Etwa 60 Prozent aller Anzeigen wegen Cybercrime betreffen Internet-Betrugsdelikte.

Betrug und Erpressung

Die Polizei registrierte 2019 um 45 Prozent mehr Cybercrime-Delikte als 2018. Erpresser-E-Mails, Internetbetrugsdelikte und Ransomware fordern die Ermittler.

Die Zahl der Anzeigen wegen Cybercrime stieg von 19.627 im Jahr 2018 auf 28.439 im Jahr 2019 an. Die Aufklärungsquote lag bei 35,8 Prozent. Die Zunahme der Zahl an Anzeigen kann auf den massiven Anstieg der Zahl an Massenerpressungs-E-Mails Anfang 2019 sowie der stark steigenden Zahl von Internetbetrug zurückgeführt werden. Weiters zeigte sich der Trend zur Nutzung von Ransomware und „Crime-as-a-Service"-Leistungen aus dem Darknet. Um gegen Erpresser-E-Mails vorzugehen, wurde im Bundeskriminalamt eine Arbeitsgemeinschaft „ARGE Erpressungsmails" eingerichtet.

Cybercrime. Cybercrime-Delikte werden in zwei Kategorien eingeteilt: Cybercrime im engeren Sinne umfasst jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnik (IKT) erfolgen. Die Straftaten sind gegen die Netzwerke oder gegen Geräte, Dienste oder Daten in diesen Netzwerken gerichtet, wie zum Beispiel bei der Datenbeschädigung, Hacking oder DDoS-Angriffen (Distributed Denial of Service). Die Zahl der Anzeigen der DDoS-Angriffe stieg um 148,3 Prozent gegenüber 2018. Die beiden häufigsten Delikte waren der widerrechtliche Zugriff auf ein Computersystem (§ 118a StGB) und der betrügerische Datenverarbeitungsmissbrauch (§ 148a StGB).

Unter Cybercrime im weiteren Sinne versteht man alle Straftaten, bei denen die IKT als Tatmittel zur Planung, Vorbereitung und Ausführung von Straftaten eingesetzt wird, wie beispielsweise Betrugsdelikte, Suchtmittelhandel im Darknet, pornografische Darstellung Minderjähriger im Internet, Cybergrooming oder Cybermobbing.

Internetbetrug. 2019 erreichte der Internetbetrug mit 16.831 angezeigten Fällen einen neuen Höchststand. Zudem machte er rund 59 Prozent aller Cybercrime-Anzeigen aus. Die Aufklärungsquote konnte gegenüber 2018 mit 37,9 Prozent stabil gehalten werden. Internetbetrug gibt es in verschiedenen Varianten. Sie reichen von Anlagebetrügereien, Gewinnversprechen in E-Mails oder Love- beziehungsweise Romance-Scam bis hin zum Bestellbetrug durch vorgetäuschte Warenlieferungen. Die Täter nutzen das Internet als Werkzeug zur Begehung dieser Taten, denn es bietet die Möglichkeit, weitgehend unerkannt eine große Anzahl an Menschen zu erreichen. Deshalb ist bei dieser Deliktsform zumeist von Massendelikten auszugehen.

Ransomware. Unter Ransomware wird eine Schadsoftware verstanden, die Nutzerdaten verschlüsselt, und für deren Wiederherstellung Lösegeld, meist in Form von Bitcoins, gefordert wird. Es existieren mittlerweile zahlreiche Varianten, die unterschiedliche Verschlüsselungsalgorithmen anwenden und unterschiedlich verbreitet werden. 2019 wurden im Bundeskriminalamt 220 Fälle von Ransomware bearbeitet. Dabei konnten einige Tatverdächtige ausgeforscht werden. Als Gefahren für eine Infektion mit einem Verschlüsselungstrojaner gelten Fernzugriffe, E-Mails mit schädlichem Dateianhang oder mit Links sowie Schad-

software, Drive-by-Downloads, Supply-Chain-Attacks oder Malvertising. Nicht nur, dass bestehende Varianten ständig weiterentwickelt werden, ändern Kriminelle auch ihre Vorgehensweisen. 2019 gerieten vermehrt Unternehmen in den Fokus von Angriffen mit Ransomware. Die Geldforderungen der Täter wurden an die wirtschaftliche Leistungsfähigkeit beziehungsweise an die IT-Infrastruktur und den Back-up-Lösungen ihrer Opfer angepasst.

Darknet. Als „Crime-as-a-Service"-Leistungen im Darknet stiegen vor allem die Zahl an Massenerpressungs-E-Mails und gezielte Erpressungen durch Ransomware und Bitcoin-Forderungen an. Die Täter benötigten kein tiefgreifendes Wissen zur technischen Durchführung, sie konnten das fehlende Wissen kaufen. Mit einem „Ransomware-as-a-Service"-Modell machten die Entwickler der Schadsoftware „GandCrab" zwischen Anfang 2018 und Mitte 2019, ihren eigenen Angaben zufolge, mehr als zwei Milliarden US-Dollar Gewinn.

Online-Kindesmissbrauch. 2019 ist die Zahl der Anzeigen wegen pornografischer Darstellung Minderjähriger um 43,5 Prozent auf 1.666 Delikte angestiegen (2018: 1.161 Anzeigen). Die Zunahme ist auf die Tatsache zurückzuführen, dass die verschiedenen Anbieter von sozialen Medien in den USA und Kanada massiv gegen die Verbreitung von Daten mit Online-Kindesmissbrauch vorgehen. Dadurch werden die einzelnen Dienste auf pornografische Darstellungen Minderjähriger überprüft und der betreffende Account gesperrt. Im Anschluss erfolgt eine Verdachtsmeldung an das jeweilige Land des Tatverdächtigen.

Ausblick. Der Kampf gegen Cybercrime fängt nicht erst bei den Expertinnen und Experten im Bundeskriminalamt an, sondern bereits bei den Polizeiinspektionen, die cyberfit sein müssen. Da dieses Deliktsfeld durch ständige Veränderungen geprägt ist, bedarf es ineinandergreifender Grund-, Aus- und Weiterbildungen der Polizistinnen und Polizisten. Besonders wichtig ist, das Berufsfeld des „Cybercops" attraktiv zu gestalten, eine flächendeckende technische Infrastruktur aufzubauen und die rechtlichen Rahmenbedingungen anzugleichen. *Romana Tofan*