Versorgung sicherstellen

Drohnengefahr, Innentäter, Bewerberüberprüfung waren unter anderem Themen beim Symposium zum Schutz kritischer Infrastruktur am 19. September 2019 im Bundesministerium für Inneres.

Geschäftsführer, Direktoren und Sicherheitsbeauftragte der strategisch bedeutendsten Einrichtungen kritischer Infrastruktur, die für die Versorgung mit den lebenswichtigsten Gütern und Dienstleistungen in Österreich verantwortlich sind, nahmen am Symposium zum Schutz kritischer Infratsruktur im Bundesministerium für Inneres teil. Die Veranstaltung fand bereits zum vierten Mal statt und wurde auch 2019 vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung ausgerichtet.

„Die Mitarbeiterinnen und Mitarbeiter des BVTs leisten umfangreiche und wichtige Arbeit zum Schutz der kritischen Infrastruktur in Österreich und tragen damit wesentlich dazu bei, wichtige gesellschaftliche Funktionen aufrecht zu erhalten“, sagte Innenminister Dr. Wolfgang Peschorn bei der Eröffnung der Veranstaltung. Zu den Einrichtungen der kritischen Infrastruktur zählen unter anderem die Energie- und Wasserversorger, Lebensmittelversorger, Krankenhäuser, Hilfs- und Einsatzkräfte, Verkehrsunternehmen, Finanzdienstleister oder IT-Dienstleister.

Ziel der Veranstaltung war es, die Teilnehmerinnen und Teilnehmer über aktuelle Bedrohungen zu informieren und ihnen eine Reihe von Maßnahmen zur Bewältigung der Gefahren und Bedrohungen darzulegen. Es gibt zahlreiche Gefahren und Bedrohungen für die Betreiber von Unternehmen kritischer Infrastruktur. „Der islamistische Extremismus und Terrorismus, der Rechts- wie auch der Linksextremismus, Wirtschafts- und Industriespionage oder Sabotage, Störaktionen durch Drohnen und Erpressungen sind Bedrohungsbilder, die eine Gefahr für die kritische Infrastruktur darstellen“, erläuterte Ing. Mag. Sylvia Mayer, MA, stellvertretende Leiterin der Abteilung für Sicherheit und Schutz im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT).

Eigenverantwortung. Jedes Unternehmen hat selbst eine Vielzahl von

Foto: Gerd Pachauer

Sylvia Mayer appellierte an die Eigenverantwortung von Unternehmen, für ihre Sicherheit zu sorgen.

Maßnahmen zu treffen, um die eigene Sicherheit und Funktionsfähigkeit gewährleisten zu können. „Gerade deshalb ist es von Bedeutung, dass sich diese Unternehmen untereinander austauschen, insbesondere in puncto Best Practices, neue Ideen und neue Produkte im Sicherheitssegment“, sagte Sylvia Mayer. Sie schilderte Vorfälle, von denen österreichische Unternehmen 2018 betroffen waren und gab einen Ausblick über die künftige Erstellung von Branchen-Risikoanalysen und Kooperationsvereinbarungen, die zwischen Unternehmen und dem BVT abgeschlossen werden sollen.

Gefahr durch Drohnen. Experten des Einsatzkommandos Cobra/Direktion für Spezialeinheiten erläuterten die Gefahren und die Herausforderungen, die „Unmanned Aerial Vehicles“ (UAVs) – besser bekannt als Drohnen – mit sich bringen. Die Zahl der Drohnen, die am Luftverkehr teilnehmen, steigt weltweit und auch in Österreich an. Damit erhöhen sich auch die Risiken von Zusammenstößen und Abstürzen. Ein Notarzthubschrauber nützt beispielsweise denselben Luftraum wie eine Drohne, nicht selten auch die gleiche Flughöhe. Das rechtzeitige Erkennen der „UAVs“ und ein sicheres Ausweichen stellen jeden Piloten vor eine gefährliche Herausforderung. In der Praxis sind solche Ausweichmanöver beinahe unmöglich. Welchen Schaden Drohnen anrichten können, zeigten die Angriffe auf die Produktionsstätten des staatlichen Ölkonzerns *Saudi Aramco* in Abkaik und Khurais, Mitte September 2019 im Osten Saudi Arabiens, mit Auswirkungen auf die gesamte Weltenergieversorgung.

