KSÖ-Sicherheitsgipfel: Walter Unger, Mark Thorben Hofmann, Manuel Scherscher, Carsten Meywirth, Alexander Janda

Grußbotschaft von Joe Biden

Beim Sicherheitsgipfel des „Kompetenzzentrum Sicheres Österreich" (KSÖ) am 19. September 2023 in Wien drehte sich alles um die Bedrohung durch Cyber-Kriminalität und mögliche Gegenstrategien.

Cyber-Angriffe sind alltägliche Realität für Unternehmen, Regierungen und Privatpersonen. Die rasante Entwicklung der digitalen Welt eröffnet Kriminellen neue Chancen und Möglichkeiten. Datenlecks, Ransomware-Angriffe, Phishing – der Raffinesse und Kaltschnäuzigkeit von global agierenden Cyber-Kriminellen sind kaum Grenzen gesetzt, wie Hacker-Profiler Mark Thorben Hofmann beim KSÖ-Sicherheitsgipfel am 19. September 2023 in seinem Vortrag bewies: US-Präsident Joe Biden gratulierte in einer Videobotschaft den Initiatoren zu der gelungenen Veranstaltung und Mark Thorben Hofmann zu seiner Präsentation über „Die Psychologie der Cyber-Kriminalität". Stimme, Mimik, Aussehen – absolut authentisch. Einzig: Es handelte sich um ein anschauliches Beispiel für einen Deepfake, bei dem künstliche Intelligenz mittels echtem Bild- und Tonmaterial eine gefälschte Version einer Person generiert, die vom Original kaum unterscheidbar ist. Hacker würden immer den Weg des geringsten Widerstands gehen, führte Hofmann aus. „Der Schwachpunkt bei Cyber-Attacken ist meist nicht die Technik, sondern menschliches Fehlverhalten. Kriminelle hacken keine Technik, sondern Menschen und nutzen Computer als Waffen", ergänzte der Kriminal- und Geheimdienstanalyst und untermauerte seine These mit einem „Klassiker" aus dem Cybercrime-Bereich: Kurz vor Feierabend erreicht die Mitarbeiterin einer Firma ein dringender Telefonanruf. Ein ihr namentlich bekannter IT-Techniker erklärt der Frau mit der ihr vertrauten Stimme, dass die Firma gerade von Cyber-Kriminellen angegriffen wird und er einen Remote-Zugriff auf ihren Computer benötige, um diesen abzuwehren. Da angeblich jede Sekunde zählt, willigt die Mitarbeiterin ein – und ermöglicht dadurch erst die echte Cyber-Attacke.

Was sich wie das Drehbuch eines schlechten Films liest, geschieht weltweit täglich. „Cyber-Kriminelle hacken uns, während sie uns erklären, dass wir gerade gehackt werden. Sie beherrschen das Spiel auf der Klaviatur menschlicher Schwächen", sagte Hofmann. „Mit einem gesunden Mix aus technischen und menschlichen Vorsichtsmaßnahmen kann man sich gut schützen", empfahl der Experte, der für ein individuelles Verifizierungssystem plädierte. „Vereinbaren Sie Gegencheckfragen, die nur die zuständigen Personen beantworten können. Wer saß bei der letzten Vorstandssitzung wo, wie viele Topfpflanzen stehen im Büro etc." Geld sei nicht die einzige Motivation von Hackergruppen, „es geht ihnen auch um Anerkennung und Respekt", ergänzte Hofmann. Viele Straftaten würden von den Tätern als „Challenge" betrachtet und „hochprofessionell" durchgeführt werden, hielt der Experte fest.

