INTERNETKRIMINALITÄT

Terror aus dem Datennetz

Sie bekämpfen Kinderpornografie im Internet, jagen Hacker, warnen vor Viren und informieren über Sicherheit in Datennetzen. Die Spezialisten der Zentralstelle im Innenministerium zur Bekämpfung der Internetkriminalität zählen zu den besten Cyberpolizisten in Europa.

Spezialisten des Bundeskriminalamtes

"Er war bereits ein "Offizier" in der Internet-Untergrundorganisation. Doch der junge Mann wollte sich weiter nach oben arbeiten. Dafür musste er Erfolge nachweisen. Anfang dieses Jahres hackte er mehrere Webseiten und verschickte eine Abart des "Love-Letter-Virus" an über 500 Adressaten. Der Virus war programmiert, sämtliche Bild- und Tondateien auf den befallenen Rechnern zu zerstören und den Zugriff auf die Computer unmöglich zu machen. Betroffen waren Rechner mit Microsoft-Betriebssystemen. Eine geschädigte Salzburger Firma erstattete Anzeige bei der Gendarmerie. Die Beamten ersuchten die Kollegen von der Zentralstelle zur Bekämpfung der Computer- und Netzwerkkriminalität um Unterstützung. Innerhalb einer Woche gelang es den Spezialisten des Innenministeriums zur Bekämpfung der Computer- und Netzkriminalität (Abt. II/16-ITB), den "Cyber-Terroristen" auszuforschen – in enger Zusammenarbeit mit dem Zentrum für Sichere Informationstechnologie Austria (A-SIT). Über den Quellcode des Virus gelangten sie zum Täter – einem 23-jährigen Programmierer im Pongau. Der Salzburger hatte die E-Mails von zu Hause abgeschickt. Er gab an, Mitglied einer weltweiten Untergrundorganisation zu sein, die militärisch organisiert sei und "für ein freies, unkontrolliertes Internet" kämpfe.

Die Ermittler beschlagnahmten vernetzte Computer, Datenträger und Software zum Cracken von Passwörtern, zum Hacken von PCs und Servern und zur Herstellung gefährlicher Viren. Das Material war dem Täter von der Untergrundorganisation zur Verfügung gestellt worden. Die sichergestellten Computerdaten würden auf Papier ausgedruckt einen Stapel von mehr als 2.000 Metern Höhe erreichen. "Wir haben die Firmen und Institutionen verständigt, die wir auf der Mail-Liste des Täters fanden", sagte Bernhard Otupal von der EDV-Spezialeinheit des Innenministeriums. Das Ausmaß der Schäden ist noch nicht bekannt, die Ermittlungen dauern an.

Neuer "Love-Letter": Bei einem ähnlichen Fall im vergangenen Jahr wurde der Virus wegen eines Programmierfehlers nicht aktiv. Das deutsche Bundeskriminalamt verständigte damals das Innenministerium in Wien, dass aus Österreich ein gefährlicher Computervirus an Adressen in Deutschland versandt worden war. Die Ermittler der Spezialeinheit übernahmen den Fall. Als Täter wurde ein 28-jähriger Computertechniker aus Niederösterreich ausgeforscht, der eine Abart des "Love-Letter-Virus" an 50 E-Mail-Adressen verschickt hatte. Er benutzte als Absender die E-Mail-Adresse antivirus_gmbh@hotmail.com und verschickte den Virus unter dem heimtückischen Titel "Neue Antivirus-Liste". Hätte der Virus funktioniert,

wären sämtliche Datenbestände auf den befallenen Computern vernichtet worden. Die Ermittler untersuchten den Inhalt der E-Mail, der der Virus als Anhang angeschlossen war. Das führte sie zu dem Provider, über den der Täter seine E-Mails verschickt hatte. Der Programmierer wählte einen anonymen Gast-Zugang für das Internet. Dabei machte er einen Fehler. Durch die Auswertung des Accounts gelang es den Beamten, die elektronische Spur bis in das Arbeitszimmer des Hackers zurückzuverfolgen.

Hundert Virenangriffe

Bei der Hausdurchsuchung fanden sie Computer, umfangreiche Software und einschlägige Unterlagen über Hack- und Virenattacken. Die Ermittler wiesen dem Täter weitere hundert Virenangriffe nach. Aufgrund der umfangreichen Beweise legte er ein Geständnis ab.

Zentralstelle im Innenministerium

Das Datennetz bietet viele Möglichkeiten für das weltweite Verbrechen. Kriminelle können an allen Orten der Erde sitzen und per Mausklick Schäden überall in der Welt anrichten. Seit 1. August 1999 besteht im Bundesministerium für Inneres eine Zentralstelle zur Bekämpfung der Internetkriminalität: die Abteilung II/16-ITB, Informationstechnologie/Beweissicherung. In dieser Spezialeinheit arbeiten besonders ausgebildete Kriminalbeamte, die bei größeren oder grenzüberschreitenden Fällen zum Einsatz kommen. Zu ihren Hauptgebieten gehören Delikte, bei denen Computer Ziel einer strafbaren Handlung werden, zum Beispiel durch Hack- oder Virenangriffe; oder Delikte, bei denen Computer als Tatmittel eingesetzt werden wie etwa Betrug. Das Hacken von Webseiten ist in Österreich nur strafbar, wenn ein Tatbestand nach den Paragrafen 126a (Datenbeschädigung) oder 148a (Betrügerischer Datenverarbeitungsmissbrauch) StGB erfüllt wird. Die Ermittler werden aktiv, wenn sie von Exekutivdienststellen aus dem In- oder Ausland von einer Computerstraftat verständigt werden. Sie unterstützen die örtlich und sachlich zuständigen Ermittler oder Datensicherungsbeamten mit Fachwissen und Technik.