Drohnenabwehr. Das Einsatzkommando Cobra ist für die Drohnenabwehr in Österreich zuständig. Die rechtlichen Voraussetzungen für den Einsatz von „UAV“-Abwehrsystemen und die „UAV“-Abwehr sind eine Bewilligung nach dem Telekommunikationsgesetz (TKG 2003) und das Vorliegen eines gefährlichen Angriffs im Sinne des Sicherheitspolizeigesetzes, beispielsweise zum Schutz geplanter anschlagsgefährdeter Veranstaltungen.

Beispiele solcher Veranstaltungen in jüngerer Vergangenheit waren der Staatsbesuch Vladimir Putins in Wien im September 2018 oder die letzte österreichische EU-Ratspräsidentschaft im zweiten Halbjahr 2018. Ein gefährlicher Angriff kann nur durch eine gerichtlich strafbare Vorsatztat verwirklicht werden, zum Beispiel durch eine Gefährdung der körperlichen Sicherheit. Fahrlässigkeitsdelikte oder Privatanklagedelikte nach dem Strafgesetzbuch oder Verwaltungsübertretungen, beispielsweise ein Verstoß nach dem Luftfahrtgesetz, rechtfertigen die UAV-Abwehr durch das EKO Cobra nicht.

Innentäter verhindern. Die Unternehmen kritischer Infrastruktur sind nicht nur Gefahren und Bedrohungen von außen, sondern auch von innen durch Mitarbeiter ausgesetzt. Dieser Risikofaktor wird in der Praxis von vielen Unternehmen unterschätzt. Karin Giangrande, BA – Leiterin „Pre-Employment Screening“ bei der *SIGNUM Consulting GmbH* – erläuterte die Gefahren, die Innentäter in einem Unternehmen mit sich bringen können. Mitarbeiterinnen und Mitarbeiter haben in der Regel Insiderwissen und können

Personalauswahl: Wichtig ist eine genaue Prüfung der Bewerbungsunterlagen.

mit diesem Wissen einem Unternehmen hohen Schaden zufügen. Der sorglose Umgang mit sensiblen Unterlagen, ein Vertrauensverhältnis zum unerkannten Innentäter wie auch das Fehlen einer Sicherheitskultur im Unternehmen, die eine solche Bedrohung berücksichtigt, sind Faktoren, die den Tätern ihre kriminellen Handlungen erleichtern.

Die Bedrohungen in einem Unternehmen gehen dabei sowohl von neu eingestellten als auch von langjährigen Mitarbeitern aus. Diese Personen haben häufig umfassende Benutzerrechte, sie kommen leicht an Daten oder Informationen heran und haben Kenntnis darüber, welche Anlagen im Unternehmen besonders kritisch sind. Innentäter können auch Geschäftspartner, Projektteilnehmer und freie Mitarbeiter sein, die ihre Position ausnutzen, um zusätzliche Einnahmen aus der Geschäftsbeziehung lukrieren zu können. Ebenso Angehörige und Freunde von Mitarbeitern können sich beispielsweise über einen Fernzugriff und mit dem Passwort des Mitarbeiters unerlaubt Zugriff auf firmeninterne Systeme verschaffen. Im Bereich der IT-Sicherheit stellt die Gefahr von Innentätern eine besondere Herausforderung dar. Die Motive der Innentäter sind unterschiedlich. Häufige Gründe sind Unzufriedenheit am Arbeitsplatz, die bevorstehende Kündigung oder ideologische Motive.

Bewerber genau durchleuchten. Unternehmen können bereits bei der Auswahl von künftigen Mitarbeitern und Mitarbeiterinnen Maßnahmen zur Vorbeugung gegen Innentäter setzen. Zu einem Risikomanagement zählen auch die Einhaltung von Sicherheitsaspekten bei der Personalwahl, wie beispielsweise die genaue Prüfung der Bewerbungsunterlagen, die Nachfrage bei bisherigen Arbeitgebern oder Universitäten und die Sicherheitsüberprüfung durch das BVT, für Mitarbeiter, die in sensiblen Bereichen beschäftigt werden sollen.

