Sabotage, Drohungen, Angriffe

2016 gab es eine Zunahme der Zahl an Angriffen gegen Unternehmen kritischer Infrastruktur. Vor allem die Zahl an Cyber-Angriffen ist gestiegen.

Banken, Mobilfunkbetreiber, der Österreichische Rundfunk (ORF), die Zentralanstalt für Meteorologie und Geodynamik, der Flughafen Wien – sie alle zählen zu Einrichtungen der kritischen Infrastruktur des Landes und sie alle wurden 2016 Opfer von Cyber-Angriffen. Kritische Infrastruktur sind Unternehmen, Systeme, Anlagen, Prozesse, Netzwerke oder Teile davon, die eine Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Ausfall schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung hätte.

Gefahr für Unternehmen kritischer Infrastruktur: Die Zahl der Cyber-Angriffe steigt an.

Österreich kann auf einen hohen Grad an Versorgungsicherheit bei Lebensmitteln, Verkehrs-, Telekommunikation-, Energie- und Finanzdienstleistungen verweisen sowie auf eine gesicherte Versorgung mit Sozial- und Gesundheitsdienstleistungen.

Die Funktionsfähigkeit kritischer Infrastruktur ist unter anderem gefährdet durch Naturkatastrophen, technische Gebrechen, menschliches Versagen, Gefahren im Cyber-Raum, Kriminalität und Terrorismus. Der Schutz der Ausfallsicherheit solcher Infrastruktur durch den Staat genießt daher Priorität.

SKI-Report. Für den Schutz kritischer Infrastruktur sind das Bundeskanzleramt und das Bundesministerium für Inneres zuständig – operativ ist es das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT). Das BVT gibt für die Betreiber kritischer Infrastruktur jährlich den Bericht zum Schutz kritischer Infrastruktur (SKI-Report) heraus. 2016 wird darin über sicherheitsrelevante Vorfälle 2015/2016 berichtet. Immer mehr Gefahren gehen von Terrorismus, Extremismus und Cyber-Bedrohungen aus. Die Zahl der Fälle mit Einzeltätern nimmt zu.

Energie. Die sinkende Verfügbarkeit von Gas- und Kohlekraftwerken als „Reserve“ und die verstärkte Einbindung erneuerbarer Energien in das Stromnetz führt zu einem steigenden Risiko längerfristiger Stromausfälle.

2016 gab es in Österreich überwiegend Stromausfälle aufgrund technischer Gebrechen und massiver Schneefälle. Im Mai 2016 wurden Kupferkabel in niederösterreichischen Umspannwerken gestohlen. Ein Kohlekraftwerk in der Lausitz in Deutschland trennten Aktivisten vom Nachschub ab.

In der Zeit von Oktober bis Dezember 2016 beschädigte ein mittlerweile ausgeforschter Täter in der Steiermark zehn Strommasten und einen Telefonleitungsmasten, indem er sie mit einer Säge oberhalb des Betonsockels ansägte. Zwei Strommasten und der Telefonmast stürzten um. Kabel rissen jedoch nicht. Weitere drei beschädigte Strommasten wurden von Mitarbeitern des lokalen Elektroversorgungsunternehmens entdeckt und gesichert. Drei angesägte Masten wurden vom Täter selbst provisorisch mit verschraubten Metallbändern gesichert und sollten erst bei einem größeren Sturm umfallen. In Oberösterreich beschädigten bislang Unbekannte im Herbst 2016 zwei Strommasten.

Finanzen. Österreichische Finanzinstitute waren 2016 Opfer von Cyber-Angriffen, die jedoch keine gravierenden Auswirkungen zeigten. Cyber-Angriffe können die Funktionsfähigkeit von Bankomaten, des unbaren Zahlungsverkehrs oder des Online-Bankings beeinträchtigen. Die Webseite der *Oesterreichischen Nationalbank* wurde im September und Dezember 2016 durch DDos-Attacken vorübergehend lahmgelegt. Zu den Angriffen bekannte sich eine türkische Aktivistengruppe.

Gesundheit. 2016 gingen einige Drohungen gegen Krankenhauseinrichtungen ein. Zu einem regional begrenzten Blutkonserven-Engpass kam es vorübergehend, da vermehrt Blutspender aufgrund einer Virus-Infektion abgewiesen werden mussten.

Die Bandbreite an Gefahren für die Gesundheitsinfrastruktur zeigte auch eine Amokfahrt auf einem Krankenhausgelände und ein Feuerwehreinsatz in Folge eines undichten Chemikalienbehälters in einem Krankenhaus.

Mobilfunkbetreiber. 2016 kam es wiederholt zu telefonischen Bombendrohungen gegen einen österreichischen Telekommunikationsbetreiber. Die Anrufe gingen auf denselben Urheber zurück und führten zu mehrmaligen Polizeieinsätzen mit Evakuierungen. Sprengstoffspürhunde der Polizei durchsuchten das Unternehmensgebäude.

Fernsehsender. Erdogan-Gegner versuchten im August 2016, in das ORF-Zentrum in Wien zu gelangen. Einigen der zehn Aktivisten schummelten sich am Portier vorbei in das Gebäude, wo sie während einer Live-Sendung eine Petition übergeben wollten. Die Aktivisten wurden von Polizisten vom Gelände begleitet, es kam zu keiner Eskalation. Ein ähnlicher Vorfall – ebenso ohne Auswirkungen – ereignete sich im November 2016 in Vorarlberg.

FOTO: GLEBSTOCK/FOTOLIA

Krankenhäuser gehören zur kritischen Infrastruktur: 2016 erhielten einige Spitäler Drohungen.

