Präsentation der Cyber-Sicherheitsstrategie: Leopold Löschl (BK), Innenministerin Johanna Mikl-Leitner, Christian Herndler (BVT).

Strategie gegen Cyber-Crime

Die Cyber-Sicherheitsstrategie des Innenministeriums ist ein Schwerpunkt der Kriminalitätsbekämpfung. Kern der neuen Strategie ist die Einrichtung des Cyber-Crime-Compentence-Centers (C4).

Mehr als ein Jahr ermittelten österreichische und bayrische Kriminalisten, dann erfolgte der Zugriff: In Deutschland durchsuchten mehr als 170 Polizeibeamte insgesamt 29 Objekte und nahmen acht Verdächtige fest, darunter den Drahtzieher der Bande. Ein weiterer Verdächtiger wurde von Ermittlern des Bundeskriminalamts am 10. Mai 2011 in Niederösterreich festgenommen.

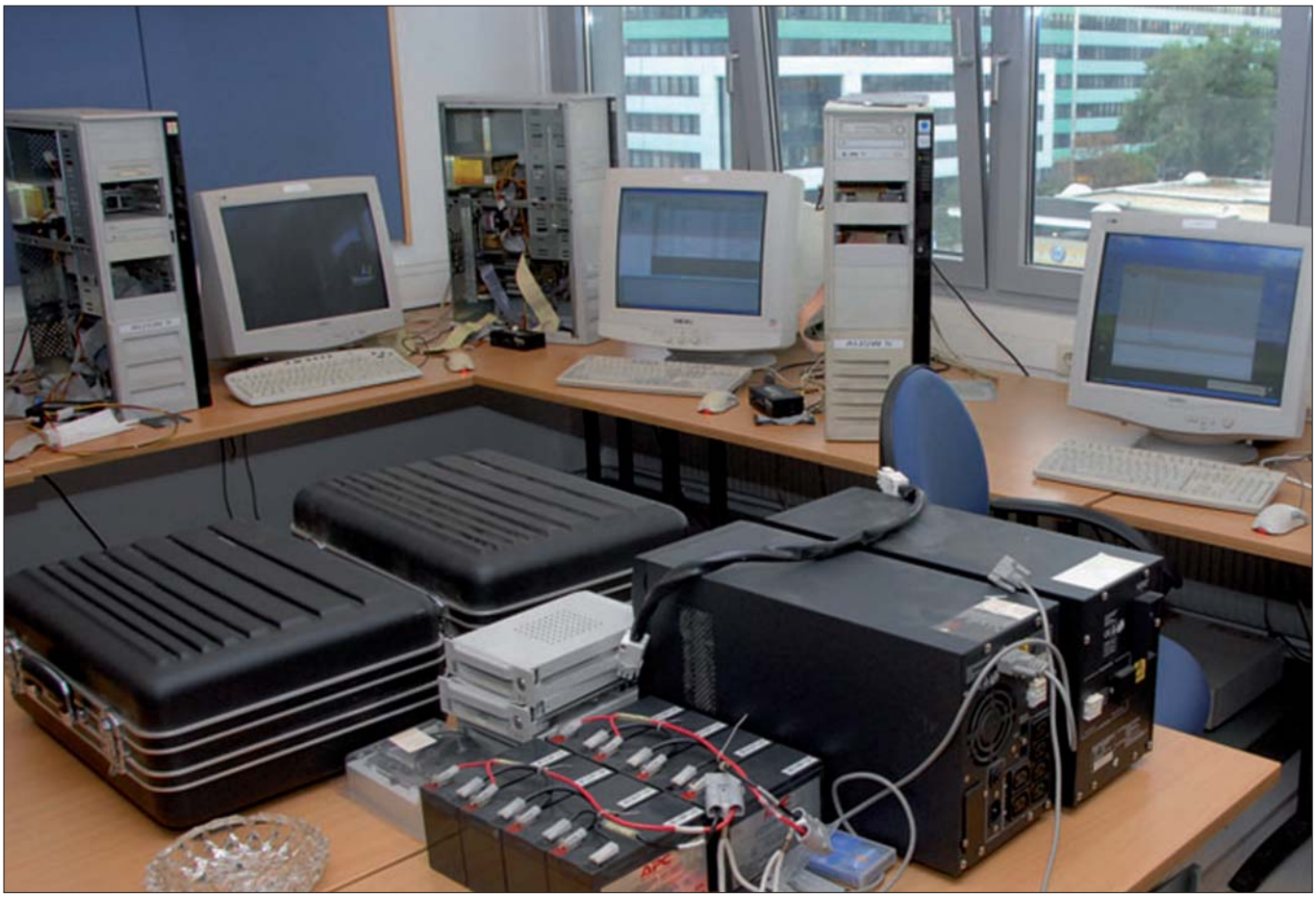
Die Bandenmitglieder hatten insgesamt über 800 professionell aufgemachte „Webshops" eingerichtet, in denen sie Elektronikgeräte, Werkzeug und andere Waren billig anboten. Die gefakten Webshops waren nur wenige Wochen online, dann wurden sie vom Netz genommen und es wurden neue Seiten eingerichtet. Rund 100.000 Kunden im deutschsprachigen Raum bestellten über diese Webshops Waren und überwiesen die Kaufsumme; die bestellten Waren wurden aber nicht geliefert. Der Gesamtschaden beläuft sich auf einen zweistelligen Millionen-Euro-Betrag. Die Überweisung der Geldbeträge der Kunden wurde verschleiert, indem Mitglieder der kriminellen Organisation meist leichtgläubige Menschen als „Finanzagenten" anheuerten, die ihre Bankkonten zur Verfügung stellten, auf die das Geld überwiesen wurde. Die Summen wurden von den „Finanzagenten" nach Abzug einer Gebühr mit Geldboten oder per anonymer Blitzüberweisung an die Bande weitergeleitet. Der festgenommene Niederösterreicher war in der kriminellen Gruppe unter anderem für die Bereitstellung der Infrastruktur verantwortlich.

