Mehr Internetbetrugs-Fälle

Die Zahl der Cybercrime-Anzeigen stieg auch 2018 an. Die Polizei verzeichnete vor allem eine Zunahme der Zahl an Fällen von Internetbetrug. Gesunken ist die Zahl der Fälle von Hacking.

Die Zahl der Cybercrime-Anzeigen stieg von 16.804 im Jahr 2017 auf 19.627 (+ 16,8 %) 2018 an. Ein Rückgang wurde bei der Zahl der Tatbestände von „Cybercrime im engeren Sinn“ verzeichnet. Darunter werden jene Straftaten verstanden, die das Ziel haben, Daten- oder Computersysteme mit Hilfe von Informations- oder Kommunikationstechniken anzugreifen. Die Anzahl der gemeldeten Fälle sank um 13,4 Prozent von 3.546 (2017) auf 3.070 (2018). Ein Rückgang (- 65 %) ist bei der Zahl der Anzeigen von Datenbeschädigung (§ 126a StGB) zu verzeichnen – von 1.186 Fällen 2017 auf 415 2018.

Cybercrime-Bekämpfung: Auslesen einer von Ermittlern sichergestellten Festplatte.

Angestiegen ist die Zahl der Fälle von Widerrechtlichem Zugriff auf Computersysteme (§ 118a StGB, + 11 %), Missbräuchlichem Abfangen von Daten (§ 119a StGB, + 9,8 %) und betrügerischem Datenverarbeitungsmissbrauch (§ 148a StGB, + 34 %). Die Aufklärungsquote bei den Delikten von Cybercrime im engeren Sinn stieg von 28,2 Prozent (2017) auf 32,1 Prozent (2018).

Anstieg. Die Zahl der Anzeigen wegen „Cybercrime-Delikten im weiteren Sinn“ stieg im Vergleich mit 2017 um 23,9 Prozent auf 16.557. Zu „Cybercrime im weiteren Sinn“ werden jene Straftaten gezählt, bei denen Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung herkömmlicher Straftaten, wie Betrug oder Erpressung unter Nutzung von Informationstechnologien sowie Urkundenfälschung verwendet werden.

2018 wurde in allen Deliktsbereichen, die unter „Cybercrime im weiteren Sinn“ fallen, ein Anstieg der Zahl der Anzeigen verzeichnet, bis auf den Straftatbestand der Urkundenfälschung. Hier wurde vor allem bei der Fälschung von besonders geschützten Urkunden eine Verringerung der Zahl der Anzeigen um 79,4 Prozent registriert. Im Vergleich mit 2017 ist die Zahl der Anzeigen wegen Erpressung (§ 144 StGB) um 237 Prozent, von 474 auf 1.599 angezeigte Fälle, angewachsen.

Data-Leaks. Ein immer wiederkehrendes Problem stellen „Data-Leaks“ (Datenlecks) dar. Geleakte Datensätze können Namen, Mailadressen, Zugangsdaten oder Passwörter beinhalten. 2018 wurden große Sammlungen geleakter Daten der letzten Jahre zusammengefasst und in gebündelter Form nicht nur im Darknet, sondern auch auf konventionellen Internetseiten zum Kauf angeboten. Diese missbräuchlich gewonnen Datensätze resultieren aus Angriffen auf verschiedene Geräte beziehungsweise Anwendungen. Einfallstor hierfür bieten schlecht gesicherte Webportale oder Mitarbeiter- und Kundenplattformen von Unternehmen.

Aufgrund der Ermittlungserfolge des Cybercrime-Competence-Centers (C4) im Bundeskriminalamt konnten 2018 annähernd 100.000 Betroffene über ihre im Netz aufgetauchten Daten informiert werden.

„Distributed Denial of Service“ – DDoS-Angriffe. Mitarbeiter des Cybercrime-Competence-Centers beteiligten sich bei internationalen *EMPACT*-Projekten *(European Multidisciplinary Platform Against Criminal Threats)* sowie an operativen Einsätzen bei der „Joint Cybercrime Action Taskforce (J-CAT)“ bei Europol, die sich mit der Bekämpfung von DDoS-Angriffen beschäftigen. Unter DDoS (Distributed Denial of Service = Verweigerung des Dienstes) versteht man einen Angriff auf die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems oder von Netzwerken, meistens mit dem Ziel, diese zu blockieren und somit regulären Benutzern keinen Zugriff mehr zu ermöglichen. Die Angriffe erfolgen häufig von vielen verschiedenen Ressourcen aus dem Internet. Neben politisch oder persönlich motivierten Angriffen versuchen Täter auch häufig, Geld mit DDoS-Angriffen zu erpressen.

Im April 2018 gelang es unter der Koordinierung von J-CAT mit der Operation „Power off“ den größten Dienstanbieter für DDoS-Angriffe „webstresser.org“ vom Netz zu nehmen. Diese internationale Amtshandlung war unter anderem ausschlaggebend dafür, dass die Anzahl der DDoS-Angriffe während der österreichischen EU-Ratspräsidentschaft im zweiten Halbjahr 2018 gering gehalten werden konnte.

Ransomware. Der „Erpressungstrojaner“ blieb auch 2018 Gegenstand der Ermittlungsarbeiten der speziell zur Bekämpfung von Ransomware eingerichteten „Soko Clavis“ des Bundeskriminalamts. Dabei gelang es den Ermittlern, mehrere Verdächtige auszuforschen, die durch Verbreitung von Ransomware Schäden in Millionenhöhe verursachten. Die Ermittler sehen sich zunehmend mit Cyber-Kriminellen konfrontiert, die nicht nur Tools verwenden, die leicht aus dem Darknet zu beschaffen sind, sondern sich auch Fachwissen aneignen.

