IT-KRIMINALITÄT

Niemandsland für Kriminelle

Das Strafrecht hält nicht mehr Schritt mit der Entwicklung der Informationstechnik. Experten überlegen Bekämpfungsstrategien.

Das Internet als eine Art Niemandsland für Kriminelle ist technisch kaum in den Griff zu bekommen, legistisch schwer zu kontrollieren. "Wir brauchen neue Strukturen – effizient, reaktions- und anpassungsfähig an den Zeitwandel der Informationstechnologie", sagte Innenminister Dr. Ernst Strasser anlässlich der Tagung "Cybercrime" am 14. Mai 2001 in Wien. Im derzeit entstehenden Bundeskriminalamt (BKA) will Strasser eine Stelle einrichten, die diesen Anforderungen entspricht und über ein Frühwarnsystem verfügt.

An der Tagung nahmen 40 Experten aus Exekutive und IT-Wirtschaft (Informationstechnik) teil. "Die Konferenz soll eine Auftaktveranstaltung sein für eine weit verzweigte Zusammenarbeit zwischen Exekutive und Internet-Unternehmen, mit internationalen Auswirkungen", erläuterte Dr. Herwig Haidinger, Leiter der Gruppe Kriminalpolizei im Innenministerium. Im November soll eine hochrangige Expertenkonferenz mit dem Thema befasst werden; die Ergebnisse der Tagung am 14. Mai bilden dafür die Grundlage. Die Experten forderten u.a. eine Anpassung des Strafrechts und Erleichterungen für die Ermittlungsarbeit der Exekutive. Im Wunschprogramm der Meldestelle gegen Kinderpornografie im Internet steht an erster Stelle die Möglichkeit, Scheingeschäfte mit Verdächtigen eingehen zu können. Die Beamten der Meldestelle könnten dadurch rascher gegen Kinderpornohändler vorgehen und sie hätten stichhaltigere Beweise.

Die Zahl der Hinweise an die Meldestelle stieg zwischen 1999 und 2000 von 500 auf 1.706, zwischen Jänner und Mitte Juni 2001 erreichten die Meldestelle 1.250 Hinweise, 27 davon mit Bezug nach Österreich. "Etwa 95 Prozent der Kinderpornodateien liegen auf amerikanischen Servern", sagte Mag. Rudolf Groß, Leiter der Meldestelle. "Hergestellt werden sie großteils in Russland und Asien." Österreich sei hauptsächlich ein Konsumentenland. Groß forderte eine internationale Anpassung der Gesetze. Selbst innerhalb der EU gebe es Schlupflöcher für Kinderpornohändler: Der Besitz von Kinderpornografie ist in Griechenland nicht strafbar; das Schutzalter für Kinder liegt zwischen 13 (Spanien) und 17 Jahren (Irland), in Österreich bei 14; als Kinderpornografie gelten in Österreich und Deutschland pornografische Aufnahmen mit Kindern unter 14 Jahren, in allen anderen EU-Ländern liegt die Altersgrenze höher, meist bei 18.

Unterschiedlich hoch sind auch die Strafen: Die Verbreitung von Kinderpornografie wird in Österreich mit Haft bis zu zwei Jahren bedroht, in Irland bis zu 14 Jahren. Die Herstellung ist in Dänemark mit höchstens sechs Monaten Haft bedroht, in Österreich mit bis zu zwei Jahren, in Italien zwischen sechs und zwölf Jahren, in Irland bis zu 14 Jahren; die Höchststrafen für den Besitz von kinderpornografischem Material gibt es in Deutschland, Irland und Luxemburg (bis zu fünf Jahre Haft). "Internet-Kriminelle sind gegenüber der Exekutive im Vorteil", betonte Bernhard Otupal von der Zentralstelle im Innenministerium zur Bekämpfung der Computer- und Netzkriminalität. "Die E-Mail eines Kriminellen braucht zwei Minuten von Wien nach New York, der Rechtsweg zwischen Österreich und den USA benötigt zwischen acht und zwölf Monaten." Die Täter arbeiteten global, die Exekutive

großteils national; Kriminelle hielten sich streng an Schweigegelübde, die Exekutive sei Informationspflichten unterworfen; organisierte Banden bedienten sich arbeitsteilig verschiedener Experten mit hohem Detailwissen, Exekutivbeamte sollten alles wissen; aus Internet-Cafés sei es möglich, völlig anonym SMS auf Handys zu versenden.

