Innenministerin Johanna Mikl-Leitner: „Die Bekämpfung der Internet-Kriminalität ist ein Schwerpunkt der kriminalpolizeilichen Arbeit.“

„Cyber Security – Cyber Crime“: Teilnehmerinnen und Teilnehmer des vom Kuratorium Sicheres Österreich organisierten Sicherheitskongresses 2011 in der Messe Wien.

Schwachstelle Mensch

„Cyber Security – Cyber Crime“ war das Thema des Sicherheitskongresses 2011 des Kuratoriums Sicheres Österreich (KSÖ) am 31. Mai 2011 in der Messe Wien. In Fachvorträgen und drei Panels informierten sich die rund 400 Teilnehmer über Sicherheit und Kriminalität im Internet.

Ziel des ersten Sicherheitskongresses des KSÖ war es, die Zusammenarbeit von Behörden, Wissenschaft und Wirtschaft bei der Bekämpfung der Internet-Kriminalität auszubauen, Betroffene für das Thema sicherer Umgang mit dem Internet zu sensibilisieren sowie sich auszutauschen und zu informieren.

„Die Informations- und Netzwerktechnologien haben sich weltweit rasant weiterentwickelt. Und damit einhergehend ist nicht nur die Anzahl der Internet-User, sondern auch die der strafbaren Handlungen im Netz gestiegen“, sagte Innenministerin Mag. Johanna Mikl-Leitner in ihrer Eröffnungsrede beim Sicherheitskongress und betonte die Notwendigkeit der neuen Cyber-Sicherheitsstrategie des Innenministeriums. „Die Bekämpfung der Internet-Kriminalität nimmt einen Schwerpunkt unserer kriminalpolizeilichen Arbeit ein.“ Die Ministerin verwies auf das Cyber-Crime-Competence-Center (C4), das unter der Federführung des Bundeskriminalamts mit dem BVT und dem BAK aufgebaut wird.

Europol-Assistant-Director Mag. Christian Jechoutek berichtete über aktuelle Bedrohungen im Zusammenhang mit dem Internet und verwies auf die Trends im virtuellen Bereich wie Quantum Computing, Remote Working, Cloud Computing, virtuelle Welten in Unternehmen, virtuelle Bezahlungssysteme, Diebstahl virtuellen Eigentums, RFID-Smart-Objects, „Cocktail-Identitäten“, Lifelogging und Transhumanismus. Notwendig für eine wirksame Bekämpfung von Cyber-Crime sei Prävention, das *Internet Crime Reporting Online System (ICROS),* Deep-Web-Tools, die Zusammenarbeit mit „ethischen Hackergruppen, Datenmobilität, die strategische und operative Auswertung sowie Gesetzesanpassungen.

Jechoutek berichtete von einem internationalen Kinderschänder-Fall, bei dessen Aufklärung Europol koordiniert und eine Schlüsselrolle eingenommen habe. 2008 entdeckten verdeckte Ermittler ein Online-Forum, in dem sich User über ihre sexuellen Vorlieben für Knaben austauschten. 2009 wurde von britischen Ermittlern der Betreiber der Website in den Niederlanden aufgespürt; im Jänner 2010 beschlagnahmte die niederländische Polizei den Server und gab ihn an Europol zur Auswertung weiter. Die Daten konnten von den Europol-Experten wiederhergestellt werden. Die Auswertungsberichte im Rahmen der „Operation Rescue“ wurden weltweit an die Strafverfolgungsbehörden verteilt. Insgesamt wurden in 13 Staaten 670 Verdächtige ausgeforscht und 184 von ihnen festgenommen. 230 Opfer konnten identifiziert werden. Der Fall habe auch gezeigt, dass eine Harmonisierung der Strafgesetze in diesem Bereich notwendig sei, betonte Jechoutek.

Über Trends und Herausforderungen referierte General Franz Lang. Der Direktor des Bundeskriminalamts wies auf die gewaltige Veränderung im Kriminalitätsgeschehen in den letzten Jahrzehnten hin. Der Schaden durch die Internet-Kriminalität betrage laut Europol etwa 750 Milliarden Euro. Die Profite der Internetkriminellen seien inzwischen höher als im Drogenhandel. In Österreich habe es im Jahr 2001 685 Cyber-Crime-Anzeigen gegeben, im vergangenen Jahr seien es 4.450 gewesen.

Ethische Bildung. A. o. Univ.-Prof. DDr. Christian Stadler wies in seinem Referat „Virtuelle Sicherheit – zwischen Legalität und Legitimität“ auf die Bedeutung von „ethischer Bildung und republikanischer Demokratie“ hin. Cyber-Crime sei seinem rechtsethisch-praktischen Wesen nach „nur“ eine neue technologische Spielart des zeitlosen kriminellen Handels. Neben phänomenzentrierten Gegenmaßnahmen wie Ausbildung von technischer Netzwerkkompetenz der Bürgerinnen und Bürger sowie die Installation von digitalen Netzwerkkontrollen bei Providern bedürfe es der prinzipiellen „Immuni-

FOTOS: KSÖ

KSÖ-Sicherheitskongress 2011: KSÖ-Präsident Erwin Hameseder, BK-Direktor Franz Lang, Christian Jechoutek (Europol).

sierung“ der Bürgerschaft durch ethische Bildung und republikanische Demokratie. Sonst werde der liberale Rechtsstaat „letztlich jenen Werten und Haltungen untreu, denen er sich existenziell immer schon verdankt – und das ist die wahre Bedrohung jenseits von bloß virtueller Sicherheit“, warnte Stadler.

