# BETRUG UND

**Internetbetrug, Daten-Leaks, Ransomware, DDoS-Angriffe: Die Zahl der Cybercrime-Delikte stieg 2020 um 26,3 Prozent auf 35.915 Anzeigen. Die Aufklärungsquote blieb mit 33,4 Prozent nahezu gleich.**

Cybercrime: Fast jede Kriminalitätsform hat bereits einen digitalen Aspekt.

NICOELNINO/STOCK.ADOBE.COM

Cybercrime ist ein Phänomen, das weltweit Jahr für Jahr im Steigen begriffen ist. Anonymisierungen, Verschlüsselungen, virtuelle Währungen und die ständige Verfügbarkeit des Internets haben diese Entwicklung in der Vergangenheit begünstigt. 2020 kam ein Beschleuniger hinzu: Covid-19. Der ansteigende Trend der letzten Jahre im Deliktsbereich Cybercrime hielt 2020 an. Durch die Verlagerung des Alltags in die eigenen vier Wände, Homeoffice, Home-Schooling und Online-Shopping bildete sich für Kriminelle ein Nährboden.

Zu Beginn des Jahres 2020 stieg die Zahl der Angriffe auf Computersysteme oder Netzwerke mit Hilfe von Schadsoftware neuerlich an. Zudem gelangten österreichische Unternehmen ins Visier eines Erpressers, der das Bild des Firmenchefs von der Firmenwebseite auf eine einschlägige Online-Kindesmissbrauch-Webseite kopierte und mit der Veröffentlichung der manipulierten Bilder drohte.

Für die Polizei stellten vor allem der Internetbetrug, besonders jener mit Covid-19-Bezug, Daten-Leaks, Ransomware, die Verbreitung von Remote Access Trojaner und Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe) die größten Herausforderungen in diesem Berichtsjahr dar.

**Unter Cybercrime im engeren Sinn** werden Angriffe auf Daten oder Computersysteme verstanden, die unter der Verwendung der Informations- und Kommunikationstechnik (IKT) stattfinden. Ein deutlicher Anstieg wurde beim betrügerischen Datenverarbeitungsmissbrauch (§ 148a Strafgesetzbuch) verzeichnet, denn die Zahl der Anzeigen verdoppelte sich auf über 10.000. Der Grund dafür ist nicht nur die Verlagerung des Lebens in die virtuelle Welt, sondern auch die Schaffung neuer Zahlungsmöglichkeiten. Hier nimmt die betrügerische Verwendung von Near-Field-Communication (NFC) bei Bankomat- oder Kreditkarten einen großen Anteil ein. Zudem ist die Zahl der Fälle von Phishing gestiegen. Zunahmen jenseits der 40-Prozentmarke wurden beim Missbrauch von Computerprogrammen und Zu-

# FÄLSCHUNG

gangsdaten (§ 126c StGB) und der Datenfälschung (§ 225a StGB) registriert. Der starke Anstieg der Zahl an Fällen von Datenfälschung liegt vor allem daran, dass durch die geänderten Lebensumstände während der Pandemie Rechtsgeschäfte vermehrt über das Internet abgewickelt wurden.

**Unter Cybercrime im weiteren Sinn** werden Straftaten zusammengefasst, bei denen die IKT als Tatmittel zur Planung, Vorbereitung und Ausführung eingesetzt wird, worunter die steigende Zahl an Internetbetrugsdelikten fällt. Diese erreichte 2020 mit 18.780 angezeigten Delikten einen neuerlichen Höchstwert (2019: 16.831). Eine leichte Zunahme wurde im Deliktsbereich Online-Kindesmissbrauch festgestellt (2019: 1.666 Fälle, 2020: 1.702 Anzeigen). Dank der erfolgreichen Ermittlungsarbeit wurde im Bereich Massenerpressungs-E-Mails ein deutlicher Abwärtstrend festgestellt. Wurden 2019 1.958 Fälle angezeigt, sank die Zahl 2020 auf 850 Anzeigen.

**Covid-19 als Booster.** Zu Beginn der Pandemie wurde nach der Neuregistrierung mehrerer Tausend Domains eine starke Zunahme der Zahl an betrügerischen Webseiten bemerkt, über die Phishing betrieben oder Schadsoftware verbreitet wurde. So teilte man in zahlreichen Aussendungen von Fake-E-Mails vermeintlicher Paketzustelldienste mit, dass aufgrund von Covid-19 keine Zustellungen möglich wären. Die Paketempfänger hätten nun die Möglichkeit, entweder durch den Link oder den Dateianhang die Option zum Paketempfang auszuwählen. Wenn der Link oder der Anhang geöffnet wurde, installierte sich die Schadsoftware.

