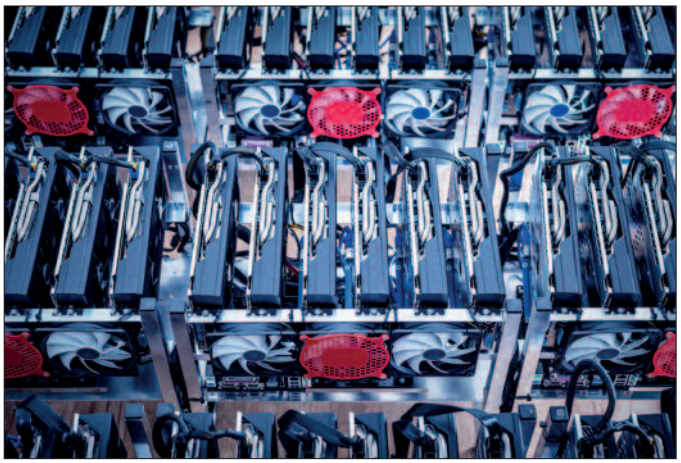
Durch Verschlüsselungssoftware wurden 2017 weltweit mehrere Hunderttausend Computer infiziert.



Die Erzeugung von Kryptowährungen benötigt enorme Rechenleistungen. Hacker zapfen dafür fremde Computer an.

Anstieg an Anzeigen

Die Polizei verzeichnete 2017 einen Anstieg der Zahl an Cybercrimedelikten um 28,2 Prozent gegenüber 2016. Gestiegen sind Fälle von Datenbeschädigung und Internetbetrügereien.

Die Zahl der Cybercrime-Anzeigen stieg von 13.103 Anzeigen 2016 um 28,2 Prozent auf 16.804 Anzeigen 2017. Die Zahl der Tatbestände von Cybercrime im engeren Sinne ist von 2.630 im Jahr 2016 um 34,8 Prozentpunkte auf 3.546 im Jahr 2017 angestiegen. Unter Cybercrime im engeren Sinne versteht man Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden. Ein überdurchschnittlicher Anstieg bei der Zahl der Anzeigen nach dem Strafgesetzbuch (StGB) wurde 2017 verzeichnet bei Datenbeschädigung (§ 126a StGB, 1.184 Anzeigen, + 80,5 %), Datenfälschung (§ 225a StGB, 231 Anzeigen, + 66,2 %) und betrügerischem Datenverarbeitungsmissbrauch (§ 148a StGB, 1.055 Anzeigen, + 29,3 %).

Die Aufklärungsquote bei Cybercrime im engeren Sinne wurde um 10,2 Prozentpunkte von 18 auf 28,2 Prozent gesteigert. „Die aktuellen Zahlen zeigen, dass wir im Bereich Cybercrime vor großen Herausforderungen stehen“, sagte Innenminister Herbert Kickl.

„Im Kampf gegen diese Kriminalitätsform sind modernste Technik und gut ausgebildete Mitarbeiterinnen und Mitarbeiter wichtige Eckpfeiler. Diese Komponenten sind im Cybercrime-Competence-Center (C4) vereint. Die Steigerung der Aufklärungsquote ist ein wichtiger Schritt und zeigt, dass im Cybercrime-Competence-Center professionelle Arbeit geleistet wird.“

Die Zahl der Cybercrime-Delikte im weiteren Sinne stieg 2017 um 26,5 Prozentpunkte gegenüber 2016. Unter Cybercrime im weiteren Sinne versteht man Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung herkömmlicher Straftaten eingesetzt wird, wie Betrugsdelikte oder Cyber-Mobbing. 2017 konnte in allen Bereichen der angezeigten Fälle ein Anstieg festgestellt werden. Im Vergleich mit 2016 stieg die Zahl der angezeigten Fälle wegen Anbahnung von Sexualkontakten mit Unmündigen (§ 208a StGB) von 80 auf 106 Delikte (+ 32,5 %).

