Digitalfunk für Unternehmen: Innenminister Wolfgang Sobotka übergab Digitalfunkgeräte an Unternehmensvertreter.


Protestaktionen gegen die Bauvorbereitungen des Murkraftwerkes in Graz im Frühjahr 2017.

# Bedrohungen erkennen

**Betreiber kritischer Infrastruktur sollen in den digitalen Behördenfunk eingebunden werden. Das Projekt wurde beim Symposium „Kritische Infrastruktur – Lagebild 2017“ vorgestellt.**

Im Herbst 2016 wurden in der Steiermark 21 Mobilfunksendemasten in drei Bezirken beschädigt. Spannungs- und Datenkabel der Sendemasten wurden durchtrennt, wodurch es zum Ausfall des Mobilfunks im Umkreis von einigen Kilometern rund um diese Anlagen kam. In der Landespolizeidirektion Steiermark wurde zur Aufklärung des Falles eine SOKO „Sendemast“ eingerichtet, die mit dem BVT und den Betreibern der Sendeanlagen zusammenarbeitete.

„Wir haben die Sendeanlagen in den betroffenen Bezirken durch Polizeistreifen verstärkt überwacht“, berichtete Hauptmann Johann Hohl, Bezirkspolizeikommandant von Voitsberg, beim Symposium „Kritische Infrastruktur – Lagebild 2017“. Bei den Ermittlungen wurden ehemalige Angestellte, Strahlengegner etc. befragt, Tatortspuren wurden ausgewertet. An den Tatorten wurden Werkzeuge sichergestellt, die zu den Beschädigungen passten. Bei einigen Sendemasten wurden vom Betreiber Videokameras installiert. Eine Person wurde gefilmt, als sie auf einen der Masten kletterte.

Der Verdächtige soll nicht nur Kabel durchtrennt haben, er soll bis zu 30 Meter hoch auf die Masten geklettert sein, um dort montierte Flugbefeuerungslampen zu zerstören, an denen sich Rettungs- und Polizeihubschrauber orientieren. Deswegen wurde er wegen vorsätzlicher Gefährdung der Sicherheit der Luftfahrt angeklagt. Laut Hohl habe der Täter jeweils in der Nacht zwischen 2 und 5 Uhr zugeschlagen, als der Vollmond schien. Als am 22. Dezember 2016 ein Betreiber einer Sendestation eine Störmeldung erhielt, leitete die Polizei eine Alarmfahndung ein und konnte einen Mann festnehmen, der sich in der Nähe des Sendemastens aufgehalten hatte. Der 23-jährige Steirer stritt alles ab. Laut Polizei soll er sich durch die „Strahlung“ gefährdet gefühlt haben. In seiner Wohnung stellten die Ermittler neben Zangen und Scheren eine größere Menge an Marihuana aus eigener Produktion sicher. Der Verdächtige wurde im März 2017 zu vier Jahren Haft verurteilt.

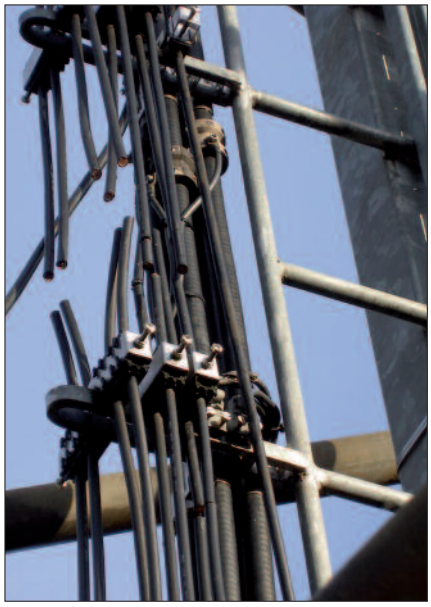
**Strommasten.** Ein mittlerweile ebenfalls ausgeforschter Täter aus dem Bezirk Murau beschädigte zwischen Oktober und Dezember 2016 in der Steiermark zehn Strommasten und einen Telefonleitungsmasten, indem er diese mit einem Werkzeug ansägte. Dadurch stürzten drei Masten ein, die anderen konnten von Mitarbeitern rechtzeitig entdeckt und gesichert werden. Drei weitere Masten wurden vom Täter selbst provisorisch gesichert, und sollten erst bei einem größeren Sturm umfallen. Der Schaden beträgt mehr als 10.000 Euro. Als Motiv für die Taten gab der Mann an, er habe sich von der Strahlung gefährdet gefühlt. In Oberösterreich wurden 2016 zwei große Strommasten von Unbekannten sabotiert. Es wurden systematisch Schrauben gelockert, und einer der Masten wäre spätestens im Winter bei größerer Eislast gekippt.

