Stromerzeugungsanlagen zählen zur kritischen Infrastruktur eines Landes und können Ziele von Sabotage werden.

FOTO: BIRN WYLEZICH/FOTOLIA

Warnen, informieren, beraten

Das Cyber-Security-Center im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung koordiniert Maßnahmen zur Stärkung der Cyber-Sicherheit und zum Schutz kritischer Infrastruktur.

Ein großflächiger Stromausfall, ein „Blackout", kann die Vorsorge eines Landes lahmlegen. Dazu zählt die Versorgung mit Strom, Treibstoffen, Wasser, Lebensmitteln und Medikamenten. Stromerzeugungsanlagen zählen zur kritischen Infrastruktur eines Landes. Diese sind auch Gefahren ausgesetzt, die von Terroristen oder Kriminellen drohen. Daher liegt der Schutz solcher Unternehmen im Interesse des Staates.

Im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) wurde ein Cyber-Security-Center (CSC) eingerichtet, das Maßnahmen zur Stärkung der Cyber-Sicherheit und zum Schutz kritischer Infrastruktur koordiniert. Das Cyber-Security-Center nahm 2015 den Probebetrieb auf und soll ab Jänner 2018 voll in Betrieb gehen.

IT-Spezialisten. „Derzeit sind wir mit dem Personalaufbau beschäftigt", sagt Dipl.-Ing. Philipp Blauensteiner, Leiter des Cyber-Security-Centers. Seit 2014 ist der Informatiker im BVT tätig, wo er mit der Leitung des Projekts „Cyber-Security .BVT" und dem Aufbau des CSC betraut ist. Blauensteiner arbeitete vorher als IT-Security-Consultant bei einer Bank. „Unsere Mitarbeiter sind IT-Spezialisten, keine Polizisten. Wir arbeiten jedoch eng mit den Ermittlern zusammen", sagt Blauensteiner. Zwei seiner elf Mitarbeiter gehörten dem österreichischen Team an, das im Oktober 2015 in Luzern die *European-Cyber-Security-Challenge* gewann. Zwei Mitarbeiter sind zertifizierte Information-System-Security-Professionals. Weiters zum Team gehören Studenten und Absolventen aus dem Bereich IT-Security, zwei frühere Mitarbeiter der *Telekom* und ein ehemaliger Bundesheer-Offizier.

Lagebild. „Unsere Aufgabe ist es, in Zusammenarbeit mit unseren Partnern den Entscheidungsträgern in Verwaltung und Wirtschaft ein Gesamtbild zur aktuellen Cyber-Lage zur Verfügung zu stellen", erklärt Blauensteiner. Im Rahmen der *Österreichischen Strategie für Cyber-Sicherheit (ÖSCS)* laufen derzeit mehrere Projekte, um die Sicherheit und Widerstandskraft der kritischen Infrastruktur gegen Cyber-Angriffe zu verbessern. Dazu gehört das KIRAS-Projekt „Cyber Incident Situational Awareness" (CISA), bei dem es um die Erstellung eines umfassenden Cyber-Lagebilds geht. Cyber-Informationen des Staates und von Unternehmen sollen zusammengeführt werden. Partner in dem Projekt sind das Innen-

ministerium, das Bundesministerium für Landesverteidigung und das Bundeskanzleramt. Die Spezialisten des Cyber-Security-Centers erarbeiten Handlungsempfehlungen für Unternehmen. „Wir nehmen dabei eine Vermittlerrolle ein“, sagt der CSC-Leiter. „Wenn uns Unternehmen berichten, wie sie erfolgreich einem Cyber-Angriff begegnet sind, leiten wir diese Informationen an andere Firmen weiter.“

Das Cyber-Security-Center arbeitet eng mit dem Cyber-Crime-Competence-Center (C4) im Bundeskriminalamt zusammen und mit *CERT.at,* dem österreichischen „Computer Emergency Response Team“. Die Mitarbeiter des C4 ermitteln bei Straftaten, die über das Internet verübt werden, etwa Onlinebetrug, Hacking und Verbreitung von Schadsoftware. Das C4 ist neben dem Cyber-Security-Center ein wichtiger Bestandteil der Cyber-Koordinierungsstruktur in Österreich. „Für uns ist es wichtig, mit den Trends und Entwicklungen vertraut zu sein und diese ins Cyber-Lagebild einfließen zu lassen“, sagt Blauensteiner.