Eine nicht weniger große Rolle spielt die Bewusstseinsbildung bestehender Mitarbeiter. In diesem Zusammenhang gilt für Mitarbeiter in sensiblen Bereichen mitunter folgendes: keine Äußerungen über Probleme im Unternehmen an externe Personen tätigen, Vorsicht bei Auslandsreisen in Bezug auf die Verwahrung von Datenträgern oder bei neuen Bekanntschaften, das Melden relevanter Wahrnehmungen im Betrieb und keine unnötigen Offenbarungen von Informationszugängen und Verantwortlichkeiten im eigenen Unternehmen. Wenn bauliche Maßnahmen, zum Beispiel durch Zutrittskontrollen oder Videoüberwachung getroffen werden, ist es von Bedeutung, dass diese von den Mitarbeitern gelebt und nicht umgangen werden.

Sicherheit in Krankenhäusern. Die Mitarbeiter des Referats „Schutz kritischer Infrastruktur“ im BVT befassen sich auch mit der Sicherheit in Krankenhäusern. Dazu verschaffen sie sich einen Überblick über das jeweilige Objekt und geben Empfehlungen zur Verbesserung der physischen Sicherheit an die Geschäftsleitung ab. Dazu gibt es die Workshop-Reihe „Schützenswertes Krankenhaus“. Dieses Projekt wurde für den österreichischen Sicherheitspreis 2018 nominiert. Ziel dieser Kooperationen ist es, die Resilienz österreichischer Krankenhäuser zu verbessern. Beispielsweise durch die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Sicherheitsthemen wie physische Sicherheit, Großschadensereignisse (Terroranschlag), Cyber-Sicherheit im Krankenhaus und Objektschutz für Kliniken. Bis dato wurden zehn Workshops und 37 Begehungen von Krankenhäusern in fünf Bundesländern durchgeführt.

Weitere Themen der Veranstaltung waren „die aktuelle Cyber-Lage in Österreich“, wobei als größte Bedrohung die sogenannten „Advanced Persistent Threats“ – bei denen Unternehmen gezielt angegriffen oder infiltriert werden sollen – thematisiert wurden, „Business-E-Mail-Compromise und CEO-Fraud“, „Objektschutzblätter in der Praxis“ und „die Umsetzung des NIS-Gesetzes in Österreich“. (Über das NIS-Gesetz wurde in der September/Oktober-Ausgabe 2019 der „Öffentlichen Sicherheit“ berichtet).

Experten des staatlichen Krisen- und Katastrophenmanagements im BMI und von *Austrian Power Grid* erörterten Erfahrungen und Erkenntnisse aus der im Mai 2019 abgehaltenen Zivilschutzübung „Helios“ – bei der das Szenario eines großflächigen Stromausfalles („Blackout“) als Übungsannahme diente. Ziel der Übung war es, Kommunikationsstrukturen der „SKKM-Familie“ (Staatliches Krisen- und Katastrophenmanagement) zu testen und weiterzuentwickeln, um im Ernstfall möglichst reibungsfrei agieren zu können.

Vernetzung. Neben den Vorträgen hatten die Teilnehmerinnen und Teilnehmer, die unter anderem aus den Bereichen Energie, Finanzen, Forschung, Lebensmittel, Transport, Wasser, Hilfs- und Einsatzkräfte kamen, die Möglichkeit, sich untereinander auszutauschen und zu vernetzen.

„Die Komplexität der Bedrohungen steigt stetig an. Künftige Herausforderungen können wir nur gemeinsam bewältigen; und es ist wichtig, dass wir durch Kooperationen miteinander und voneinander lernen. Die Mitarbeiter des BVT stehen als Partner jederzeit zur Verfügung“, betonte Sylvia Mayer.

Gernot Burkert

FOTO: PIXEL-SHOT/STOCK.ADOBE.COM