SKI-Symposium: Vertreter von Sicherheitsbehörden und Sicherheitsverantwortliche von Unternehmen.

Thomas Müller: „Die Art und Weise der Entlassung eines Mitarbeiter hat Einfluss, ob er sich am Unternehmen rächen will."

Cyber-Sicherheit erhöhen

Beim Symposium „Kritische Infrastruktur – Lagebild 2018" im Innenministerium wurden Gefahren für Unternehmen der kritischen Infrastruktur und Schutzmaßnahmen diskutiert.

Cyberangriffe auf Unternehmen spielen eine immer größere Rolle und passieren fast täglich", sagte die Generaldirektorin für die öffentliche Sicherheit, Dr. Michaela Kardeis, beim Symposium „Kritische Infrastruktur – Lagebild 2018", am 14. Juni 2018 im Bundesministerium für Inneres; veranstaltet vom Referat „Schutz kritischer Infrastruktur" im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT). Alle Lebensadern unserer Gesellschaft seien mittlerweile auf IT-Systeme angewiesen und immer stärker miteinander vernetzt. Das bedeute ein immer größeres Risiko für unsere Energieversorgung, Transportsysteme oder Gesundheitsdienstleistungen. Der Ausbau des Cyber-Security-Centers im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung soll zur Erhöhung der Cyber-Sicherheit für diese kritische Infrastruktur in Österreich beitragen, sagte Kardeis.

Schutz vor Angriffen. Am Symposium nahmen die Sicherheitschefs der für die Bevölkerung wichtigsten Unternehmen und Organisationen teil. Darunter *OMV, Austrian Power Grid, Raiffeisen International*, *Österreichische Bundesbahnen, Flughafen Wien,* zahlreiche Krankenhäuser, Lebensmittelhändler und Wasserversorger Österreichs. „Wir versuchen, den Sicherheitschefs einen Überblick über die Bedrohungen für ihre Organisationen zu bieten und geben ihnen Tipps, wie sie sich davor schützen können", sagte Referatsleiterin Mag. Sylvia Mayer. „Ein weiteres Anliegen ist uns die Vernetzung zwischen den Unternehmen. Sicherheitsbeauftragte setzen Maßnahmen in ihrer Organisation und sie können davon profitieren, sich mit anderen darüber auszutauschen." Mayer ging auf Vorfälle 2017 ein, die unter anderem von gewalttätigem Aktionismus zur Verhinderung des Baus eines Kraftwerks, Spionageangriffen, Bombendrohungen gegen Krankenhäuser und Bahnhöfe reichten.

Michaela Kardeis: „Das Cyber-Security-Center im BVT soll ausgebaut werden."

Sylvia Mayer: „Unternehmen vor Gefahren warnen und unterstützen."

Angriffe erkennen. Eine BVT-Expertin erläuterte, wie Mitarbeiter radikalisiert werden und wie man dies erkennt. Kriminalpsychologe Dr. Thomas Müller sprach über die Gefahr von Innentätern in Unternehmen. Beispielsweise könne die Art und Weise, wie sich eine Organisation von einer Mitarbeiterin oder einem Mitarbeiter trenne, maßgeblichen Einfluss darauf haben, ob sich diese Person später an dem Unternehmen rächen wolle.

Neben Angriffen von innen wurde Augenmerk auf die Gefahren von außen gerichtet. In einem „Red-Team-Assessment" können externe Unternehmen beauftragt werden, zu versuchen, in die Unternehmen der kritischen Infrastruktur zu gelangen, um mögliche Schwachstellen aufzudecken.

Wie man mit einer telefonischen Bombendrohung in einem Unternehmen umgehen soll, wie man die Ernsthaftigkeit einer Drohung erkennt und wie Evakuierungen oder Produktionsstillstände weitgehend verhindert werden können, darüber informierte ein Experte des Einsatzkommandos Cobra/Direktion für Spezialeinheiten.

Das Symposium mit dem Titel „Kritische Infrastruktur – Lagebild 2018", an dem über 230 Personen teilnahmen, fand zum dritten Mal statt und hat sich mittlerweile zu einer bekannten Plattform mit dem vorrangigen Ziel des Vernetzens und Informationsaustausches entwickelt. *S. M.*

Fotos: Gerd Pachauer