Trends und Entwicklungen. 2015 waren in Österreich zahlreiche Unternehmen – auch der kritischen Infrastruktur – Ziel eines Cyber-Betrugsschemas, das als „CEO-Fraud“ bekannt wurde. Dabei werden vor allem Finanzabteilungen großer Unternehmen mit Hilfe von gefälschten E-Mails, die vermeintlich vom CEO (Geschäftsführer) des Unternehmens versandt werden, dazu gebracht, hohe Geldbeträge ohne Rückfragen für ein „streng geheimes Projekt“ auf verschiedene Konten zu überweisen. In Österreich wurden Schäden von mehr als 90 Millionen Euro registriert. Ein Dauerbrenner sind Phishing-Mails, in denen versucht wird, an persönliche Daten zu kommen. Zu den Trends zählen weiters die Verbreitung von Ransomware und DDoS-Attacken.

Ransomware (Erpressersoftware) wird über präparierte E-Mails, durch Sicherheitslücken in Webbrowsern und durch Herunterladen aus dem Internet *(Drive-by-Download)* verbreitet. Betroffen sein können Privatpersonen sowie Unternehmen, Behörden und sonstige Organisationen. Sobald ein Computer, ein Smartphone oder ein Tablet mit der Schadsoftware infiziert ist, werden die Daten darauf verschlüsselt,

KSÖ-Cybersecurity-Planspiel: Franz Einzinger (BMI), Franz Leitgeb (BMLVS), Wolfgang Czerni (KSÖ).

sodass nicht mehr darauf zugegriffen werden kann. Von der Verschlüsselung sind auch externe Datenträger und Netzlaufwerke betroffen. Sofern die Daten nicht vorsorglich mit einem Back-up gesichert wurden, sind diese verloren, wenn nicht innerhalb einer bestimmten Zeit „Lösegeld“ dafür bezahlt wird.

DDos-Attacken. 2015 traten kriminelle Vereinigungen wie „DD4BC“ und „Armada Collective“ in Erscheinung. Sie erpressten zahlreiche Unternehmen mit der Androhung, Onlinedienste eines Unternehmens mittels DDoS-Attacken lahmzulegen, falls diese nicht bereit seien, einen Geldbetrag zu bezahlen. Anfang 2016 wurde auch ein großer Mobilfunkbetreiber Ziel eines derartigen Angriffs. Der Angriff dauerte mehrere Tage an – die Auswirkungen für Kunden konnten durch das gut vorbereitete firmeninterne Notfallsteam minimiert werden.

Unter *DDoS (Distributed Denial of Service*) versteht man einen Angriff von vielen verteilten Rechnern (Bot-Netzen) auf ein Netzwerk, um es außer Kraft zu setzen. Beispielsweise wird eine Webseite mit derart vielen Anfragen überlastet, dass sie blockiert wird. Bot-Netze bestehen aus bis zu Hunderttausenden illegal verbundenen Computern. „Besonders anfällig sind vor allem Computer, die mit veralteter Software und mangelndem Virenschutz ausgestattet sind“, sagte CSC-Leiter Blauensteiner. Ermittler des österreichischen Bundeskriminalamts konnten die *DD4BC*-Gruppe ausforschen und damit einen international beachteten Erfolg erzielen.

Sicherheitslücken. Ein Problem 2015 waren Schwachstellen in zentralen Netzwerkkomponenten der internationalen IKT-Infrastruktur. Bei diesen Geräten handelt es sich um das Rückgrat eines jeden Computer-Netzwerkes. Zu den spektakulärsten Sicherheitslücken in diesem Bereich zählten im September 2015 *SYNful Knock* und im Dezember 2015 das *Juniper-Backdoor*. Bei *SYNful Knock* handelte es sich um einen Angriff auf Netzwerk-Komponenten des weltweit führenden Anbieters von Netzwerk-Lösungen für das Internet. Dabei wurde die eingebaute Update-Funktionalität vieler Geräte missbraucht, um Teile der geräteeigenen Software mit Schadcode zu überschreiben. Beim *Juniper-Backdoor* handelte es sich um zwei ursächlich nicht zusammenhängende Sicherheitslücken beim weltweit zweitgrößten Netzwerkausrüster. Diese ermöglichten Angreifern das Mitlesen von verschlüsseltem Netzwerkverkehr.