Kriminelle Netzwerke. Ein Befund, dem nicht nur die Teilnehmer der Paneldiskussion „Cyber-Angriffe auf Staat und Wirtschaft – Risiken und Auswirkungen" zustimmten, sondern auch der Leiter der Gruppe „Cybercrime" des deutschen Bundeskriminalamts, Carsten Meywirth. „Seit 2015 beobachten wir eine Umstrukturierung krimineller Akteure", berichtete der Cyber-Kriminalist. Statt Einzelpersonen würden sich Tätergruppen verstärkt in

Fotos: Katharina Schiffl

„cyberkriminellen Ökosystemen mit kleinteiligen Arbeitsabläufen“ organisieren, bei denen sich die einzelnen „Kleinunternehmer“ persönlich nicht kennen. Analog zum legalen Wirtschaftssystem hätten sich diverse Plattformen gebildet, über die Kriminelle „Dienstleistungen und Know-how“ erwerben bzw. anbieten. „Sie müssen heute selbst technisch nicht versiert sein, um ein Cyber-Krimineller zu werden.“ Egal, ob Schadcodesoftware, gestohlene Kreditkartendaten oder Geldwäsche-Möglichkeiten – im Darknet gebe es nichts, was es nicht gibt. Selbst Stellenausschreibungen für illegale Services oder Helpdesk-Angebote wie in der realen Wirtschaftswelt seien keine Seltenheit, sagte Meywirth.

Vernetzte Gegenstrategie. „Cyber-Kriminalität ist eine globale Bedrohung. Wenn wir sie effektiv bekämpfen wollen, müssen wir neue Strategien anwenden“, ergänzte Meywirth. Tatortbezogene Ermittlungen würden „ins Leere“ führen, geografische Orte keine Rolle mehr spielen. „Nur als Team aus diversen Strafverfolgungsbehörden können wir Cyber-Kriminelle erfolgreich bekämpfen“, plädierte er für einen „engen Schulterschluss aller relevanter Akteure“. Als Best-Practice-Modell stellte Meywirth die 2020 geschaffene Cybercrime-Abteilung des deutschen Bundeskriminalamts vor, die er leitet. Mit kreativen Lösungsansätzen, flachen Hierarchien und einem Mitarbeiter-Mix aus IT-Spezialisten und Ermittlungsbeamten sei in Deutschland diese Vernetzungsstrategie bereits erfolgreich umgesetzt.

Prävention. Die Notwendigkeit eines gemeinsamen „Cybercrime-Fighting-Systems“ als Gegenprogramm zum „Crime-as-a-Service“-Konzept krimineller Tätergruppen konstatierten auch die Experten der Paneldiskussion „Cybersicherheit – Lösungswege und Prävention für Unternehmen und Behörden“. Der Informationsaustausch und die Vernetzung unterschiedlicher Behördenstellen und Dienste seien essenziell, um „schlagkräftig“ gegen Cyber-Kriminelle vorgehen zu können und „die Resilienz in der Gesellschaft insgesamt zu stärken“, betonte Klaus Mits vom österreichischen Bundeskriminalamt. Darüber hinaus appellierte der Abteilungsleiter an Cybercrime-Opfer, Anzeige bei der Polizei zu erstatten, denn „nur so können wir gegen Kriminelle tätig werden“.

Kriminaldienstreform. Den Abschluss der Veranstaltung bildete ein Ausblick von Manuel Scherscher, Abteilungsleiter im Bundeskriminalamt, auf die Eckpunkte der Kriminaldienstreform mit dem Schwerpunkt Cybercrime. Im Endausbau des im Frühjahr 2024 beginnenden Reformprozesses ist u. a. die Einrichtung von Cybercrime-Referaten in den Landeskriminalämtern sowie die Einrichtung von Kriminalassistenzdienststellen geplant. Das *Cybercrime Competence Center (C4)* wird zu einer eigenen Abteilung innerhalb des Bundeskriminalamtes.

„Die Reform ist ein wichtiger Schritt im Zeitalter der Digitalisierung. Ziel der größten Polizeireform seit 20 Jahren sind die Spezialisierung der Aufgabengebiete, eine Entlastung der Polizeiinspektionen, die Professionalisierung der Ermittlungsarbeit sowie die stärkere Einbindung der Bevölkerung in die Präventionsarbeit“, hielt Scherscher fest. *Jürgen Belko*