Als Ransomware wird Schadsoftware bezeichnet, die den Zugriff auf Daten und elektronische Systeme einschränkt oder verhindert. Diese Ressourcen werden erst wieder nach Bezahlung eines Lösegeldes („Ransom“) freigegeben.

FOTO: GERD PACHAUER

Internetbetrug erfolgt in verschiedensten Formen: von der vorgetäuschten Warenlieferung bis zum Gewinnversprechen. Aufgrund der zunehmenden Digitalisierung verlagern sich immer mehr Vorgänge ins Internet. Da sich Kriminelle rasch den Neuerungen anpassen, werden immer neuere und gezieltere Betrugsformen entwickelt, die durch Anonymisierung und Verschleierung der Finanzflüsse unerkannt und für Täter „sicher" durchzuführen sind. Aufgrund des weltweiten Zugangs zum Internet sind Kriminelle in der Lage, ein breites Publikum anzusprechen und zu Opfern zu machen.

Besonders häufig sind das Versenden von Gewinnversprechen via E-Mail, Bestellbetrügereien mittels Fake-Webshops, das Verwenden falscher Identitäten und Kontaktdaten bei Online-Einkäufen oder das „Love-Scamming" in den soziale Medien zu beobachten.

Kryptowährungen und Behördenwallets. „Cryptos", wie Bitcoin oder Ethereum, werden trotz Kursverlusten bei legalen sowie illegalen Bezahlvorgängen verwendet. Bei Ermittlungen gegen einen Suchtmittelverkäufer im Darknet ist das C4 auf eine bislang unbekannte Kryptowährungstransaktion, „Smart Contracts" gestoßen. Hierbei handelt es sich um Computerprotokolle, die Verträge abbilden, überprüfen oder die Verhandlung und Abwicklung eines Kaufs technisch unterstützen.

Seit 2018 ist das C4 rechtlich und technisch befähigt Kryptowährungen sicherzustellen. Dafür werden extra Behörden-Wallets eingerichtet, in denen die virtuelle Währung aufbewahrt wird. Das Gericht erklärt die sichergestellten „Cryptos" meist für verfallen. Anschließend ist das C4 ermächtigt, die Verwertung vorzunehmen und die Geldsummen an die jeweiligen Gerichte zu transferieren.

Kinderpornografie. Im Tatbestand Pornografische Darstellung Minderjähriger (§ 207a StGB) kam es im Vergleich mit 2017 zu einer erheblichen Zunahme der Zahl an Anzeigen um 58,4 Prozent auf 1.161 angezeigte Straftaten. Dies ist unter anderem darauf zurückzuführen, dass die Anbieter von sozialen Medien in den USA und Kanada der Verbreitung kinderpornografischen Materials den Kampf angesagt haben. Sollte ein geprüfter Inhalt positiv sein, wird der Account gesperrt und eine Verdachtsmeldung erfolgt an das jeweilige Land, das den Verursacher dann identifizieren kann. In diesem Zusammenhang stellt das „Liken" und Weiterleiten von Videos, die sexuelle Handlungen von Minderjährigen mit Tieren zum Inhalt haben, einen neuen und unterschätzten Tat-Modus dar. Als „Spaßvideos" werden diese an andere Benutzer weitergeleitet, ohne zu bedenken, dass sowohl der Besitz als auch die Verbreitung eines solchen Videos strafbar ist.

Das Bundeskriminalamt hat Behörden-Wallets für Kryptowährungen eingerichtet, in denen sichergestellte virtuelle Währung aufbewahrt wird.

Negativtrend. Der Trend vom Vorjahr setzt sich auch 2019 durch. Die vorläufigen Daten der Kriminalstatistik aus dem ersten Halbjahr zeigen, dass die Internetkriminalität weiterhin eine große Herausforderung bleibt. In den ersten sechs Monaten wurden 13.020 Delikte zur Anzeige gebracht, im Jahr 2018 waren es 8.659 gemeldete Straftaten. Ein besonderer Anstieg von 32,3 Prozent auf 8.187 Anzeigen ist im Bereich Internetbetrug zu erkennen.

Prävention. Die Polizei hat ein Maßnahmenpaket ausgearbeitet. Für Privatpersonen wurde eine Präventions- und Informationskampagne auf unterschiedlichen Medien initiiert, um möglichst viele Menschen zu erreichen und ihnen Tipps für den sicheren Umgang mit dem Internet bereitzustellen. Weiters wird eine österreichweite Roadshow starten, die Informationen an alle Interessierten vermitteln wird. Präventionsmaßnahmen wie „Under.18", „Sicher in den besten Jahren" und „Cyber.Sicher" werden verstärkt durchgeführt.

Polizei kontaktieren. Verdächtige Sachverhalte im Bereich Cybercrime können rund um die Uhr an die Internetmeldestelle *against-cybercrime@bmi.gv.at* weitergeleitet werden. Informationen finden sich in jeder Polizeiinspektion und unter *www.bundeskriminalamt.at/praevention* sowie in der Polizei-App. Die Beamtinnen und Beamten der Kriminalprävention stehen unter der Telefonnummer 059 133 mit Rat und Tat zur Seite. *Romana Tofan*

FOTO: IURIIMOTOV/ADOBE.STOCK.COM