Internet der Dinge. Eine große Herausforderung für die kommenden Jahre liegt im Bereich des „Internet of Things“ (Internet der Dinge). Die Informationstechnik wird Teil von Geräten oder Gegenständen des Alltags (Haushaltsgeräte, Kleidung, Fahrzeuge). Betroffen sein werden der private Wohnbereich (*Smart Homes*), der Individualverkehr (*Smart Cars*) und der öffentliche Verkehr (z. B. Flugverkehr). Die in diesen Bereichen eingesetzte Cyber-Technologie ist relativ jung. Berichte von Sicherheitsunternehmen zeigten 2015 teils gravierende Sicherheitsmängel in der Haussteuerung per Internet. Im Februar 2015 wurde bekannt, dass sich Fahrzeuge eines deutschen Premiumherstellers über dessen vernetzte Assistenzsysteme innerhalb weniger Minuten öffnen ließen. Im April 2015 wurde ein IT-Sicherheitsexperte festgenommen, der behauptet hatte, mehrmals über das Entertainment-System in die Avioniksysteme von im Flug befindlichen Flugzeugen vorgedrungen zu sein. Und im Juli 2015 wurde ein fahrender US-Geländewagen gehackt und aus mehreren Kilometern Entfernung wurde dessen Motor während der Fahrt abgestellt.

Auch die potenzielle Verwundbarkeit von Unternehmen der kritischen Infrastruktur nimmt zu. Diese Unternehmen verfügen oft über Schwachstellen in Kontrollsystemen, die über Internet erreicht werden können. Dazu zählen Kontrollsysteme wie *SCADA (System Supervisory Control and Data Aquisition)*. Im Unterschied zu klassischen IT-Produkten sind die Entwick-

FOTO: WOLFGANG ROSENKRANZ

lungszyklen von Steuerungs- und Kontrollsystemen um ein Vielfaches länger, was zur Folge hat, dass Sicherheitsupdates („Patches“) nicht im selben Umfang bzw. Zeitrahmen zur Verfügung gestellt werden. Viele der verwendeten Protokolle stammen aus einer Zeit, als diese Systeme in abgeschotteten („air-gapped“) Umgebungen liefen und umfangreiche Sicherheitskonzepte für den Cyber-Bereich nicht notwendig waren. Mit der fortschreitenden Komplexität und Vernetzung solcher Systeme bestehen mittlerweile mannigfaltige Anbindungen an andere – oft auch von außen erreichbare – Netze. Da diese Steuerungssysteme in zahlreichen Einrichtungen kritischer Infrastruktur, unter anderem in Kraftwerken, Pipelines und Pumpwerken, eingesetzt werden, besteht ein immer dringlicherer Bedarf, die Sicherheitsmaßnahmen im Cyber-Bereich zu forcieren.

Cyber-Angriffe. Im Juli 2015 erfolgte ein Cyber-Angriff auf die italienische Firma „Hacking Team“ – einen Hersteller von Spionagesoftware, zu dessen Kunden Geheimdienste und Regierungen in vielen Ländern zählen. Den Angreifern gelang es, Hunderte Gigabyte an unternehmensinternen Daten zu stehlen und im Internet zu veröffentlichen. Darunter befanden sich Kundenlisten, Inhalte interner Kommunikation, Rechnungen und große Teile des Sourcecodes der Spionagesoftware. Experten befürchten, dass die Spionagesoftware durch die Verbreitung im Internet als Basis für neue Schadprogramme herangezogen wird.

