ANGRIFFE, BETRU

Der Cybercrime-Report zeigt wieder eine signifikante Steigerung der Zahl der Anzeigen: 65.864 Delikte wurden 2023 registriert, eine Zunahme von 9,4 Prozent im Vergleich mit 2022.

Cyber-Kriminalität: Seit Jahren der am stärksten wachsende Bereich in der Kriminalstatistik

Die Cyber-Kriminalität ist seit Jahren der am stärksten wachsende Bereich in der polizeilichen Anzeigenstatistik und ist eine der größten Herausforderungen für die Sicherheit Österreichs, da sich das Internet durch die Digitalisierung zunehmend als Tatort entwickelt hat. 2023 wurde eine neuerliche Steigerung der Zahl der angezeigten Delikte von 9,4 Prozent im Vergleich zum Vorjahr registriert (2023: 65.864, 2022: 60.195). Seit 2019 hat sich die Internetkriminalität mehr als verdoppelt (2019: 28.440). Die Aufklärungsquote lag im Berichtsjahr bei 31,6 Prozent.

Die Herausforderungen, Daten und Infrastruktur zu schützen, um die Sicherheit in der digitalen Welt zu garantieren, wachsen ständig, weshalb neben repressiven präventive und strategische Maßnahmen nötig sind. In der Kriminaldienstreform wird dieser Bereich technisch, organisatorisch und personell aufgerüstet. Die Einrichtung von Cybercrime-Trainingscenters oder der Ausbau von Ausbildungskooperationen sind wichtige Maßnahmen im Kampf gegen internationale Cybercrime-Gruppierungen. Weitere Schwerpunkte liegen in der Verstärkung der internationalen Zusammenarbeit mit anderen Strafverfolgungsbehörden.

Cybercrime im engeren und weiteren Sinne. Cybercrime im engeren Sinne umfasst kriminelle Handlungen, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnologie (IKT) begangen werden. Die Zahl der Anzeigen in diesem Bereich ging um 6,4 Prozent zurück, was auf eine geänderte statistische Erfassung zurückzuführen ist. Die zunehmende Digitalisierung führt dennoch zu einem Anstieg der strafbaren Handlungen in diesem Bereich. Wenn die IKT zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt wird, spricht man von Cybercrime im weiteren Sinne. Der Internetbetrug stellt den größten Bereich dar und ist maßgeblich für den Anstieg der Deliktszahlen verantwortlich. Organisierte Tätergruppen nutzen technische Anonymisierungen und Verschleierungen der Finanzflüsse, um Betrugshandlungen unerkannt durchzuführen. Die Verlagerung von Straftaten ins Internet und die Nutzung von Crime-as-a-Service-

FOTO: ACRONYM - STOCK.ADOBE.COM

UG, ERPRESSUNG

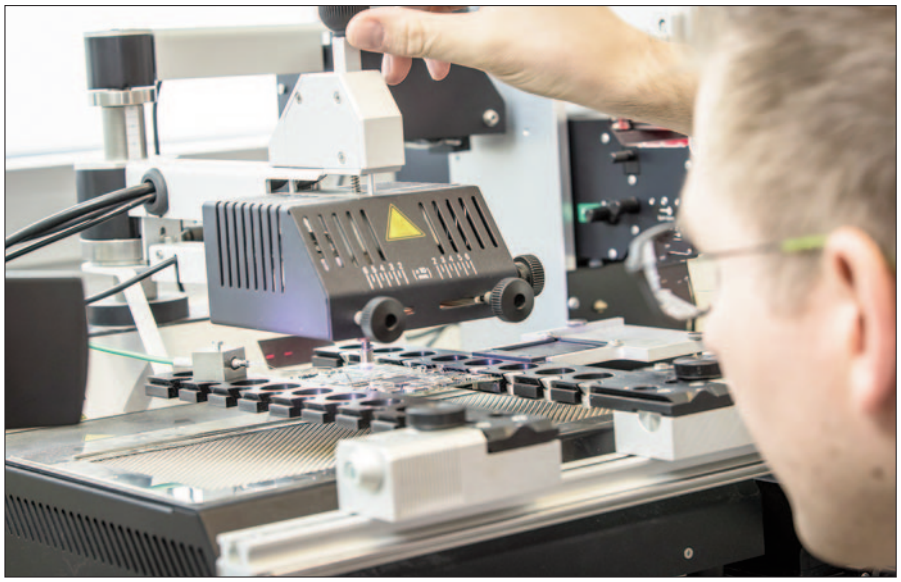
Diensten im Darknet hat ebenfalls zugenommen.

