Kinderpornografie: In der Meldestelle im Bundeskriminalamt gingen im vergangenen Jahr 2.742 Hinweise ein.

„Darknet“: Cyber-Kriminelle nutzen vermehrt Online-Ressourcen und die Infrastruktur des alternativen Netzwerks.

Betrug und Erpressung

2015 stieg die Zahl der Fälle von betrügerischem Datenmissbrauch, digitaler Erpressung und Internetbetrug. Es gab weniger Fälle von „Hacking“.

Im vergangenen Jahr wurden in Österreich ca. 10.000 Fälle von Cybercrime registriert; um 11 Prozent mehr als 2015. Die Aufklärungsquote betrug 41,5 Prozent, um 0,7 Prozentpunkte mehr als 2014. Die Ursache der Zunahme der Zahl an Cybercrime-Delikten liegt laut Bundeskriminalamt (BK) unter anderem an der zunehmenden Technisierung der Täter und der Nutzung von Verschlüsselungs- und Anonymisierungstechniken. Das geht aus dem Cybercrime-Report 2015 des Bundeskriminalamts hervor.

Die Zahl der Anzeigen wegen Internetbetrugs stieg um 12,6 Prozent von 6.635 (2014) auf 7.473 (2015). Die Zahl der Fälle von betrügerischem Datenmissbrauch, vor allem durch Schadware, erhöhte sich um 60 Prozent von 404 (2014) auf 647 (2015).

Die Zahl der Cybercrime-Delikte im „engeren Sinn“ ist um 3,3 Prozent gesunken. Das sind Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden wie Datenbeschädigung, Hacking, DDoS-Attacken. Die Zahl der Anzeigen wegen widerrechtlichen Zugriffs auf ein Computersystem („Hacking“) sank von 677 (2014) um 42 Prozent auf 387 Anzeigen (2015).

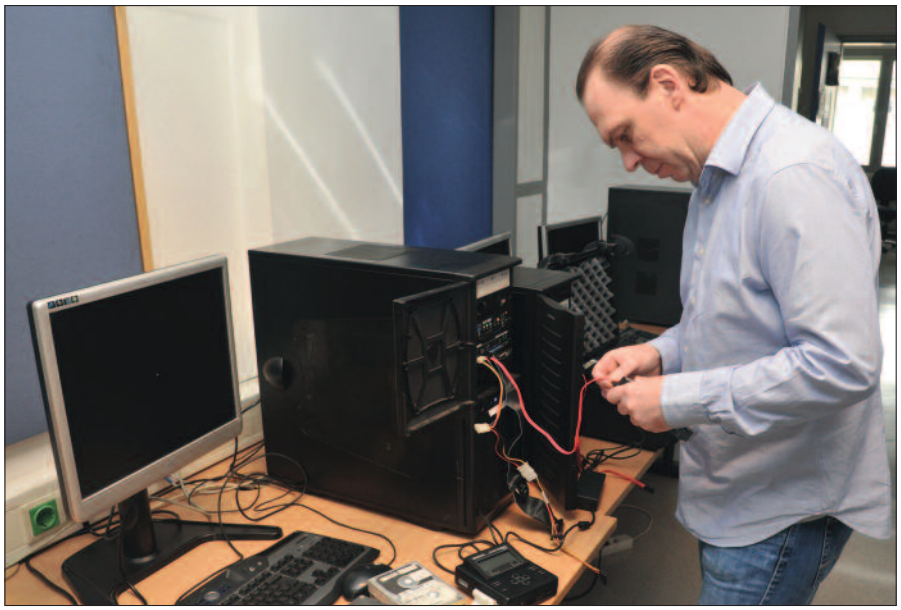
Ransomware. 2015 stieg die Zahl der Fälle von digitaler Erpressung mit einer Schadsoftware, die Daten und Systeme verschlüsselt. Für die Entschlüsselung verlangen die Täter Lösegeld (engl. Ransom), meist in Form des virtuellen Zahlungsmittels *Bitcoin* oder durch Prepaid-Karten. Beide Zahlungsformen sind anonym und erschweren die Strafverfolgung. Die Verbreitung der Verschlüsselungssoftware erfolgt über präparierte E-Mails, durch Sicherheitslücken in Webbrowsern oder unbemerkt durch Downloads aus dem Internet (Drive-by-Download). Betroffen sind Privatpersonen, Unternehmen, Behörden und sonstige Organisationen.