Ransomware. Durch die Verschlüsselungssoftware *Petya/NotPetya* und *WannaCry* wurden 2017 weltweit mehrere Hunderttausend Computer infiziert. Diese Schadsoftware verschlüsselt die Daten der infizierten Computersysteme. Die Täter verlangen von den Opfern für die Entschlüsselung eine bestimmte Summe in der Kryptowährung Bitcoin. Trotz Bezahlung des Lösegeldes, werden die Daten der Opfer in der Regel nicht entschlüsselt. Die im Bundeskriminalamt zur Bekämpfung von Ransomware eingerichtete „Soko Clavis“ verzeichnete in den Monaten Februar und März 2017 einen sprunghaften Anstieg bei der Zahl der Anzeigen wegen Erpressung durch Verschlüsselungssoftware.

Seit Ende 2017 gibt es neue Angriffsvarianten. Bis dahin waren Phishing-Mails mit Links zur Schadsoftware oder Dateianhänge hauptsächlich für die Verschlüsselung der Daten verantwortlich. Nun erfolgen Angriffe oft über die RDP-Schnittstelle (Remote Desktop Protokoll). Solche mangelhaften oder mit einfachen Passwörtern abgesicherten Schnittstellen sind das Angriffsziel der Täter. RDP-Schnittstellen werden zum Fernsteuern oder zur Fernwartung eines Computers und zum Darstellen dessen Bildschirminhaltes benötigt.

Die Zugangsdaten werden mit spezieller Software geknackt, um in die Systeme der Opfer einzudringen und die Daten zu verschlüsseln. Auch die Geldforderungen der Täter haben sich geändert. Früher wurden von den Tätern fixe Geldbeträge für die Entschlüsselung eines Gerätes verlangt. Nun wird nach vorheriger Abschätzung der finanziellen Möglichkeiten der Opfer die Höhe des Lösegeldes individuell abgestimmt. Hilfe bei Entschlüsselungsprogrammen bietet die Internetseite *www.nomoreransom.org*.

Kryptojacking. Der Wertzuwachs der Bitcoins machte den Einsatz von Kryptowährungen für kriminelle Handlungen immer beliebter. Kryptowäh-

Fotos: Michal Bednarek/Fotolia, Nicescene/Fotolia

Die Zahl der Angriffe auf Daten oder Computersysteme ist 2017 um knapp 35 Prozent gestiegen.

rungen wurden häufig für die Begehung klassischer Delikte zum Beispiel Betrugshandlungen mit Bitcoin-Bons und Phishing-Versuche zur illegalen Aneignung von Zugangsdaten verwendet. 2017 wurden im Zusammenhang mit Kryptowährungen neue kriminelle Phänomene wahrgenommen, wie beispielsweise die Verwendung fremder Rechenleistung zum „Minen" (Schürfen). So wird der kryptografische Prozess bezeichnet, mit dem neue Bitcoins errechnet werden. Das erfordert eine hohe Rechenleistung. Der Wert von Bitcoins rührt daher, da sie aufwendig herzustellen sind.

Das Erschleichen fremder Rechenleistung, um Bitcoins zu „schürfen" oder zu „minen", wird als „Kryptojacking" bezeichnet. Über „Mining-Trojaner" verschaffen sich Kriminelle Zugang zu Rechnern. Die Besitzer der befallenen Computer müssen mit Leistungseinbußen ihrer Geräte rechnen, da sie mit dem „Mining" ausgelastet sind. Außerdem steigt der Stromverbrauch. Kriminelle bringen daher zunehmend Geräte aus dem Internet der Dinge etwa Router, Drucker, Webcams und andere Geräte mit Internetanschluss unter ihre Kontrolle. Die kriminelle Handlung ist nur dann rentabel, wenn das „Mining" ohne nennenswerte eigene Ausgaben erfolgen kann und die Kosten auf viele andere Geschädigte verteilt werden können. Nicht nur Kleinkriminelle betreiben illegales Krypto-Mining, auch die organisierte Kriminalität hat dieses lukrative Geschäftsmodell entdeckt. Vor „Mining-Trojanern" schützen Virenschutzprogramme. Man kann sich die Malware auch durch den Besuch bestimmter Websites im Netz einhandeln oder durch Werbebanner. Schutz davor bieten etwa Miner-Block-Erweiterungen in Internetbrowsern.