Der Flughafen Wien-Schwechat war 2016 von DDoS-Angriffen betroffen.

Transport und Verkehr. Im August 2016 führten Kommunikationsprobleme zwischen *Eurocontrol* und *Austrocontrol* zu stundenlangen Flugverspätungen und Flugausfällen. Ein Hardware-Fehler soll die Übermittlung von Fluggastdaten verhindert haben, wodurch Mitarbeiter der Austrocontrol die für die Landungen erforderlichen Daten manuell ergänzen mussten. Das technische Problem, von dessen Auswirkungen ca. 3.000 Passagiere betroffen waren, konnte nach etwa vier Stunden behoben werden. Der Normalzustand war erst in den Morgenstunden des Folgetages wiederhergestellt.

Wasser. In einer Kläranlage in Salzburg traten 2016 beim Auffüllen des Tanks mehrere Tausend Liter flüssiges Eisensulfat aus, das bei Kontakt reizend bis ätzend auf die Haut und beim Einatmen auf die Schleimhäute wirkt. Es bedurfte des Einsatzes speziell ausgebildeter Feuerwehrleute und einer Spezialfirma, um die Flüssigkeit abzupumpen. Es wurde niemand verletzt und es bestand keine Gefahr für die Umwelt.

Cyber-Angriffe. Im Jänner 2016 kam es zu DDoS-Angriffen auf einen Mobilfunkbetreiber. Die Angriffe führten zu stundenlangen Systemausfällen. Ebenfalls im Jänner 2016 legten DDoS-Angriffe auf die Zentralanstalt für Meteorologie und Geodynamik mehrere Server lahm, wodurch der Datenaustausch mit Wetterdiensten teilweise unterbrochen wurde. Anfang September 2016 wurden Einrichtungen der kritischen Infrastruktur von mutmaßlich politisch motivierten DDoS-Angriffen betroffen. In mehreren Wellen wurden der Flughafen Wien-Schwechat, die *Oesterreichische Nationalbank,* die Website eines prominenten österreichischen Politikers, das Bundesministerium für Landesverteidigung und Sport, das Bundesministerium für Europa, Integration und Äußeres sowie weitere Ziele angegriffen. Für diese Vorfälle soll die türkische Hackergruppe „Aslan Neferler Tim“ verantwortlich gewesen sein. Sie reagierte damit nach eigenem Bekunden auf – aus ihrer Sicht – türkeifeindliche Aktionen, die von den betroffenen Einrichtungen gesetzt worden waren. Alle Angriffsopfer waren offenbar gut auf eine derartige Situation vorbereitet: Es kam zu keinem Ausfall eines sicherheitskritischen Systems.

Im September und Oktober 2016 fanden die drei größten bislang bekannten DDoS-Angriffe statt. Die Angriffe erfolgten auf Basis des Botnets *MIRAI*. Das erste Opfer war im September der amerikanische Journalist, Aufdecker und IT-Sicherheitsexperte Brian Krebs. Sein Blog „Krebs on security“ wurde Ziel eines DDoS-Angriffes mit einer Bandbreite von etwa 620 Gigabit/Sekunde.

Kurze Zeit später folgte ein Angriff auf den französischen Hosting-Provider *OVH,* der kurzzeitig eine Bandbreite von etwa 1 Terrabit/Sekunde erreichte. Der folgenschwerste Angriff folgte schließlich im Oktober, als der amerikanische DNS-Service-Provider *Dyn* mit einer Bandbreite von 1,2 Terrabit/Sekunde angegriffen wurde. Da eine Reihe von populären Internet-Diensten Kunden von *Dyn* sind, kam es zu Ausfällen, unter anderem bei *GitHub, Twitter, Reddit, Netflix* und *Airbnb*. Es ist zu befürchten, dass dies erst der Anfang davon war, was *MIRAI* zu leisten imstande ist. Der Quellcode von *MIRAI* ist frei im Internet verfügbar und steht jedem technisch Versierten zur Verfügung.

Ausblick. Die Zahl an unbemannten Luftfahrzeugen („Drohnen“) nimmt zu. Beim Betrieb von Drohnen kommt es immer wieder zu Zwischenfällen. Sie sorgen in letzter Zeit immer häufiger für Aufregung über Regierungsgebäuden, Atomkraftwerken, Justizvollzugsanstalten oder in der Nähe von Flughäfen. *UAVs (Unmanned Aerial Vehicles)* werden immer öfter im Service- oder Wartungsdienstleistungsbereich kritischer Infrastruktur eingesetzt. Kritische Infrastruktur oder Menschenansammlungen sind als Angriffsziele nicht auszuschließen. Selbst für den Privatgebrauch konzipierte UAVs sind leistungsfähig genug, um für Angriffe genutzt zu werden. Die Zahl der UAVs in den USA wird sich nach Schätzungen der US-Luftfahrtbehörde *FAA* bis 2020 nahezu verdreifachen. In Österreich ist ebenfalls ein Anstieg der Verkaufszahlen bemerkbar.

EU-Richtlinie. Die Bestrebungen nationaler Gremien in Österreich nach einer Erhöhung der Netz- und Informationssicherheit sowie nach einer Steigerung der Cyber-Resilienz, wurden im August 2016 auf europäischer Ebene durch das In-Kraft-Treten einer europäischen Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) ergänzt und unterstützt. Da europäische Richtlinien im Regelfall keine unmittelbare Rechtskraft in den Mitgliedstaaten haben, ist es erforderlich, die Richtlinie bis Mai 2018 in nationales Recht (Bundesgesetz für Cyber-Sicherheit) umzusetzen.

Fotos: Michael Fritscher/Picturedesk.com, Egon Weissheimer