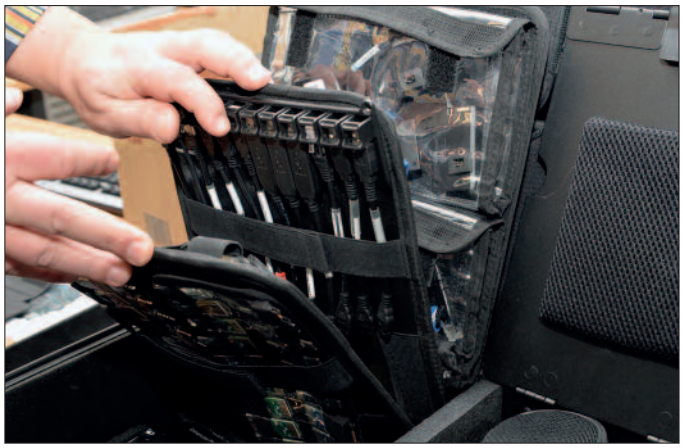
Sicherung von Handy-Daten: Bezirks-IT-Ermittler der Polizei sind die ersten Ansprechpartner bei IT-Kriminalität.



Zur Ausrüstung der Bezirksermittler gehören Computer, Kabel, Stecker und bei Bedarf forensische Software.

Ermitteln, sichern, unterstützen

Bezirks-IT-Ermittler der Polizei ermitteln in Fällen von Internetkriminalität, nehmen Anzeigen auf, sichern Daten von elektronischen Geräten und beraten Opfer von Cybercrime-Fällen.

Internetkriminalität nimmt weltweit zu. Die Cyber-Kriminellen sind technisch versiert, die Angriffsmethoden werden raffinierter. Diese Entwicklung erfordert rasche und unkomplizierte Hilfe für die Opfer. Aus diesem Grund werden österreichweit auch auf Bezirksebene speziell geschulte Polizistinnen und Polizisten eingesetzt, die in IT-relevanten Fällen wie Stalking, Drohungen über soziale Medien oder Internetbetrug ermitteln.

Cybercrime-Bekämpfung. 2011 wurde im Bundeskriminalamt das Cybercrime-Competence-Center, kurz C4, eingerichtet. Aufgrund der internationalen Auswirkungen der Cyber-Kriminalität nimmt das C4 eine zentrale und koordinierende Rolle bei IT- Ermittlungen und der elektronischen Beweismittelsicherung ein.

„Seit der Gründung des C4 hat sich das Büro ständig weiterentwickelt. Mittlerweile gibt es neben Forensikern, Ermittlern mit IT-Ausbildung und IT-Kenntnissen auch Mitarbeiter, die sich mit relevanten Themen wissenschaftlich auseinandersetzen“, berichtet Oberrat Mag. (FH) Gert Seidl, Leiter des Referates 5.2.1.C4 (Zentrale Aufgaben) im Bundeskriminalamt. „Da an den Umgang mit sichergestellten und kriminalpolizeilich relevanten Daten spezielle Anforderungen gestellt werden, musste neben dem IT-System des Innenministeriums, dem BAKS, eine eigene kriminalpolizeiliche EDV-Infrastruktur aufgebaut werden. Somit können auch große Mengen sensibler Daten, die bei Ermittlungen gesichert worden sind, in einem eigenständigen System von den Ermittlern bearbeitet werden“, erläutert der Experte.

Das C4 ist für Ermittlungen bei Fällen von „Cyber-Kriminalität im engeren Sinn“ zuständig. Das sind jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden. (z. B. Datenbeschädigung, Hacking, DDoS-Attacken).

Die „Meldestelle für Internetkriminalität“ im C4 *(against-cybercrime@bmi.gv.at)* bietet der Bevölkerung rund um die Uhr eine kompetente Ansprechstelle. Sollten Anrufer bereits Opfer von Cyber-Attacken geworden sein, wird ihnen von C4-Mitarbeitern erklärt, welche weiteren Schritte zu veranlassen sind. Ebenso besteht für die Opfer die Möglichkeit, eine kriminalpolizeiliche Beratung in Anspruch zu nehmen. Wer durch eine Straftat geschädigt wurde oder konkrete Hinweise auf einen Täter hat, kann das in jeder Polizeidienststelle anzeigen.