Neues Referat. Mit 1. November 2017 wurde im Cybercrime-Competence-Center das Referat für Entwicklung und Innovation eingerichtet, um neueste Entwicklungen aus Wissenschaft und Forschung für die polizeiliche Anwendung zu erschließen. Aufgabe des Referats ist Forschung und Bewertung von Phänomenen im Bereich der IT-Kommunikation insbesondere im Internet, einschließlich der automatischen maschinengestützten Kommunikation (Internet of Things); die wissenschaftliche Entwicklung von Konzepten und Werkzeugen zur Kriminalitätsbekämpfung, Abwehr und Aufklärung mit Hightech-Ansätzen sowie künstlicher Intelligenz und Methoden der Datenanalyse; die Bewertung neuer Entwicklungen und Technologien sowie der Aufbau und Betrieb einer IT-spezifischen wissenschaftlichen Wissensdatenbank; die wissenschaftliche Entwicklung, der Aufbau und Betrieb eines Echtzeit-Lagebildes über kriminelle Aktivitäten und Bedrohungen im Cyber-Raum; die Vernetzung mit Forschungseinrichtungen sowie Ziel- und Bedarfsdefinitionen für die Sicherheitsforschung im Cyber-Bereich; Sachverständigentätigkeit im Bereich der Informations- und Kommunikationstechnik.

Beweissicherung und Analyse. 2017 konnte wieder ein deutlicher Anstieg der Zahl an forensischen Auswertungen verzeichnet werden. Aufgrund der technischen Entwicklung wird die Auswertung digitaler Medien immer schwieriger. Herstellerspezifische verschlossene Systeme mit ausgeprägten Verschlüsselungsverfahren stellen die elektronische Beweissicherung fortwährend vor Herausforderungen. Insbesondere in der mobilen Forensik werden Datensicherungen und Auswertungen immer schwieriger. Mit einer selbst entwickelten technischen Lösung zum Öffnen versperrter Geräte konnte 2017 ein Vorstoß in diesem Bereich erzielt werden.

FOTO: TEROVESALAINEN/FOTOLIA

Mobile Geräte. Daten werden vermehrt auf verschlüsselten Medien oder in der Cloud gespeichert. Dadurch können sich neue Abhängigkeiten und neue Gefahren ergeben, aber auch Chancen der professionelleren und sicheren Betreuung von IT-Systemen. Bei der forensischen Sicherung von Daten im Darknet wird die „Live-Forensik" immer wichtiger. Erschwert wird die Arbeit der Ermittler technisch und rechtlich. Rechtliche Grundlagen – insbesondere bei grenzüberschreitenden Amtshandlungen – stellen die Datensicherer vor immer größere Herausforderungen.

Big Data. Ermittler beschlagnahmten 2017 bei Wirtschafts-, Korruptions- und Gewaltdelikten Daten im dreistelligen Terabyte-Bereich. Derartige Datenmengen für das Gericht verwertbar zu machen, stellt die Datensicherung und deren Auswertung vor Herausforderungen. In Zusammenarbeit mit den zuständigen Fachabteilungen im BK sowie in den Landeskriminalämtern wurde an der Weiterentwicklung und der Einführung von Such- und Analysetools gearbeitet. Diese sollen künftig eine leichtere und effizientere Bearbeitung von Massendaten ermöglichen.

Kfz-Forensik. Auch die Zahl der forensischen Auswertung von Fahrzeugdaten ist gestiegen. 2017 wurden vermehrt Motorräder mit elektronischen Werkzeugen gestohlen sowie Kfz durch überwinden der elektronischen Wegfahrsicherungen. Es wurden vermehrt Autos mit Keyless-Entry/Keyless-Go-Systemen durch „Funkstreckenverlängerer" in Betrieb genommen und gestohlen. Der Fortschritt in der Automobilindustrie, insbesondere des autonomen Fahrens sowie autonomer Verkehrsleitsysteme, ergibt neue Sicherheitslücken, die Gegenstand von Ermittlungen werden und forensische Datensicherungen erforderlich machen können. Der Einsatz von Drohnen – privat und kommerziell – geht mit neuen Kriminalitätsformen und neuen Bedrohungen einher. Durch die steigende Zahl der missbräuchlichen Verwendung von Drohnen als Tatmittel sind neue Ermittlungsmethoden zur forensischen Beweismittelsicherung erforderlich.