Auszuwertende Datenmengen nehmen stark zu. Die Arbeit der Forensiker des *Cyber-Crime-Competence-Centers (C4)* spielt bei strafrechtlichen Ermittlungen eine wesentliche Rolle. Der elektronischen Beweismittelsicherung im *C4* und den Landeskriminalämtern kommt eine maßgebliche Bedeutung in den Ermittlungen zu. Aufgrund der technischen Entwicklungen und der Zunahme an Speicherplatz, nimmt auch das Volumen an Daten zu, die nach Sicherstellungen ausgewertet werden müssen. So belief sich die Gesamtmenge an sichergestellten Daten auf 1.572 Terabyte. Nicht nur die Menge an auszuwertendem Material stellt eine Herausforderung dar, sondern auch die eingesetzten Schutzmechanismen der Hersteller, was die Datensicherung und Auswertung komplexer gestaltet.

Internetbetrug bleibt eines der häufigsten und am stärksten wachsenden Cybercrime-Delikte. Die Täter nutzen das Internet zur Anbahnung und Ausführung der Tat. Die Betrugsarten sind vielfältig und umfassen unter anderem betrügerische Anrufe, falsche Gewinnversprechen, betrügerische Investitionsangebote, Love-Scams, Phishing-Attacken und betrügerische Aktivitäten im Onlinehandel. Organisierte Tätergruppen nutzen die Anonymität des Internets und erreichen mit minimalem Aufwand eine große Anzahl potenzieller Opfer, was zu finanziellen Verlusten führt. 2023 wurden 34.069 Fälle von Internetbetrug gemeldet, was einem Anstieg von 23,3 Prozent gegenüber 2022 entspricht. Die Aufklärungsquote sank um 4,8 Prozentpunkte, was auf die Verschleierungsmethoden der Täter zurückzuführen ist.

Zur Bekämpfung dieser Delikte setzt das Bundeskriminalamt sowohl auf präventive als auch auf repressive Maßnahmen. Zum einen wird die Öffentlichkeit über Betrugsphänomene informiert und sensibilisiert und zum anderen steht die internationale Kooperation im Fokus. Mit der Einrichtung des datenbankgestützten Lagebilds Betrug setzte das Bundeskriminalamt einen weiteren Meilenstein.

20 Millionen Euro Schaden. Ein häufiges Phänomen ist der „falsche Polizist“. Hier werden vorwiegend ältere Menschen Opfer von Kriminellen. Die Täter versuchen, mit überzeugenden Geschichten das Vertrauen der Opfer zu gewinnen und fordern sie auf, Wertgegenstände und Bargeld zum eigenen Schutz an einen „Kollegen“ zu übergeben. 2023 verursachten Betrüger mit diesem Modus Operandi einen Schaden von knapp 20 Millionen Euro. Da sich diese Betrugsmasche vorwiegend gegen ältere Personen richtet, wurde ein



Die Arbeit der Forensiker des Cyber-Crime-Competence-Centers (C4) im Bundeskriminalamt spielt bei strafrechtlichen Ermittlungen eine wesentliche Rolle

Internetbetrug bleibt das am stärksten wachsende Cybercrime-Delikt

Präventionsmodell entwickelt, das in Zusammenarbeit mit der Wirtschaftskammer Österreich, den Banken und dem Seniorenrat Österreich bei einer *Gemeinsam.Sicher*-Aktion vorgestellt wurde.

Kryptowährungen, vor allem Bitcoin, spielen bei vielen Straftaten – vor allem Erpressungs- und Betrugsdelikten – zunehmend eine Rolle. Die Ermittlungen gestalten sich aufgrund der enormen Anzahl an Blockchains und den ständigen Weiterentwicklungen herausfordernd. Fast täglich werden neue Währungen geschaffen, die den Nutzerinnen und Nutzern von hoher Anonymität bis zu niedrigen Transaktionsgebühren alles bieten. Regelmäßige Weiterbildungen in diesem Bereich sowie eine gute internationale Kooperation und ein laufender Austausch von Informationen und Erkenntnissen ist daher für Ermittlungserfolge entscheidend.

Pig-Butchering – Liebes- und Investmentbetrug. Ein aktueller Modus Operandi ist das „Pig-Butchering“ in Kombination mit dem klassischen Love-Scamming. Hierbei wird über Wochen und Monate eine freundschaftliche oder Liebes-Beziehung zu den Opfern aufgebaut, um sie finanziell auszunutzen. Die Kriminellen bewerben dabei eine Kryptoinvestitions-Website, auf der sie angeblich hohe Renditen erwirtschaftet hätten. Sobald das Vertrauen der Opfer gewonnen ist, werden diese dazu gebracht, immer größere Summen zu investieren. Wenn die Opfer misstrauisch werden oder keine weiteren Zahlungen leisten können, schränken die Betrüger

