COMPUTER- UND NETZWERKKRIMINALITÄT

Hohe Dunkelziffer

Die Spezialisten des Bundeskriminalamtes bearbeiteten im vergangenen Jahr 3.335 Anzeigen wegen Computerkriminalität.

Das Jahr 2003 war das "Jahr der Würmer und Viren". Dennoch hatten die Spezialisten des Bundeskriminalamts zur Bekämpfung der Computer- und Netzwerkkriminalität um 30 Prozent weniger Anzeigen zu bearbeiten als im Jahr davor. Insgesamt gab es im Jahr 2003 in Österreich 3.335 Anzeigen wegen Computerdelikte; 2002 waren es 4.785. Die Aufklärungsquote verringerte sich um 18,5 Prozent. 689 der 3.335 Anzeigen im vergangenen Jahr wurden wegen gefährlicher Drohung erstattet, 343 wegen Betrug und 170 wegen Kinderpornografie.

"Wer das Internet benutzt, muss damit rechnen, dass er sich die Kriminalität in sein Zimmer holen kann. Er kann aber auch weltweit kriminell tätig werden", sagte der Direktor des Bundeskriminalamts, Dr. Herwig Haidinger bei einer Pressekonferenz am 13. April in Wien. Die Anonymität spiele bei der Internetkriminalität eine große Rolle.

IT-Sicherheitspolitik

"Man muss davon ausgehen, dass die Dunkelziffer hoch ist", berichtete Klaus Mits, Leiter der Abteilung "Kriminalpolizeiliche Assistenzdienste" im Bundeskriminalamt. Unternehmen sollten für sich eine IT-Sicherheitspolitik formulieren, jeder Internet-User sollte sich mit Viren-Scanner und Firewall ausrüsten. Betrugsdelikte machen einen großen Teil der Computerkriminalität aus. "Die Betrugshandlungen sind zumeist recht einfach. Zum Beispiel liefert der Versteigerer bei Internetauktionen die Ware nicht oder derjenige, der etwas ersteigert hat, zahlt nicht", erläuterte DI Markus Blank vom Bundeskriminalamt.

Checkliste zur Beweissicherung

Das Bundeskriminalamt präsentierte eine von den österreichischen Fachleuten entwickelte Check-Liste für die Sicherung von Beweismitteln im Zusammenhang mit der Computer- und Netzwerkkriminalität. Das Projekt "Seizure of E-Evidence" (Elektronische Beweissicherung) basiert auf einer österreichischen Checkliste. Sie wurde im Rahmen eines von der EU geförderten Projekts gemeinsam mit deutschen, britischen und schwedischen Stellen sowie Europol und Interpol zu einem Handbuch für Europas Exekutivbeamte entwickelt. Kooperationspartner war das Zentrum für sichere Informationstechnologie (A-SIT), einem Unternehmen des Bundes, der Österreichischen Nationalbank und der Technischen Universität Graz.

"Jeder hinterlässt im Internet Spuren. Die müssen gefunden, analysiert und ausgewertet werden. Wir wollen mit dem Projekt jene Beamten unterstützen, die als Erste am Tatort sind", sagte Abteilungsleiter Klaus Mits "So kann zum Beispiel schon das einfache Abfotografieren der Steckplätze an der Hinterseite des Computers eines Verdächtigen zu einem hieb- und stichfesten Beweismaterial vor Gericht werden. Das Abmontieren hingegen kann Beweismaterial vernichten."

Öffentliche Sicherheit, Ausgabe 05-06/2004

Neue Tatbestände

Österreich hat im legistischen Bereich mit dem Strafrechtsänderungsgesetz 2002 auf die neue Bedrohung im Bereich der IT-Medien reagiert. Mit dieser Gesetzesnovelle wurde die "Convention on Cybercrime" des Europarats umgesetzt. Ziel der Konvention ist die Definition von Straftatbeständen im Zusammenhang mit dem Gebrauch der neuen Technologien, die Festlegung von Methoden für kriminalpolizeiliche Ermittlungen und die Strafverfolgung sowie die Festlegung internationaler Kommunikationswege. Mit dem Strafrechtsänderungsgesetz 2002 wurden im Zusammenhang mit Computer- und Netzwerkkriminalität folgende Tatbestände im Strafgesetzbuch (StGB) geschaffen bzw. geändert:

- § 126a (Datenbeschädigung) und 148a (betrügerischer Datenverarbeitungsmissbrauch) wurden angepasst;
- Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB);
- Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB);
- Missbräuchliches Abfangen von Daten (§ 119a StGB);
- Missbrauch von Tonaufnahme- oder Abhörgeräten (§ 120 Abs 2a StGB);
- Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB);
- Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB);
- Datenfälschung (§ 225a StGB).

BUNDESKRIMINALAMT

"Cybercops"

Das Büro 5.2 im Bundeskriminalamt ist zuständig für die Bekämpfung der Computerkriminalität und ist Ansprechpartner für alle Dienststellen in Österreich.

Für die Bekämpfung der Computer- und Netzwerkkriminalität ist in der Abteilung 5 des BK das Büro 5.2 zuständig; es besteht aus vier Referaten:

- Internationale Beziehungen (Ref. 5.2.1)
- Netzwerkkriminalität (Ref. 5.2.2)
- Computerkriminalität (Ref. 5.2.3)
- ADA-Applikation (Ref. 5.2.4)

Die Mitarbeiter des Büros 5.2 ermitteln nicht nur bei Fällen von Computer- und Netzwerkkriminalität, sondern sind auch Ansprechstelle für nationale und internationale Dienststellen; sie unterstützen Organisationseinheiten des Innenministeriums auf technischem Gebiet, beraten Dienststellen in der Zentralstelle und sind in nationalen und internationalen Gremien vertreten. Nationale Kooperationen gibt es mit der Institution A-SIT, dem Forschungszentrum Seibersdorf, den österreichischen Internet-Service-Providern

(ISPA), der Universität Wien, der TU Graz, dem Bundesrechenzentrum und der Wirtschaft. International kooperieren die Ermittler mit Europol und Interpol, der internationalen Organisation für Computerbeweissicherung (IOCE) und dem "European Network of Forensic Science Institutes" (ENFSI). Geplant sind Ausbildungsprogramme mit dem FBI sowie mit Deutschland und der Schweiz. Das Büro ist "National Central Reference Point" (NCRP) im Bereich Computer- und Netzwerkkriminalität.

Datensicherung

Zu den wichtigsten Aufgaben zählen die einheitliche und forensisch korrekte Sicherung von Beweisen im Zusammenhang mit der IT-Kriminalität, vor allem die Datensicherung. Neben dem Büro II/BK/5.2 bestehen regionale Datensicherungseinheiten bei den Kriminalabteilungen der Landesgendarmeriekommanden sowie in den Bundespolizeidirektionen Wien und Salzburg. In den anderen Bundespolizeidirektionen gibt es Sachbearbeiter für Datensicherung.

Kontakt:

Bundeskriminalamt,
Büro 5.2 (Computer- und Netzwerkkriminalität),
1090 Wien,
Josef-Holaubek-Platz 1,
E-Mail: ccu@bmi.gv.at