Gert Seidl: „Es ist geplant, dass Bezirks-IT-Ermittler in jedem Bezirk zur Verfügung stehen.“

Auf Landesebene sind die Landeskriminalämter – unabhängig von der Kompetenz des C4 im Bundeskriminalamt – für Ermittlungs-, Assistenz- und Ausbildungsaufgaben zuständig. Adäquat zum C4 obliegt ihnen die Bekämpfung der Internetkriminalität im engeren Sinn auf nationaler Basis. Dazu zählen sämtliche kriminalpolizeilichen insbesondere technischen Maßnahmen bei Cybercrime-Ermittlungen aber auch die forensische Sicherung, Auswertung und Datenbereitstellung bei Sicherstellungen von IT-Medien. Weiters unterstützen sie auch bei internetbasierenden Ermittlungen anderer Fachbereiche – zum Beispiel in sozialen Medien, in Chatforen oder bei tiefergehenden Ermittlungen im Darknet. Sie unterstützen die Assistenz- und Ermittlungsbereiche innerhalb des LKA und nachgeordneter Dienststellen wie Polizeiinspektionen, wenn es beispielsweise darum geht, eine forensisch korrekte Beweismittelsicherstellung sowie den Transport und die Verwahrung solcher Medien durchzuführen. Sie schulen ersteinschreitende Polizistinnen und Polizisten in den Polizeiinspektionen und vermitteln Grundkenntnisse an alle Mitarbeiterinnen und Mitarbeiter der Landespolizeidirektionen.

Auf Bezirksebene sind die Bezirks-IT-Ermittler (BezIT-Ermittler) der Polizei für IT-Ermittlungen zuständig. „Es ist geplant, dass österreichweit in jedem Bezirk, rund um die Uhr, speziell ge-

Fotos: Gernot Burkert, Gerd Pachauer, Egon Weissheimer

schulte Polizistinnen und Polizisten für Ermittlungen zu IT-spezifischen Straftaten zur Verfügung stehen“, sagt Seidl. Diese Kolleginnen und Kollegen sind in der Lage, IT-Ermittlungen einzuleiten oder je nach Sachverhalt und Zuständigkeit die Ermittlungen eigenständig zu führen und abzuschließen. „Die Aufgaben der Bezirks-IT-Ermittler betreffen nicht nur klassische Cybercrime-Sachverhalte. Sie unterstützen sämtliche Ermittlungen mit IT-Bezug. Zum Beispiel in einem Mordfall, wenn es darum geht, Handy-Daten oder Daten eines Navigationssystems auszuwerten, um ein Bewegungsprofil des Täters zu erstellen, oder Ermittlungen anhand öffentlich zugänglicher Quellen durchzuführen“, erklärt Seidl.

Häufige Aufgaben der Bezirks-IT-Ermittler sind Ermittlungen bei Delikten wie Stalking oder Drohungen über soziale Medien oder Internetbetrug. Sie unterstützen Kolleginnen und Kollegen im Streifendienst bei Amtshandlungen mit Bezug zur Internetkriminalität. Sie forschen IP-Adressen und/oder Ports aus, identifizieren Internetanschlüsse der Tatverdächtigen. Neben der Aufnahme von Anzeigen und der Sicherung von Beweismitteln, informieren und beraten sie Opfer von Cyber-Angriffen über die nächsten Schritte zur Verhinderung weiterer Schäden. Beispielsweise dann, wenn durch eine Ransomware (Verschlüsselungstrojaner) Daten auf einem Computer gesperrt wurden, für deren Entsperrung ein „Lösegeld“ verlangt wird. „Die Webseite *nomoreransom.org* bietet die Möglichkeit, anhand der verschlüsselten Daten oder des Erpresserschreibens, die Art des Verschlüsselungstrojaners festzustellen. Sollte dies gelingen, wird geprüft, ob es dazu bereits ein Entschlüsselungstool gibt. Im günstigsten Fall können die verschlüsselten Dateien wieder hergestellt werden“, erläutert Gert Seidl.

Die Webseite *nomoreransom.org* wurde durch eine Initiative der „National High Tech Crime Unit“, der niederländischen Polizei, des europäischen Cybercrime-Centers von Europol und „McAfee“ gegründet. Mittlerweile sind das österreichische Bundeskriminalamt sowie zahlreiche andere internationale Behörden und Organisationen Projektpartner. Ziel ist es, Opfern von Ransomware bei der Entschlüsselung zu helfen, ohne dass das Lösegeld an die Cyber-Kriminellen bezahlt wird. Zur Ausrüstung der Bezirksermittler gehören in der Regel ein Notebook, ein Speichermedium, ein mobiler Internetzugang oder ein Smartphone mit Internetzugang sowie allenfalls benötigte forensische Software.

Die Zahl der Cybercrime-Delikte nimmt zu, denn sie können mit wenig Aufwand und Werkzeug von überall in der Welt aus begangen werden.

Erfahrungen als Bezirks-IT-Ermittlerin. „Die Aufgabenbereiche der Bezirks-IT-Ermittler sind vielfältig und umfangreich. Deshalb sind ihre Tätigkeiten in den einzelnen Bundesländern unterschiedlich gewichtet. Ob der Schwerpunkt stärker auf die Datensicherung oder Datenauswertung oder auf die digitalen Ermittlungen gelegt wird, hängt auch von den Fähigkeiten, den Interessen und von dem zur Verfügung stehenden Equipment des einzelnen Ermittlers ab“, erläutert Dipl.-Ing. Christina Schindlauer, BSc. Schindlauer ist Leiterin des Referats „Entwicklung und Innovation“ (Referat 5.2.4) im C4 im Bundeskriminalamt. Davor war die Expertin von 2016 bis 2019 als Ermittlerin in der „Sonderkommission Clavis“ im BK tätig, eine auf Ransomware-Delikte spezialisierte Sonderkommission, die national alle derartigen Fälle übernommen hat.