Dieser Betrugsfall zeigt die internationale Dimension von Internet-Kriminalität auf. Die Täter agieren von verschiedenen Ländern aus, der Server kann sich überall befinden, und die Spuren werden über die Grenzen hinweg verschleiert. Erschwert wird die Strafverfolgung durch die unterschiedliche Gesetzgebung in den betroffenen Staaten.

„Werkzeug Internet". Strafbare Handlungen mit dem „Werkzeug Internet" sind in den letzten Jahren zahlreicher und komplexer geworden. Die Anonymität des Internets und die Verwendung hoch entwickelter Softwareprogramme erschweren die Ermittlungen der Kriminalisten. Häufig kann bei Delikten im Internet weder auf die Identität noch auf die Hintergründe des Angreifers geschlossen werden, da die Abwehr- und Rückverfolgungsmöglichkeiten teilweise begrenzt sind.

„Die Internetkriminalität kann national nur begrenzt bekämpft werden. Ihre Bekämpfung ist eine internationa-

FOTO: EGON WEISSHEIMER



Forensische Beweissicherung im Bundeskriminalamt: Sichergestellte Datenträger; Auswertegeräte.

FOTO: EGON WEISSHEIMER

le Herausforderung. Eine enge länderübergreifende Zusammenarbeit nimmt daher einen zentralen Stellenwert ein", sagt Mag. Rudolf Unterköfler, Leiter der Abteilung 7 (Wirtschaftskriminalität) im Bundeskriminalamt. „In vielen Fällen der Internet-Kriminalität sind die Täter organisiert und international vernetzt." Von der Internetkriminalität seien nahezu alle Deliktsbereiche betroffen – vom Kreditkartenbetrug über Telefonangriffe bis hin zur Kinderpornografie. Die konventionelle Kriminalität setzt sich im Internet fort.

Die Täter verwischen ihre Spuren im World Wide Web mittels Verschlüsselungssoftware und setzen zur Verschleierung der Geldströme oft mehrere „Finanzagenten" hintereinander ein.

4.450 Fälle von IT-Kriminalität wurden im vergangenen Jahr in Österreich registriert; 2005 waren es 2.453 Delikte. Im ersten Quartal 2011 wurden bereits 1.129 Delikte angezeigt. Häufigste Deliktsarten in diesem Bereich waren Betrugsfälle durch Internetauktionen (1.874 angezeigte Fälle im Jahr 2010) und durch Missbrauch des Internets (1.490). Die Zahl der Anzeigen wegen Hackings stieg von 29 (2009) auf 142 (2010) an. In den ersten drei Monaten dieses Jahres wurden bereits 56 Hacking-Fälle gemeldet.