Interpol hat ein Frühwarnsystem eingerichtet, das ermöglicht, Warnungen und Informationen über Computerstraftaten schnell auszutauschen. Das geschieht über den National Central Reference Point on Information Technology. Wird eine IT-bezogene Straftat bekannt, kann diese Information in einer international lesbaren Form codiert und über das Internet an die nationalen und internationalen Sicherheitsbehörden verbreitet werden. Anlaufstelle in Österreich ist die Abteilung II/16-ITB. Sie leitet die Informationen an die Fachbeamten in den Bundesländern weiter. Die Abteilung vertritt Österreich in Belangen IT-Kriminalität im European Network of Forensic Science Institute on Computer Crime (ENFSI). In der ITB-Abteilung gibt es mehrere Untergruppen, zuständig für die Bereiche Beweissicherung, Netzwerkkriminalität, Verschlüsselungssysteme, Auswertung und Analyse. Die Beamten unterstützen die Fachabteilung bei der technischen Beweismittelsicherung und bereiten die sichergestellten Daten für eine Auswertung in lesbarer Form auf.

Die den Beamten zur Verfügung stehende Technik entspricht den internationalen Ansprüchen, auch den forensischen. Das Herzstück der Technik sind Imagingsysteme, Datensicherungssysteme, die es ermöglichen, Kopien der beschlagnahmten Daten zu machen, ohne sie zu verändern. Die gesicherten Daten werden mit verschiedenen Analyse- und Auswertungstools untersucht; die Befunde der zuständigen Fachabteilung übermittelt. Diese entscheidet, ob ein strafbarer Tatbestand vorliegt. Bei Delikten wie Kinderpornografie ermitteln die Internetfahnder selbst vor Ort und machen Hausdurchsuchungen.

Information und Prävention

Die Spezialisten der Abteilung II/16-ITB nehmen laufend an Kursen und internationalen Treffen teil, etwa im Bundeskriminalamt Wiesbaden und bei der US-Bundeskriminalpolizei FBI; sie arbeiten mit Universitäten zusammen und mit dem A-SIT. Ihr Wissen geben sie an die Datensicherungsbeamten weiter, die es in jeder Bundespolizeidirektion und jedem Landesgendarmeriekommando gibt – etwa 100 in ganz Österreich. Die Netzwerk-Polizisten wollen in Veranstaltungen das Bewusstsein für mögliche Verbrechen in oder mit dem Computer wecken. In Zukunft sollen regelmäßig Informationstage veranstaltet werden. Die Spezialisten beraten auch das Parlament in Fragen sicherer Informationstechnik. Bei der Vorbereitung des Signaturgesetzes zeigten sie kriminalpolizeiliche Bedenken auf, die bei der Entstehung des Gesetzes berücksichtigt wurden. Derzeit arbeiten sie an in einem interministeriellen Arbeitskreis mit, der sich mit der Entstehung einer europaweit gültigen Richtlinie für E-Commerce befasst. Gegen Hacker- oder Virenattacken aus dem Internet gibt es keinen hundertprozentigen Schutz. Die Spezialisten des Innenministeriums empfehlen Anti-Viren- und Firewall-Software aus dem Fachhandel, die durch regelmäßiges Updating auf den neuesten Stand gebracht werden soll.

Siegbert Lattacher

II/16-ITB

Cyber-Polizisten

Wer von einem Netzwerk- oder Computerdelikt Kenntnis erlangt, soll sich an die Datensicherungsbeamten der Polizei oder Gendarmerie wenden. Diese verständigen bei schwer wiegenden Fällen die Spezialisten der Abteilung II/16-ITB des Innenministeriums zur Bekämpfung der Computer- und Netzwerkkriminalität.

Information: ccu@bmi.gv.at

EUROPÄISCHE KOMMISSION

eEurope 2002

Im Dezember 1999 startete die Europäische Kommission die Initiative „eEurope“ zur Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informations-Infrastrukturen und Bekämpfung der Computerkriminalität. Im Juni 2000 billigte der Europäische Rat auf der Tagung in Feira den umfassenden „eEurope“-Aktionsplan und forderte seine Umsetzung bis 2002. Der Aktionsplan befasst sich schwerpunktmäßig mit der Sicherheit von Datennetzen und der Bekämpfung der Cyberkriminalität. In Ländern, in denen noch keine auf die Bekämpfung der Computerkriminalität spezialisierten Polizeidienste bestehen, sollen derartige Dienste auf nationaler Ebene eingerichtet werden. Österreich war eines der ersten Länder, das eine Spezialeinheit zur Bekämpfung der Computerkriminalität eingerichtet hat. Die Spezialisten des Innenministeriums zur Bekämpfung der Computerkriminalität genießen in den weltweiten Computercrime-Foren hohes Ansehen.