DDoS-Erpresser. Eine Tätergruppe namens „DD4BC“ war 2014 und 2015 weltweit für zahlreiche erpresserische E-Mails und DDoS-Angriffe verantwortlich. Ziel einer DDoS-Attacke (Distributed Denial of Service) ist es, die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems zu blockieren und Benutzern keinen Zugriff mehr zu ermöglichen. Dabei senden die Täter E-Mails an Online-Unternehmen, in denen sie diese auffordern, einen bestimmten Betrag mit dem virtuellen Zahlungsmittel *Bitcoin* zu entrichten, ansonsten würden sie den Zugriff auf Webseiten der Unternehmen mittels DDoS-Angriffen blockieren. Im Frühjahr 2015 trat diese Form der Online-Erpressung auch in Österreich verstärkt auf. Fünf Online-Unternehmen erstatteten Anzeige beim Bundeskriminalamt. Mitarbeiter des Cybercrime-Competence-Centers (C^4) nahmen die Ermittlungen auf und stellten internationale Kontakte her. Es stellte sich heraus, dass die Gruppe DD4BC auch in anderen Ländern aktiv war, weshalb das C4 eine gemeinsame Ermittlung mit Europol initiierte. Bei einer Polizeiaktion am 15. und 16. Dezember 2015 in Banja Luka in Bosnien wurden sieben Verdächtige festgenommen, darunter auch der Haupttäter. Die Ermittler stellten 600 Gigabyte elektronisches Datenmaterial sicher und forschten 59 E-Mail-Accounts und 251 Bitcoin-Wallets aus. Insgesamt waren 310 Unternehmen betroffen.

Darknet. In der Bekämpfung des Drogenhandels im Darknet arbeiten IT-Experten der Polizei und Drogenermittler zusammen. Die Drogenermittler bringen ihr Fachwissen bezüglich Suchtmittel und Täterverhalten ein, die IT-Experten gewährleisten eine professionelle Datensicherung zur Anklageerhebung, verfolgen Flüsse virtuellen Geldes. In einem Fall wurden innerhalb eines Jahres 14.000 Bestellungen und 6.000 Konsumenten registriert. Innerhalb von 16 Monaten wurde ein Betrag von 4,4 Millionen Euro umgesetzt.

Kinderpornografie. In der Meldestelle im Bundeskriminalamt für Kinderpornografie und Sextourismus zum Kindesmissbrauch gingen im vergangenen Jahr 2.742 Hinweise ein, wobei

Fotos: Kaspersky Lab, Egon Weissheimer



Cybercrime-Competence-Center im Bundeskriminalamt: Die Mitarbeiter stellten 2015 über 136 Terabyte an elektronischen Beweisen sicher.

310 Meldungen einen Österreichbezug aufwiesen. Österreich war an der internationalen Operation „Pacifier" von Europol beteiligt. Hintergrund waren Ermittlungen wegen des Besitzes und der Verbreitung pornografischer Darstellungen Minderjähriger. Die Ermittler werteten 50 IP-Adressen in Österreich aus und stellten unzählige kinderpornografische Dateien sicher.

Im Fall eines deutschen Staatsangehörigen mit österreichischem Wohnsitz erging ein Hinweis an die Meldestelle, dass über eine Social-Media-Plattform von einem Unbekannten pornografische Darstellungen Minderjähriger hochgeladen worden waren. In Zusammenarbeit mit den US-Behörden wurde der Mann ausgeforscht. Bei der Auswertung der sichergestellten Datenträger stellten die Kriminalisten fest, dass der Verdächtige Kontakt zu einem Mittäter auf den Philippinen hatte. Außerdem wurde er von den deutschen Behörden wegen Kindesmissbrauchs per Haftbefehl gesucht.