Der durch Cyberkriminalität verursachte jährliche Schaden beträgt nach Schätzungen von Europol 750 Milliarden Euro. Jeden Tag sind mehr als 150.000 Viren und andere Files mit Schadware im Umlauf.

Cyber-Sicherheitsstrategie. Die Informations- und Netzwerktechnologien haben sich rasant entwickelt; parallel dazu ist der Zahl der Internetuser gestiegen. Fast vier Fünftel der Österreicher über 14 Jahre nutzen das Internet zuhause und bei den Neun- bis Sechzehnjährigen sind es laut einer Studie des Forschungsverbunds EU Kids Online vom Jänner 2011 bereits 98 Prozent; 48 Prozent von ihnen haben einen Internet-Anschluss in ihrem Zimmer. Gleichzeitig ist die Zahl der Straftaten gestiegen, bei denen Informationstechnologien und Kommunikationsnetze genutzt werden. Viele Geschädigte erstatten keine Anzeige, weil die Schadensumme gering ist, weil sie sich schämen, auf Betrüger hereingefallen zu sein, oder weil sie der Meinung sind, dass die Täter ohnedies nicht ausgeforscht werden können.

Für die Sicherheitsbehörden bedeutet die Bekämpfung der IT-Kriminalität eine große Herausforderung. Innenministerin Mag. Johanna Mikl-Leitner präsentierte am 18. Mai 2011 die neue Strategie gegen die Internet-Kriminalität. „Die Gewährleistung von Sicherheit im Internet erfordert ein hohes Engagement des Staates im Innern und in enger internationaler Zusammenarbeit", sagte die Innenministerin. „Eine Cyber-Sicherheitsstrategie kann nur dann erfolgreich sein, wenn alle betroffenen Akteure gemeinsam ihre jeweilige Aufgabe wahrnehmen. Die Cyber-Strategie des Innenministeriums ist daher so aufgebaut, dass zukünftig in der gesamten Polizeistruktur die Bekämpfung der Internetkriminalität einen Schwerpunkt einnimmt."

Die neue Strategie sieht die Bekämpfung von Cyber-Crime auf drei Ebenen vor:

• Auf lokaler und regionaler Ebene sind die Polizistinnen und Polizisten in den rund 900 Polizeiinspektionen und in den 110 Bezirks- und Stadtpolizei-

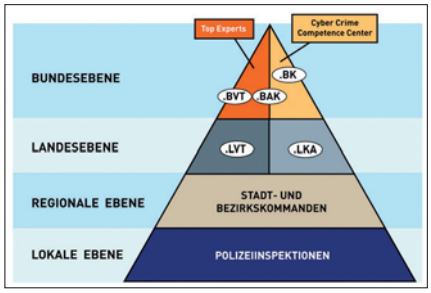
kommanden eingebunden: Heuer werden 300 Präventionsbeamtinnen und -beamte für die Verhinderung von Internetkriminalität ausgebildet.

• In den neun Landeskriminalämten sind Expertinnen und Experten bei technischen Ermittlungs- und Beweissicherungsmaßnahmen tätig. Darüber hinaus sind die neun Landesämter für Verfassungsschutz und Terrorismusbekämpfung (LVT) bei Ermittlungen und Recherchen mit Cyber-Crime konfrontiert, etwa bei NS-Wiederbetätigung.

• Auf oberster Ebene wird im Bundeskriminalamt als zentrale Koordinierungs- und Meldestelle das Cyber-Crime-Competence-Center (C4) eingerichtet. Hier arbeiten neben Fachleuten des Bundeskriminalamts auch Spezialisten des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) und des Bundesamts zur Korruptionsprävention und Korruptionsbekämpfung (BAK).