**Beim Symposium** „Kritische Infrastruktur – Lagebild 2017“ im Bundesministerium für Inneres in Wien zeigten Expertinnen und Experten der Polizei und des Verfassungsschutzes aus Österreich, Deutschland und der Schweiz, welche Arten von Bedrohungen Unternehmen kritischer Infrastruktur ausgesetzt sein können und präsentierten Abwehrmaßnahmen. Der Verfassungsschutz im Innenministerium und die militärischen Nachrichtendienste sehen Betreiber kritischer Infrastruktur, die mit dem Internet verbunden sind, einer immer größeren Bedrohung durch Cyber-Angriffe ausgesetzt.

Von Bedeutung sind vor allem Unternehmen, Systeme und Organisationen für die Daseinsvorsorge in der Gesellschaft. An der Veranstaltung nahmen über 270 Personen teil, darunter die Geschäftsführer und Sicherheitsbeauftragten der strategisch wichtigsten Unternehmen und Organisationen der kritischen Infrastruktur Österreichs.

„Ziel der Veranstaltung ist es gewesen, die Geschäftsführer und Sicherheitsbeauftragten zu sensibilisieren und die Zusammenarbeit zwischen den Unternehmen und den Sicherheitsbehörden zu verstärken“, sagte Ing. Mag. Sylvia Mayer, Leiterin des Referats Schutz kritischer Infrastruktur im BVT. „Der Schutz kritischer Infrastruktur kann nur

Fotos: Thomas Cerny/LPD Wien, Erwin Scheriau/Expa/Picturedesk



**Sabotage: durchtrennte Datenkabel bei Mobilfunksendemasten.**

**Übung „Aida 2017“: Polizei und Bundesheer in Niederösterreich übten den Schutz kritischer Infrastruktur.**

in vertrauensvoller Kooperation zwischen den staatlichen Stellen und den Unternehmen und Organisationen, die eine Anlage kritischer Infrastruktur betreiben, erfüllt werden.“ Mayer betonte die gute Zusammenarbeit der Sicherheitsverantwortlichen der Unternehmen und Organisationen der kritischen Infrastruktur mit den Mitarbeitern ihres Referats. Dazu zählen 400 Unternehmen aus den verschiedensten Bereichen der Daseinsvorsorge – darunter Stromversorger, öffentliche Verkehrsunternehmen, Krankenhäuser, Medikamentenhersteller und Banken.

Da der Ausfall bestimmter Unternehmen der kritischen Infrastruktur schwerwiegendere Folgen hätte, als der Ausfall anderer, wurden die Unternehmen in die Kategorien A, B und C eingestuft. „Wir unterscheiden dabei zwischen dem Zeitfaktor, der Art der Auswirkung, dem Ausmaß der Auswirkung und der Redundanz“, erläuterte Referatsleiterin Mayer. Zum „Zeitfaktor“ zählen Ausfälle von Unternehmen kritischer Infrastruktur, die sich innerhalb kurzer Zeit bemerkbar machen und sich unmittelbar auf die Gesellschaft auswirken. Unter „Art der Auswirkungen“ fallen jene Unternehmen, deren Ausfall sicherheitspolizeiliche Auswirkungen oder die Gefährdung von Leib und Leben nach sich ziehen würde. Unter „Ausmaß der Auswirkungen“ zählen Unternehmen, bei deren Ausfall eine Vielzahl von Menschen betroffen ist. Unter „Redundanz“ zählen Ausfälle, deren Leistung nicht oder kaum durch andere Infrastrukturen ersetzt werden kann.