In Frankreich kam es im April 2015 zu einem Cyber-Angriff auf den Fernsehsender „TV5 Monde“. Die Fernsehkanäle waren mehrere Stunden blockiert. Gleichzeitig wurde während der Attacke auf den Webseiten und Social-Media-Konten des Senders Propaganda für die Terrormiliz „Islamischer Staat“ (IS) verbreitet. Bis heute ist die Urheberschaft des Angriffs unklar. Laut der Polizei könnte es sich bei dem offensichtlich islamistischen Hintergrund auch um ein Täuschungsmanöver handeln, das von den eigentlichen Angreifern und ihren Motiven ablenken sollte.

In Deutschland wurde ein Cyber-Angriff auf den deutschen Bundestag entdeckt. Mehrere Monate verbreitete sich Schad- bzw. Spähsoftware unbemerkt im Netzwerk des Bundestages, bevor im Mai 2015 das Ausmaß des Angriffs sichtbar wurde. Nach Meinung von Experten handelte es sich bei diesem Vorfall um den bisher größten Cyber-Angriff auf den Bund und das deutsche Parlament.

Internet der Dinge: Die Informationstechnik wird Teil von Geräten oder Gegenständen des Alltags sein – etwa im Wohnbereich („Smart Homes“).

Prävention. Ein Schwerpunkt der Arbeit des CSC waren 2015 Beratungen, Awareness-Veranstaltungen sowie Informationen und Frühwarnungen an Betreiber kritischer Infrastruktur zu Bedrohungen im Cyberspace. Der Fokus im Jahr 2016 liegt im Bereich Cyber-Krisenmanagement sowie auf den rechtlichen Grundlagen. Derzeit werden für Cyber-Sicherheit auf EU-Ebene und auf nationaler Ebene rechtliche Rahmenbedingungen geschaffen.

Im Juli 2016 verabschiedete das Europäische Parlament die Richtlinie zur Netz- und Informationssicherheit. Eine interministerielle Arbeitsgruppe, an der Vertreter des BVT beteiligt ist, widmet sich der Umsetzung dieser Richtlinie in ein Bundesgesetz für Cyber-Sicherheit. Das Bundesgesetz soll neben der rechtlichen Basis für eine Erhöhung der Netz- und Informationssicherheit auch der Steigerung der Resilienz dienen – der Widerstandsfähigkeit im Bereich Cyber-Sicherheit.

Cyber-Planspiele. Die *Österreichische Strategie für Cyber-Sicherheit* sieht unter anderem vor, dass durch regelmäßige Cyber-Übungen das Cyber-Krisenmanagement und die Krisenmanagement- und Kontinuitätspläne getestet werden. Im Mai 2016 fand ein vom *Kuratorium Sicheres Österreich (KSÖ)* veranstaltetes Planspiel zum Cyber-Krisenmanagement statt, an dem auch das CSC teilnahm. Auf europäischer Ebene entsandte das CSC Beobachter zum Planspiel *Locked Shields* des *NATO Cooperative Cyber Defence Centres of Excellence (CCDCOE)*. Dabei konnten Erfahrungen zum Schutz kritischer IKT-Infrastruktur gesammelt werden.

Ziel der Cyber-Übung „Strategic Decision-making in Cyber Security“ im September 2015 war das Training der strategischen Entscheidungsfindung im Cyber-Krisenmanagement sowie die Kommunikation und Koordination zwischen den beteiligten staatlichen Stellen und den Betreibern kritischer Infrastruktur.

Die Übung wurde von der *European Defence Agency (EDA)* und der *Europäischen Agentur für Netzwerksicherheit (ENISA)* organisiert. Die Vertreter des Cyber-Security-Centers beteiligten sich im Team „Innere Sicherheit und Justiz“ daran.

Die Analyse zeigte, dass sich die österreichische Konzeption des Cyber-Krisenmanagements mit ziviler Ausrichtung unter der Koordination des Cyber-Security-Centers bewährt und die ressortübergreifende Kommunikation rechtzeitig initiiert wurde. Derzeit laufen die Vorbereitungen zum europaweiten Planspiel „Cyber Europe“, das von der ENISA im Herbst 2016 zum vierten Mal seit 2010 veranstaltet wird.

Siegbert Lattacher

Foto: Weedezign/Fotolia