Internationale Zusammenarbeit. „Gerade im Bereich der IT-Kriminalität ist die nationale und internationale Zusammenarbeit entscheidend", erläutert Mag. Leopold Löschl, Leiter des Büros 5.2 (Computer- und Netzwerkkriminalität) im Bundeskriminalamt. „Das Competence-Center versteht sich großteils als High-Level-Supportstelle, die national und international koordiniert. Durch die Zusammenarbeit der Spezialisten des Bundeskriminalamts, des BVT und des BAK werden auch Synergieeffekte genutzt."

Mitarbeiter des Cyber-Crime-Competence-Centers im Innenministerium.



Aufbau der Cyber-Sicherheitsstrategie.

Sichergestellte Festplatten: Riesige Datenmengen.

„Die Entwicklung im Bereich Netzwerktechnologien läuft rasant – zum Beispiel im Bereich der mobilen Endgeräte, die als täglicher Begleiter immer mehr zur digitalen Signatur werden", betont Löschl. Im Kompetenzzentrum kommen auch neue Arbeitsmethoden zum Einsatz, um rechtzeitig auf neue Entwicklungen und Gefahren reagieren zu können. Die zunehmende Verwendung von Verschlüsselungssoftware und Anonymisierungsdiensten erfordere zudem den Ausbau des forensischen Fachwissens, erläutert der Büroleiter.

„Wir werden auch die Kooperation mit der Wissenschaft verstärken", sagt Löschl. „Denn das Know-how von externen Fachleuten ist für die wirksame Bekämpfung der Internetkriminalität ein entscheidender Faktor." Derzeit läuft ein Projekt mit der Fachhochschule St. Pölten. Ausgebaut wird die Zusammenarbeit mit der Wirtschaft: So wurden IT-Forensiker des Bundeskriminalamts, der Landeskriminalämter und des BVT bei IT-Unternehmen geschult. Diese Kooperation wird ausgebaut. Ausgebildet werden die Spezialisten auch im Ausland – etwa im Rahmen europäischer Projekte von Europol und OLAF.

Künftig soll das im C4 entwickelte Know-how an die regionalen Ermittler weitergegeben werden. Die zentrale Internetmeldestelle *against-cybercrime@bmi.gv.at* ist eine Ansprechstelle für Bürgerinnen und Bürger, die verdächtige Wahrnehmungen im Internet machen.

INTERNET-KRIMINALITÄT

Maßnahmen zur Prävention

• Vorsicht beim „Einkauf im Internet", wenn eine Vorauszahlung gefordert wird.

• Vertrauliche oder persönliche Daten sollten ausschließlich über verschlüsselte Seiten bekannt gegeben werden. Die Übertragung ist sicher, wenn die Internetadresse in der Browserleiste mit https:// beginnt.

• Virenschutz verwenden und regelmäßig Updates durchführen.

• Software (Betriebssystem und Browser) regelmäßig aktualisieren. Die Hersteller stellen in regelmäßigen Abständen kostenlose Updates zur Verfügung, mit denen Sicherheitslücken im System behoben werden.

• Eine Firewall schützt den PC im Internet vor gefährlichen Daten oder ungewollten Zugriffen. Firewalls sind im Handel und als (kostenlose) Freeware erhältlich.

• Vorsicht bei der Weitergabe der E-Mail-Adresse oder bei der Eintragung der Daten in Internetformulare. Man sollte immer davon ausgehen, dass die Daten missbräuchlich verwendet werden könnten.

• Keine vertraulichen Daten übermitteln, wenn man per E-Mail dazu aufgefordert wird. In solchen Fällen sollte die Seriosität der E-Mail überprüft werden – eventuell durch Rücksprache mit dem Absender. Bankangestellte fragen nie per E-Mail nach Zugangsdaten. Solche Anfragen kommen in der Regel von Betrügern.

• Keine Passwörter (PIN, TAN u. a.) auf dem PC speichern.

• Sichere Passwörter verwenden – das sind Passwörter mit acht oder mehr Stellen, die aus einer Kombination von Buchstaben, Sonderzeichen und Ziffern bestehen.

• Keine E-Mails öffnen, deren Herkunft man nicht kennt. Es könnten sich Viren, Würmer oder Trojaner darin verbergen.

• Datenbestand regelmäßig sichern; Sicherungskopien erstellen.

Internet-Meldestelle: against-cybercrime@bmi.gv.at

FOTOS: BMI, EGON WEISSHEIMER (2)