In drei Panels beschäftigten sich Experten mit den Themen „Social Networks“, „Cyber Crime“ und „Sicherheitsfalle mobile Endgeräte“.

Panel „Social Networks“. Weltweit nutzen etwa 580 Millionen User „Facebook“ – unter ihnen 2,5 Millionen Österreicherinnen und Österreicher. „Social Media“ haben in den letzten Jahren zu einer Umkehrung der Mediennutzungsgewohnheiten geführt: 80 Prozent der Nachrichten werden heute aus dem Internet, dem Teletext oder Social-Media-Plattformen bezogen – zu Lasten der klassischen Nachrichtenmedien. Allerdings ist bei sozialen Netzwerken eine gesunde Skepsis nötig. Die Polizei ist zunehmend mit Fällen wie Mobbing via Facebook konfrontiert. Die Diffamierung eines unschuldigen Österreichers als Kinderschänder auf Facebook ist ein Beispiel dafür, wie der Ruf eines Unschuldigen willkürlich langfristig ruiniert werden kann. Übergriffe via Social Media werden oft als Kavaliersdelikte abgetan. Das Bundeskriminalamt hat in diesem Bereich eine Koordinationsfunktion übernommen, um derartigen Fällen künftig verstärkt nachzugehen.

Die Teilnehmerinnen und Teilnehmer der Podiumsdiskussion sprachen sich für die verantwortungsvolle Nutzung des Internets aus, mahnten jedoch ein, speziell der jüngeren Generation bei der sicheren Nutzung des Internets behilflich zu sein.

Panel „Cyber Crime“. Internetkriminalität ist in Österreich weit verbreitet. Das ergab eine Studie des Kuratoriums für Verkehrssicherheit (KfV), die im Panel II „Cyber Crime“ vorgestellt wurde. Für die Studie „Österreich als Opfer von Cyberkriminalität“ wurden 500 Personen ab 14 Jahren telefonisch befragt. Jeder zehnte Befragte berichtete über negative Erfahrungen beim Online-Shopping. Entweder wurde eine bestellte und bezahlte Ware nicht geliefert oder es kam die falsche Ware an. Fünf Prozent der Online-Banking-User hatten Erfahrungen mit Phishing gemacht. 48 Prozent der Befragten hatten negative Erfahrungen mit Computerviren; zwölf Prozent mit angeblichen Gratis-Downloads, die sich als kostenpflichtig herausgestellt hatten.

Drei Prozent gaben an, Fotos oder Videos von gewaltdarstellendem Material erhalten oder selbst weitergeleitet zu haben; bei zwei Prozent war es links- oder rechtsradikales, terroristisches oder fremdenfeindliches Material. 68 Prozent der Befragten gaben an, private Angaben im Internet zu machen (Frauen: 74 %, Männer: 63 %). Viele von ihnen veröffentlichen in sozialen Netzen neben ihren Namen auch ihr Foto (75 %) und das Alter (72 %). 18 Prozent gaben die Wohnadresse und 12 Prozent die Mobiltelefonnummer bekannt. Ein Fünftel der Befragten war mit eigenen Fotos und Videos konfrontiert, die andere in ein soziales Netz gestellt hatten. Drei Viertel der Befragten wurden von fremden Personen im Internet kontaktiert, jeder Siebente wurde nach weiteren Angaben gefragt wie Wohnungsadresse und Telefonnummer. Zwei Drittel der Befragten waren der Auffassung, dass nicht ausreichend über die sichere und richtige Nutzung des Internets in der Schule oder auf dem Arbeitsplatz aufgeklärt wird. Vier Fünftel erachten eine intensivere Aufklärungsarbeit bei Kindern und Jugendlichen als sehr sinnvoll.

Panel „Sicherheitsfalle mobile Endgeräte“. Im Panel III wiesen die Experten vor allem auf die Unsicherheit bzw. den geringen Schutz von mobilen Endgeräten hin – wie Handys, Blackberry, Smartphones und Laptops. Zudem gebe es bei der Nutzung der Geräte erhebliche Spannungen zwischen den Chancen und Risiken einerseits sowie zwischen der Benutzerfreundlichkeit und Sicherheit andererseits.

Einig waren sich die Diskussionsteilnehmer, dass die schwächste Stelle bei der Nutzung mobiler Endgeräte der Mensch ist – der Nutzer, dessen Unwissenheit zu hohen Risiken führen kann. Es könne aber nicht sein, dass die alleinige Verantwortung dem Nutzer aufgebürdet werde. In diesem Zusammenhang wurde kritisiert, dass sowohl Wirtschaft, Forschung als auch Verwaltung ihre Hausaufgaben nicht gemacht hätten.

Als Lösungsansätze zur Hebung der Sicherheit mobiler Endgeräte wurde vorgeschlagen:

- diversifizierte Berechtigungsprofile für mobile Endgeräte;
- Bewusstseinsbildung von Management und Mitarbeitern;
- stärkere Zusammenarbeit von Verwaltung, Wirtschaft und Wissenschaft.

M. L./W. R./ W. S.

Fotos: KSÖ