Das Cybercrime-Competence-Center (C^4) im Bundeskriminalamt ist die nationale Zentralstelle zur Bekämpfung von Cyber-Kriminalität in Österreich. In den Landeskriminalämtern gibt es ebenfalls Expertinnen und Experten auf dem Gebiet der IT-Forensik und der Bekämpfung von Cybercrime. Das C^4 beschäftigte 2015 37 Mitarbeiterinnen und Mitarbeiter aus Verwaltung, Polizei und Technik und ist in folgende Bereiche unterteilt: Zentrale Aufgaben, IT-Beweissicherung, Ermittlungen und Cybercrime-Meldestelle *(against-cybercrime@bmi.gv.at)*. Die Techniker des C^4 leisteten in etwa 20 komplexen Fällen technische Unterstützung bei Auswertungen und Ermittlungen. Im Bereich der IT-Beweissicherung wurden von den Mitarbeitern des C^4 2015 über 136 Terabyte (TB) an elektronischen Beweisen gesichert.

Smartphones und Tablets sowie Smart-Watches oder Minicomputer wie Raspberry Pi gewinnen immer mehr an Bedeutung für kriminalpolizeiliche Ermittlungen. Im Fachbereich „Mobile Forensik" wurden 1.200 mobile Geräte sowie die Fahrzeugelektronik und Datenspeicher von mehr als 100 Kraftfahrzeugen ausgewertet.

Meldestelle. Die Mitarbeiter der Cybercrime-Meldestelle bearbeiteten 10.000 Mitteilungen aus der Bevölkerung sowie von in- und ausländischen Dienststellen. In dringenden Fällen, etwa bei Suizidankündigungen über das Internet, können die Mitarbeiter des C^4-Journaldienstes die Einleitung von Maßnahmen zur technischen Unterstützung anderer Dienststellen veranlassen – wie Datensicherung, Handy und Navigationssystemauswertung.

Unterstützung für Kroatien. Im Juli 2014 begann in Kooperation mit der Cyber-Einheit des spanischen Innenministeriums ein 15 Monate laufendes, EU-finanziertes Projekt in Kroatien. Die Aufgabe der österreichischen Expertengruppe bestand darin, das „Ivan Vucetic Center" des kroatischen Innenministeriums beim Aufbau eines IT-Forensik Centers zu beraten.

Das Zentrum für Kriminaltechnik, Forschung und Expertise „Ivan Vucetic" ist Mitglied des „European Network of Forensic Science Institute" (ENFSI) und wird als herausragende Institution für forensische Wissenschaft in den Bereichen Schusswaffen, Daktyloskopie, DNA, Chemie und Toxikologie angesehen.

Kontakt. Verdächtige Sachverhalte im Internet können der Internetmeldestelle im Bundeskriminalamt *against-cybercrime@bmi.gv.at* gemeldet werden. Information sind in jeder Polizeiinspektion sowie auf der Homepage *www.bmi.gv.at/praevention* und per BMI-Sicherheits-App erhältlich. Die Spezialisten der Kriminalprävention stehen kostenlos und österreichweit unter der Telefonnummer 059 133 zur Verfügung.

FOTO: EGON WEISSHEIMER

STFRAFRECHT

Cybercrime

Delikte, die zu „Cybercrime im „engeren Sinne" gehören, sind beispielsweise

- § 118a Strafgesetzbuch (StGB): Widerrechtlicher Zugriff auf ein Computersystem,
- § 119 StGB: Verletzung des Telekommunikationsgeheimnisses,
- § 119a StGB: Missbräuchliches Abfangen von Daten,
- § 126a StGB: Datenbeschädigung,
- § 126b StGB: Störung der Funktionsfähigkeit eines Computersystems,
- § 126c StGB: Missbrauch von Computerprogrammen oder Zugangsdaten,
- § 148a StGB: Betrügerischer Datenverarbeitungsmissbrauch sowie
- § 225a StGB: Datenfälschung.

Unter Cybercrime im „weiteren Sinn" versteht man Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung für herkömmliche Straftaten eingesetzt wird, wie Betrugsdelikte, Kinderpornografie, Cyber-Grooming oder Cyber-Mobbing.