Schindlauers Karriere als Polizistin begann in Salzburg in der Polizeiinspektion Hauptbahnhof. Im Herbst 2009 wechselte sie ins Kriminalreferat Salzburg, um bei Vermögensdelikten im Internet zu ermitteln. Dort fing sie auch als Bezirks-IT-Ermittlerin an.

Money-Mules. „Ich kann mich an einen Fall aus meiner Zeit als Bezirks-IT-Ermittlerin 2015 erinnern, bei dem die Täter mittels E-Banking-Trojanern von Konten verschiedener Bankinstitute Gelder auf inländische – von Money-Mules eröffnete Konten – überwiesen haben.“ Money-Mules werden angeworben, um Geld zu empfangen und weiterzuleiten. Es gibt zwei Arten davon: Wissende, die über die Organisation und die kriminellen Handlungen Bescheid wissen und nicht Wissende, die über angeblich lukrative Jobangebote im Internet oder durch Zeitungsannoncen angeworben werden und dann Geldwäscherei begehen, im Glauben, sie würden einer legalen Tätigkeit nachgehen. In dem von Schindlauer geschilderten Fall konnten 51 Money-Mules zu den Geldtransaktionen, die durch den „Emotet-Trojaner“ (2015) verursacht wurden, miteinander in Zusammenhang gebracht werden. Bei fünf dieser Personen handelte es sich um österreichische und deutsche Staatsangehörige. Die Money-Mules, die festgenommen wurden, machten unterschiedliche Angaben, wenn es darum ging wie sie angeheuert wurden. Die Mehrzahl sei von einem Unbekannten in ihrem Heimatland angesprochen worden, der ihnen einen Job in der Baubranche in Österreich angeboten habe. Sie erhielten Geld für die Reise nach Österreich. In Österreich wurden sie von einem unbekannten Mann, der Russisch sprach, in Empfang genom-

Foto: DragonImages/Stock.adobe.com

men. Die Money-Mules bekamen eine Unterkunft in einem Hotel und Taschengeld. Sie mussten zum Schein einen österreichischen Wohnsitz anmelden. Die Adresse wurde ihnen vorgegeben, die Unterschrift des vermeintlichen Vermieters war gefälscht. Mit dem Meldezettel konnten sie Bankkonten eröffnen. Die Zugangsdaten zum Online-Banking wurden an eine Kontaktperson im Internet weitergegeben. Dabei wurden etwa 100 Bankkonten eröffnet, auf die Gelder von einem E-Banking-Trojaner überwiesen werden sollten. „Einer der Beschuldigten hat zugegeben, dass jeder von ihnen 500 bis 1.000 Euro pro Behebung erhalten sollte. Das Geld ist an Personen der dahinterliegenden Organisation übergeben worden. Es handelt sich in diesem Fall um ein Beispiel von Crime as a Service“, sagt Schindlauer. Elf Personen wurden in Österreich festgenommen, zehn davon wurden verurteilt – in den meisten Fällen wegen betrügerischen Datenverarbeitungsmissbrauchs (§ 148a StGB) oder wegen Geldwäscherei (§ 165 StGB). Die Haftstrafen betrugen durchschnittlich 5 bis 18 Monate. Die Schadenssumme in diesem Fall lag bei etwa 210.000 Euro.

„Die Täter haben grenzüberschreitend agiert. Betroffene dieser Malware-Attacke hat es in Österreich, Deutschland, der Schweiz und in 52 übrigen Ländern gegeben“, sagt Schindlauer. Das Geld wird weiter nach Osten – beispielsweise in die Ukraine – über Geldtransferinstitute versendet. Mittlerweile werden auch Kryptowährungen wie Bitcoins genutzt, um die Gelder zu waschen „Ohne koordiniertes internationales Vorgehen, ist derartigen Tathandlungen kaum Einhalt zu gebieten“, sagt Schindlauer.

Ziel für die Zukunft ist es, dass Bezirks-IT-Ermittler in den Polizeiinspektionen bzw. in den Bezirks- oder Stadtpolizeikommanden mehr für kriminalpolizeiliche Ermittlungen bei Cyber-Kriminalität und digitale Forensik eingesetzt werden. Ob sich Polizisten für den Job des Bezirks-IT-Ermittlers eignen, wird von den Landeskriminalämtern beurteilt. „Die Ausbildung zum Bezirks-IT-Ermittler besteht aus einer Grundausbildung im Bundeskriminalamt und aus einer Praxisphase in den Landeskriminalämtern sowie aus periodischen Fortbildungen“, erklärt Seidl.

Gernot Burkert