**Phishing-E-Mails** und -Webseiten traten 2020 gehäufter auf. Ein besonders aufsehenerregender Fall war der Betrug mit *FinanzOnline*. Es wurden E-Mails mit der falschen Absende-E-Mail-Adresse *(finanzOnline@bmf.gv.at)* versendet, in denen eine Steuerrückerstattung von über tausend Euro versprochen wurde, man musste nur dem angegebenen Link folgen. Wurde der Link angeklickt, gelangte man auf eine Phishing-Webseite, auf der persönliche Informationen und Kreditkartendaten gefordert wurden.

**Love-Scam und Stranded Traveller.** Durch das Social Distancing gab es auch einen starken Zuwachs der Zahl an Betrugshandlungen, wie „Love-Scam“ oder „Stranded Travellers“. Bei Ersterem wird das Opfer auf Social-Media-Plattformen in eine emotionale Bindung mit der Betrügerin oder dem Betrüger verstrickt, mit dem Ziel, das Opfer finanziell auszubeuten. Beim


Grafik: Europol

Stranded-Traveller-Betrug bittet eine dem Opfer bekannte und von Kriminellen gehackte Person unter dem Vorwand um Geld, in einem anderen Land ausgeraubt worden zu sein und dadurch kein Geld für die Heimreise zu haben. In Fake-Shops, aber auch über reguläre Plattformen wurde eine Zunahme der Zahl an Fällen von Betrug mit Desinfektionsmitteln und Atemschutzmasken sowie Fake-Apps und Bank-Trojanern festgestellt.

Die Zahl der Crime-as-a-Service-Dienste nahmen im Internet ebenfalls weiter zu. Die zum Kauf angebotenen Leistungen umfassten vorwiegend Hackingtools und Schadsoftware wie Verschlüsselungstrojaner sowie Dienstleistungen zur Geldwäsche. Es konnte ein Anstieg bei der Zahl der Nutzung von Bot-Netzwerken verzeichnet werden, die für DDoS-Angriffe oder zum Versand von Spam-E-Mails genutzt werden. Weiters wurde ein vermehrtes Inverkehrbringen von Falschgeld, gestohlenen Kreditkartendaten oder gefälschten Urkunden registriert. Durch die gekauften Dienste benötigten die Täter kein fundiertes technisches Wissen mehr. Das führte dazu, dass die Zahl der Täter sowie der Opfer stieg.

**Fraud-Calls.** Betrüger nutzten die Covid-19-Pandemie, um aus den Ängsten und der Verunsicherung der Menschen Profit zu schlagen. Stromkundinnen und -kunden wurden Opfer von „Fraud Calls“ (betrügerischen Anrufen). Dadurch, dass die Täter die richtige Internationale Bankkontonummer (IBAN), die Höhe der letzten Stromrechnung und weitere Details richtig nennen konnten, schufen sie eine Vertrauensbasis. Diese wurde den Kundinnen und Kunden jedoch zum Verhängnis. Denn die Betrüger wollten die Opfer unter Vorspiegelung falscher Tatsachen zum Stromanbieterwechsel drängen.

**Cyber-Trading-Fraud.** Schäden in Millionenhöhe erlitten Opfer des Cyber-Trading-Frauds oder Investment Scams. Die Kriminellen nahmen zunächst über das Telefon, Online-Werbungen, Social Media oder E-Mails Kontakt zu ihren späteren Opfern auf. Ihnen wurden hohe Gewinne versprochen und sobald sie investierten, wurden sie zu immer höheren Investments gedrängt. Doch ihr Geld sahen die Geschädigten nie wieder.

**Beim Tech-Support-Scam** („Microsoft Betrug“) kamen auch 2020 wieder vermehrt Fälle zur Anzeige. Dabei wurden die Opfer entweder direkt telefonisch kontaktiert oder es erschien am Gerät eine Warnmeldung, dass ein Hacker in den Computer eingedrungen sei und ein zertifizierter Support zur Unterstützung für die Bereinigung zur Verfügung stehe. Das Opfer wurde

vom „Support-Mitarbeiter“ dann überzeugt, ihm vollen Zugang auf das Gerät (Computer, Smartphone, Tablet) zu erteilen, wodurch der Täter nicht nur die Daten der oder des Geschädigten stehlen konnte, sondern auch mit einer Sperre des Endgerätes drohte, sollte die Gebühr nicht bezahlt werden.