**Wesentliche Bedrohungen** für die kritische Infrastruktur sind Terrorismus, Spionage, Extremismus und Einzeltäter.

- *Terrorismus:* Laut dem BVT sind Unternehmen kritischer Infrastruktur erhöht durch Terrorismus bedroht. Bei Anschlägen geht es darum, Ziele mit einem hohen Symbolwert zu treffen, um eine breite mediale Aufmerksamkeit zu erreichen. Dies trifft insbesondere den Sektor öffentlicher Verkehr und Transport. Im Jänner 2017 führte die Polizei Ermittlungen wegen des Verdachts geplanter Anschläge auf die Verkehrsinfrastruktur in Wien.
- *Spionage:* Nachrichtendienste und Konkurrenzunternehmen sind an technischem Know-how, Produkten oder Marketingstrategien von Unternehmen interessiert, um Wettbewerbsvorteile zu erlangen. Die zunehmende elektronische Vernetzung hat zu erhöhten Risiken geführt. Im September 2016 wurde das Aufstellen zweier Wärmebildkameras in der Nähe einer Anlage kritischer Infrastruktur angezeigt. Ermittlungen ergaben, dass die Kameras einem amerikanischen Unternehmen gehörten, und Betriebsvorgänge innerhalb des Unternehmens hätten aufzeichnen können.
- *Extremismus:* Die Palette der Aktivitäten reicht von gewalttätigen Demonstrationen, Brandanschlägen und Sachbeschädigungen bis hin zu Cyber-Angriffen auf Unternehmen. Aktionen zeigen sich vor allem gegen Bauprojekte auf dem Energiesektor oder gegen den Finanzsektor, wie zuletzt beim Bau des Murkraftwerkes in Graz, wobei es zu Drohungen gegen Vorstände des Unternehmens kam. Aktivisten der „Identitären Bewegung“ entrollten am 6. März 2017 auf dem Dach des ORF-Landesstudios Steiermark in Graz ein Transparent und entzündeten bengalische Feuer. Sie konnten noch vor dem Eintreffen der Polizei flüchten.

Darüber hinaus sind seit Mitte 2014 schnell wachsende, den Rechtsstaat ablehnende staatsfeindliche Verbindungen zu verzeichnen. Mitarbeiter der Betreiber von Unternehmen der kritischen Infrastruktur wurden 2016 von Vertretern dieser staatsfeindlichen Verbindungen kontaktiert. Diese lehnen es zum Beispiel ab, eine Mahnung wegen einer ausstehenden Stromrechnung zu begleichen und schicken den Sachbearbeitern eine Kulanzmitteilung mit dem Hinweis, die Mahnung verstoße gegen die Universal- und Menschenrechte. Das BVT hat Handlungsempfehlungen für den Umgang mit Vertretern staatsfeindlicher Verbindungen an die Unternehmen kritischer Infrastruktur ausgesandt.

- *Einzeltäter:* 2016 wurden Unternehmen kritischer Infrastruktur durch Einzeltäter bedroht, die keiner Ideologie zuzurechnen waren. Es gab Bombendrohungen gegen Telekommunikationsbetreiber, Rettungsdienste oder Krankenhäuser, die mitunter die Evakuierung von Gebäuden und Unterbrechung des Betriebs erforderten.

**Kooperation stärken.** „Diese Bedrohungen zeigen, dass eine verstärkte Kooperation notwendig ist, um den Gefahren gemeinsam begegnen zu können“, sagte Referatsleiterin Sylvia Mayer. In

Fotos: Albin Fuss/BMLVS, LPD Steiermark

**Gefahrenquelle Internet: Kraftwerke werden über Systeme gesteuert, die oft ungeschützt mit dem Netz verbunden sind.**

Gesprächen wird das Vertrauen untereinander gestärkt sowie der Informationsaustausch verbessert. Experten des BVTs stellen ihr Wissen zur Sicherheit von Anlagen, IT-Sicherheit, Risiko- und Krisenmanagement sowie Bedrohungen durch Terrorismus, Extremismus etc. zur Verfügung. Mit gemeinsamen Übungen bereiten sich die Landespolizeidirektionen, das Bundesheer und Unternehmen auf den Ernstfall vor. Das hilft auch, Strukturen und Kommunikationswege kennenzulernen und besser einschätzen zu können.