Die "Macht der Maus"

Ein strafrechtliches Problem in Bezug auf SMS-Straftaten sieht Staatsanwältin Dr. Risa Schuhmeister-Schmatral: "Es ist nicht zu erkennen, was im Täter vorgeht. Das Strafrecht ist aber darauf ausgelegt, neben der äußeren Tatseite – dem objektiven Geschehen – die innere Tatseite zu beurteilen – was im Täter vorgegangen ist." Im Fall einer gefährlichen Drohung sei es beispielsweise für die Beurteilung der Ernsthaftigkeit wichtig zu wissen, mit welchem Tonfall die Drohung ausgesprochen wurde – bei einer Drohung mittels SMS liege bloß ein schriftlicher Ausspruch vor.

Generell liege dem österreichischen Strafrecht eine Denkphilosophie zugrunde, die mit den Entwicklungen in der Informationstechnologie nicht Schritt halte. "Das Strafgesetz ist darauf aufgebaut, zwischenmenschliche Konflikte zu regeln", erläuterte Schuhmeister-Schmatral. "Im Internet treffen sich anonyme Daten." Auch der Schadensbegriff des derzeitigen Strafrechts ist schwer umlegbar auf den Schaden, der beispielsweise durch Hacking entstehe oder durch ein Bombardement mit E-Mails. Nach Ansicht der Staatsanwältin reichen die derzeitigen Schadensgrenzen für erhöhte Strafrahmen nicht aus. "Es kann nicht sein, dass für einen Milliardenschaden durch Hacking dieselbe Strafe droht wie für einen Betrug mit einem Schaden von 500.000 Schilling."

Schuhmeister-Schmatral forderte IT-Ausbildungsmöglichkeiten für Richter und Staatsanwälte und Spezialgerichten. "IT-Kriminalität ist gefährlicher als organisierte Kriminalität", betonte die Juristin. "Mit der Macht der Maus kann innerhalb kurzer Zeit mehr Schaden angerichtet werden als wir uns vorstellen können. Wir haben die Anonymität noch nicht im Griff, hinken zeitlich hinterher und stehen Experten gegenüber, die monatelang am Computer herumspielen und Wege durch das Netz finden, die schwer nachvollziehbar sind."

Gerhard Brenner

IT-SICHERHEIT

Forderungskatalog

Für die hochrangige Folgekonferenz im November 2001 wurde am 14. Mai ein Forderungskatalog erstellt:

- Das Telekommunikationsgesetz sollte Internet-Unternehmen (Provider) verpflichten, Einwähldaten (Logfiles) sechs Monate gespeichert zu lassen.
- Das Sicherheitspolizeigesetz sollte die Provider verpflichten, der Exekutive Kundendaten innerhalb festgelegter Zeit weiterzugeben; der Exekutive sollte ein Durchsetzungsmechanismus zur Verfügung stehen.
- EU-weite Anpassung der Gesetze: Kinderpornografie (Schutzaltersgrenzen, Strafrahmen für Herstellung, Handel und Besitz), rechtsradikale
- Inhalte unter Strafe stellen, ebenso Hacking (in Österreich nicht strafbar, wenn keine Schädigungsabsicht nachweisbar ist).

- Selbstverpflichtung der Internet-Provider, ihre Server frei zu halten von verbotenen Inhalten; Strafdrohung für "schwarze Schafe" unter den Providern.
- Scheinkaufmöglichkeit für Internet-Ermittler.
- Informationspflicht für Internet-
- Provider ihren Kunden gegenüber, wie sie sich vor Internetkriminalität schützen können; Schaffung eines Problembewusstseins.
- Schaffung einer nationalen Plattform gegen Internetkriminalität, an der alle relevanten Institutionen teilnehmen (etwa Exekutive, Justiz, Internet-
- Unternehmen, private Organisationen).
- Gemeinsame Ausbildung von Exekutive und Justiz durch Internet-Unternehmen, um Gefährdungspotenziale kennen zu lernen.