**SIM-Swap-Betrug.** Das *Cybercrime-Competence-Center (C4)* im Bundeskriminalamt nahm Ermittlungen zu 65 Fällen von SIM-Swapping auf. Hierbei verschafft sich der Täter zunächst personenbezogene Daten über das künftige Opfer, denn SIM-Swapping setzt in der Regel die Kenntnis von Name, Mobiltelefonnummer und anderer Daten wie Adresse oder Zugangsdaten zum Online-Portal des Mobilfunkbetreibers voraus. Diese Informationen erlangen die Kriminellen oft durch Social Engineering, wie etwa Phishing-Mails, oder sie erwarben die Daten. Dadurch konnten sich Betrüger beim Mobilfunkanbieter als Opfer ausgeben und eine neue SIM-Karte ordern. Die Telefonnummer kann auf die neue SIM-Karte übertragen werden. Dadurch ist der Betrüger imstande, alle eingehenden Anrufe und Textnachrichten zu empfangen, einschließlich der Einmalpasswörter für Banken, die an die Telefonnummer des Opfers gesendet werden. Der Täter ist so in der Lage, durch den Erhalt des Einmalpassworts per SMS, Banktransaktionen abschließen.

**Klärung von 26 Kraftfahrzeugdiebstählen.** Bei einer Schwerpunktaktion, an der Experten der Kfz-Forensik des *Cybercrime-Competence-Centers* mit dem Landeskriminalamt Niederösterreich zusammenarbeiteten, wurden zwölf Mitglieder einer polnischen Tätergruppe ausgeforscht und gefasst, die 26 vollendete und fünf versuchte *Audi*-Diebstähle in Niederösterreich begangen hatten. Die Schadenssumme belief sich auf 670.000 Euro. Den Ermittlern gelang es, zehn gestohlene Pkws im Wert von 285.000 Euro sicherzustellen. Sechs der zwölf Täter befinden sich in Österreich, einer in Deutschland sowie zwei weitere in Polen in Haft. Zwei der Täter wurden bereits zu mehrjährigen Freiheitsstrafen verurteilt.

**Prävention.** Zum Start des „Europäischen Monats für Cyber-Sicherheit“ im Oktober veröffentlichte Europol

**SIM-Swap-Betrug: Mit betrügerisch erlangten SIM-Karten können Kriminelle Anrufe, Textnachrichten und Passwörter des rechtmäßigen Besitzers erlangen.**

und dessen Partner eine Aufklärungskampagne. Ziel war es, die Bürgerinnen und Bürger über die unterschiedlichsten Formen von Internetkriminalität aufzuklären und zu sensibilisieren. Da sich der gewohnte Alltag durch die Pandemie stark veränderte und das Leben hauptsächlich in den eigenen vier Wänden stattfand, bieten drei Infografiken von Europol hilfreiche Tipps, um das Zuhause vor Cyber-Angriffen zu sichern. Dazu gehören nicht nur der richtige Schutz des WLANs oder der Endgeräte, sondern auch Sicherheitsratschläge zum Thema Onlineshopping und Cyber-Sicherheit der Kinder.

Hinweise zur sicheren Telearbeit sollen nicht nur die Nutzerinnen und Nutzer davor schützen, Opfer eines Cyber-Angriffs zu werden, sondern auch Unternehmen über die Risiken aufklären und Tipps zur Absicherung geben.

**Ausblick.** Die Kriminalpolizei will Cybercrime in all seinen Erscheinungsformen noch effektiver bekämpfen. Ein wichtiges Thema ist auch der Umgang mit großen Datenmengen, die, bedingt durch die immer größer werdenden Speichermedien immer mehr Ressourcen bei der Sicherung und Analyse benötigen. Die Vernetzung mit externen Partnern, wie wissenschaftlichen Einrichtungen wird vorangetrieben.

**Cybercrime-Abteilung**. Das *Cybercrime-Competence-Center* wird zu einer eigenen Abteilung ausgebaut, in der sich 120 Expertinnen und Experten auf aktuelle und künftige Phänomene spezialisieren, wobei die nationale und internationale Arbeit im Fokus steht.

Um auch auf internationaler Ebene vertreten zu sein, wurde ein Spezialist zu Europol entsandt, damit eine schnelle und technisch kompetente Informationsweitergabe bei operativen Fällen gewährleistet wird. Zudem ist der weitere Ausbau des „Cybercrime-Experts-Circle“ des C4 geplant, der als Plattform aufgebaut wurde, um praktisch anwendbares Wissen mit Expertinnen und Experten aus Partnerländern zu teilen. Da die Bekämpfung von Cybercrime nicht erst im Bundeskriminalamt anfängt, sondern auf Landes- und Bezirksebene, soll es auch auf diesen Ebenen eine personelle Verstärkung geben.

**Cyber-Kriminelle** setzen ein aktives Handeln des Opfers voraus, denn ohne einen heruntergeladenen Anhang, ohne ein ausgefülltes Datenblatt oder ohne einen angeklickten Link haben es Täter nicht einfach, Menschen zu schädigen. Daher ist die Sensibilisierung der Bevölkerung und die Schaffung eines Sicherheitsbewusstseins von großer Bedeutung. *Romana Tofan*

FOTO: PHEELINGSMEDIA/STOCK.ADOBE.COM