Ein Objektschutzkatalog umfasst die wichtigsten Objekte und Anlagen aller Unternehmen der Kategorie A, wie Rechenzentren, Umspannwerke und Leitstellen. Die Landesämter für Verfassungsschutz und Terrorismusbekämpfung haben über diese Objekte Informationen zur Umgebung, Ein- und Ausgänge sowie kritische Bereiche innerhalb des Objektes, um in Anlassfällen die Einsatzkräfte rasch mit den wichtigsten Informationen versorgen zu können.

**Meldepflichten bei Angriffen.** Dem Parlament soll bis Herbst 2017 ein Entwurf des Innenministeriums für das Bundesgesetz für Cyber-Sicherheit vorlegen. Darin sollen die Zuständigkeiten von Polizei und Militär im Fall schwerwiegender Cyber-Angriffe auf Infrastrukturbetreiber und die Republik geregelt werden. Betreiber kritischer Infrastruktur sollen verpflichtet werden, schwerwiegende Cyber-Angriffe zu melden.

Die Größe des Unternehmens ist dabei nicht entscheidend, sondern die Art des Schadens. Wird durch einen Angriff das öffentliche Leben betroffen, muss der Schaden angezeigt werden. Informationen über Angriffe sollen künftig anderen Infrastrukturbetreibern zur Verfügung stehen, damit sie sich vor Angriffen auf die eigenen Systeme schützen können.

**Digitalfunk für Unternehmen.** Betreiber von Unternehmen kritischer Infrastruktur sollen Partner in dem vom Innenministerium betriebenen „Digitalfunk BOS Austria“ werden – dem Kommunikationssystem der Sicherheitsbehörden und der Organisationen mit Sicherheitsaufgaben. Das digitale Funknetz, mit dem inzwischen fast alle Bundesländer und Sicherheitsorganisationen verbunden sind, gewährleistet eine ausfallsichere und verschlüsselte Kommunikation untereinander. *ÖBB, Flughafen Wien, A1 Telekom* und etwa 120 weitere Betreiber bekommen Zugang zu diesem Behördenfunknetz.

„Wir möchten diese für die Funktion der Gesellschaft so wichtigen Unternehmen und Organisationen dahingehend unterstützen, dass sie auch im Fall eines ernsten Infrastrukturversagens schnell und sicher untereinander und mit dem BVT kommunizieren können“, sagte Innenminister Mag. Wolfgang Sobotka bei der Präsentation des Projekts „GEMEINSAM.SICHER mit den Betreibern kritischer Infrastruktur“ beim Symposium.

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

SCHUTZ KRITISCHER INFRASTRUKTUR

## Rechtslage

**Sicherheitspolizeigesetz.** Die zentrale Rechtsnorm für die sicherheitsbehördliche Zuständigkeit für den Schutz kritischer Infrastruktur befindet sich in § 22 SPG. Grundsätzlich ist die Polizei für den Schutz von Rechtsgütern zuständig, wenn es bereits zu strafbaren Handlungen gekommen ist. Eine der Ausnahmen von diesem Grundsatz findet sich in § 22 SPG, in dem der vorbeugende Schutz von Rechtsgütern geregelt ist. Dieser gilt unter anderem für verfassungsmäßige Einrichtungen wie das BMEIA, völkerrechtliche Objekte wie Botschaften und seit 2014 auch für die kritische Infrastruktur.

**Strafgesetz.** Mit der Strafrechtsnovelle 2016 wurde der Schutz kritischer Infrastruktur verbessert. Angriffe auf Computersysteme von diesen Unternehmen, Sachbeschädigungen oder Datendiebstahl sind seit 1. Jänner 2016 ebenso mit einer höheren Strafe qualifiziert, als bei sonstigen Unternehmen.

Wo bei einem normalen Diebstahl eine Strafe von bis zu sechs Monaten droht, ist für den Diebstahl eines wesentlichen Bestandteils einer kritischen Infrastruktur eine Strafhöhe von bis zu drei Jahren festgelegt.

FOTO: WERNER SABITZER