zu erreichen. Öffentliche Verkehrsmittel sind bevorzugte Ziele, da mit geringen Mitteln viele Menschen getötet und verletzt werden können und eine hohe Medienpräsenz zu erwarten ist.

Im März 2015 wurde von der Terrororganisation IS und deren ideologisch getreuen Gruppierungen in Nordafrika über soziale Medien dazu aufgerufen, in Österreich Zugentgleisungen herbeizuführen oder von Brücken Steine auf fahrende Autos zu werfen. Darüber hinaus sind öffentliche Verkehrsmittel und Bahnhöfe häufig Ziele von Bombendrohungen. Wenngleich diese Drohungen zumeist keine terroristischen Hintergründe haben, werden dadurch Großeinsätze ausgelöst.

FOTO: GINA SANDERS/FOTOLIA



Die Verwundbarkeit von Unternehmen kritischer Infrastruktur hängt auch von den Kontrollsystemen ab.

Durch Computerpannen kam es international zu Vorfällen und Ausfällen auf Flughäfen. Unter anderem legte eine Störung des IT-Systems den Flughafen in Budapest für mehrere Stunden lahm. In Österreich führten Schwankungen im Stromnetz und darauf folgende Ausfälle von Servern zum Stillstand Dutzender Züge im Schienenverkehr.

Am Gesundheitssektor (Krankenhäuser, Pharmaindustrie) kam es 2015 zu Diebstählen medizinischer Bedarfsartikel und endoskopischer Geräte. In Österreich gab es einige Ausfälle bei Mobilfunkbetreibern, die aber nicht auf terroristische oder extremistische Hintergründe zurückzuführen waren.

Österreichische Banken registrierten wiederholt Cyber-Attacken, die nach Angaben der Unternehmen keine gravierenden Auswirkungen zeigten. Zu einem überwiegenden Teil wurden Systemausfälle beim Online-Banking, bei den Kontoausdruckautomaten und bei Bankomaten registriert, die durch Systemfehler hervorgerufen worden waren.

Bundesministerien und Höchstgerichte zählen in Österreich ebenso zur kritischen Infrastruktur. Sie waren 2015 hauptsächlich von Cyber-Angriffen betroffen, deren Urheber häufig nur durch Drohungen und Nötigungen in Erscheinung traten. Die Angriffe beeinträchtigten ihre Funktionsfähigkeit nicht.

BVT-Maßnahmen. Das BVT versucht durch verstärkte Kommunikation, Kooperation und Koordination mit Betreibern von Unternehmen der kritischer Infrastruktur deren Schutz und Sicherheit und damit die gesamtstaatliche Resilienz zu verbessern.

Die Bundesregierung hat 2008 das „Österreichische Programm zum Schutz kritischer Infrastruktur“ beschlossen (Masterplan APCIP 2008). Der Masterplan APCIP 2014 dokumentiert die abgeschlossenen Arbeiten und enthält den Masterplan auf Basis der Erkenntnisse der letzten Jahre. Damit wird dem Auftrag der Sicherheitsstrategie und dem Arbeitsprogramm der Bundesregierung nach Erarbeitung eines gesamtstaatlichen Konzepts zum Schutz kritischer Infrastruktur Rechnung getragen. Der Masterplan wurde von Mitarbeitern des BKAs und des BMI federführend erarbeitet und mit den relevanten Ressorts, Ländern, Interessensvertretungen und ausgewählten strategischen Unternehmen akkordiert.

2015 wurden Gespräche mit Betreibern verschiedener Sektoren geführt – mit dem Ziel der Bewusstseinsbildung zu Gefahren und Risiken sowie staatlicher Unterstützungsmaßnahmen und der Stärkung des Vertrauens zum regelmäßigen Informationsaustausch. Darüber hinaus erfolgten Beratungen über sicherheitsrelevante Themen wie Risiko- und Krisenmanagement, Objektschutz, Cyber-Sicherheit und Terrorismus. In der zentralen Kontakt- und Meldestelle im BVT gingen zahlreiche Meldungen und Anfragen von Unternehmen ein, außerdem wurden über das Frühwarnsystem Warn- bzw. Informationsschreiben an Betreiber übermittelt.

Das BVT führt einen Objektschutzkatalog, in dem Objekte identifiziert und in der Infrastruktur-Datenbank des BVT erfasst wurden. Für diese Objekte wurden Einsatzpläne mit sicherheits- und einsatzrelevanten Informationen erstellt. Dadurch soll gewährleistet werden, dass im Krisenfall rasch und richtig reagiert werden kann und Maßnahmen der Betreiber und der Behörden sich bestmöglich wechselseitig ergänzen.

Zentrale Kontakt- und Meldestelle im BVT: SKI@bvt.gv.at

FOTO: ARJUNA KODISINGHE/FOTOLIA