„IO-Threats". Das Projekt „IO-Threats" setzt sich mit Internet of Things (IoT) und damit einhergehenden Bedrohungen auseinander. Ziel ist es, forensisch und polizeilich tätig zu werden. Dabei werden potenzielle Angriffsszenarien auf den österreichischen Smart-Home-Markt beleuchtet. Gleichzeitig findet eine Bewertung der Rechtslage statt, die darauf ausgerichtet ist, polizeiliche Maßnahmen nach Projektabschluss zu etablieren. Das Projekt läuft von September 2017 bis März 2019. Projektteilnehmer sind neben dem C4 das *Joanneum Research,* eine außeruniversitäre Forschungseinrichtung der Uni Graz, das *Austrian Center for Law Enforcement Sciences (ALES),* ein Unternehmen sowie das Polizei- und Justizforschungszentrum der Universität Wien.

Upload-Plattform. Terroranschläge stellen die Sicherheitsbehörden bei den Ermittlungen vor neue Herausforderungen. Die Identifizierung der Täter sowie das Auffinden und die Sicherung von Beweisen spielen eine große Rolle. An vielen öffentlichen Plätzen sind Videosysteme installiert, die für kriminalpolizeiliche Auswertungen herangezogen werden können. Diese Systeme sind nicht flächendeckend eingesetzt. Für die Ermittlungen sind relevante Plätze daher nicht umfasst oder nicht eindeutig einsehbar. Oft ist auch die Qualität der Aufnahmen mangelhaft.

Gefährliche Situationen erfordern eine rasche Übersicht über die Geschehnisse, um mögliche weitere Gefahren zu verhindern. Es müssen alle Informationen herangezogen werden, die Aufschluss über den Ablauf der Geschehnisse liefern. Mit Smartphones können Bild-, Video- und Tonaufzeichnungen erstellen werden. Da derartige Aufzeichnungen Informationen für Ermittlungen beinhalten können, soll nach dem Vorbild der bayrischen Polizei der Bevölkerung die Möglichkeit geboten werden, Aufnahmen über eine Upload-Plattform der Polizei zu übermitteln. Dazu steht künftig ein Web-Portal zur Verfügung, das bei Großschadenslagen aktiviert und der Link zu dieser Upload-Plattform in Medien publiziert wird. Eine Sichtungsgruppe bewertet und klassifiziert die Daten.

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

VEREINIGUNG DER AUTODIEBSTAHLSERMITTLER

Vortrag von BK-Experten

Chefinspektor Horst Reisner, MSc und Kontrollinspektor Armin Rauchbüchl, MSc vom Cybercrime-Competence-Center nahmen im August 2018 in Pittsburgh in den USA an einer Veranstaltung der „International Association of Auto Theft Investigators", IATTI) teil zum Thema „Downloading and analyzing digital data from Vehicles". Die beiden Kfz-Forensiker des Bundeskriminalamts erläuterten technische Möglichkeiten der Kfz-Forensik, Trends, die Arbeitsweise und Zusammenarbeit in der österreichischen Polizei sowie Entwicklungen in der EU. Weitere Themen des Seminars waren Kfz-Diebstahl und -Verschiebung, Manipulationen an Fahrzeugen, Ermittlungen nach Straftaten mit Fahrzeugen in Zusammenhang mit einem Terrorhintergrund. Bei der Veranstaltung ging hervor, dass der Bedarf an der Sicherung digitaler Informationen in Zusammenhang mit der Strafverfolgung und Aufklärung von Straftaten steigt, was eine Spezialisierung von Fachkräften verschiedener Polizei- und Justizbehörden erfordert. Auch bei der Verkehrsunfallaufnahme wird die Sicherung digitaler Informationen aus Steuergeräten und Sensoren eine bedeutende Rolle spielen.

Horst Reisner, IAATI-Präsident William H. Johnson, Armin Rauchbüchl.

FOTO: BUNDESKRIMINALAMT