INTERNETBETRUG

Präventionstipps

• Wenn Sie im Internet etwas verkaufen, geben Sie ausschließlich die für die Bezahlung durch den Käufer notwendigen Daten bekannt (Empfängername, IBAN, allenfalls BIC) oder verwenden Sie auf der Plattform angebotene sichere Zahlungsmethoden (z. B. PayLivery von willhaben).
• Wenn sich ein „Familienmitglied“ unter einer neuen Telefonnummer mit Forderungen nach Geld an Sie wendet, handelt es sich zumeist um Betrug. Verwenden Sie ausschließlich die Ihnen bisher bekannten Kontaktdaten oder versuchen Sie die Kontaktaufnahme über Ihnen bekannte Freunde oder Social-Media-Kontakte und hinterfragen Sie die Forderung. Stellen Sie allenfalls Fangfragen, die nur Ihr echtes Familienmitglied richtig beantworten kann.
• Wenn Sie beim Kauf und Verkauf von Waren über das Internet, insbesondere bei höherwertigen Gütern und Fahrzeugen, aufgefordert werden, Kosten wie Transportversicherung, Zoll und dergleichen zu übernehmen, handelt es sich zumeist um eine Betrugsmasche. Im Voraus bezahltes Geld ist zumeist aussichtslos verloren (Vorschussbetrug).
• Wenn Sie bei Bezahlvorgängen nach einem Verkauf im Internet eine „Autorisierungsnachricht“ Ihres Bankanbieters erhalten, ist das eine Fälschung. Wenn Sie die Bankverbindung bestätigen, geben Sie dabei in den meisten Fällen eine (unerwünschte und schädigende) Zahlung frei.
• Wenn ein Angebot zu gut klingt, um wahr zu sein, dann seien Sie skeptisch. Das gilt nicht nur für Einkäufe im Internet, sondern auch für Investment-Angebote. Achten Sie auf die Seriosität derartiger Werbungen und bedenken Sie die Möglichkeit von KI-generierter Fake-Werbung.
• Ist ein Schaden entstanden, verständigen Sie sofort Ihr Bankinstitut oder Ihren Kreditkartenanbieter und ersuchen Sie um Rückbuchung. Sperren Sie Ihr Konto und/oder Ihre Kreditkarte und erstatten Sie Anzeige bei der nächsten Polizeidienststelle. Nehmen Sie allenfalls Kontakt mit der jeweiligen Verkaufsplattform auf, berichten Sie das Geschehene und Ersuchen Sie, mögliche elektronische Spuren für die polizeilichen Ermittlungen vorab zu sichern und Ihnen oder der Behörde zur Verfügung zu stellen.
• Weitere Tipps und Informationen zur Anzeigenerstattung finden Sie auf der Webseite des Bundeskriminalamtes: *www.bundeskriminalamt.at*

FOTOS: GERD PACHAUER, FIZKES - STOCK.ADOBE.COM

Cybercrime: Wer Opfer eines digitalen Delikts geworden ist, sollte das in der nächsten Polizeiinspektion anzeigen

den Zugang zu den Geldern ein und starten Erpressungsversuche.

Auftragsmord über das Darknet. Im März 2023 wurde das Landeskriminalamt (LKA) Niederösterreich von einer ausländischen Dienststelle über einen Versuch zur Vergabe eines Auftragsmordes im Darknet informiert.

Unter dem Pseudonym „Sunnyboy" versuchte ein Mann, einen Auftragsmörder zur Ermordung einer Frau in Niederösterreich zu finden. Erste Zahlungen waren bereits mittels Kryptowährungen erfolgt. Die Polizei forschte das Opfer aus und brachte es in Sicherheit. Für die weiteren Ermittlungen wurden die Fachbereiche Darknet- und Blockchain-Ermittlungen des *C4* hinzugezogen. Durch das technische Know-how des Täters und die Verschleierungsmaßnahmen waren die Ermittlungen aufwendig. Den Ermittlerinnen und Ermittlern gelang es, den Täter zu identifizieren und festzunehmen.

Phishing. Auch die Zahl von Phishing-E-Mails und -Webseiten ist 2023 gestiegen. Diese zielen darauf ab, persönliche Daten sowie Bezahldaten zu stehlen, um diese missbräuchlich zu verwenden. Alle größeren Finanz-, Transport-, Verkaufs- und Unterhaltungsdienstleister in Österreich waren im Berichtsjahr Gegenstand von Phishing-Mails. Eine besondere Gefahr beim Aufruf von Phishing-Webseiten stellt der Download von angeblichen Rechnungsdokumenten oder sonstigen Programmen für Mobilgeräte dar, es handelt sich oft um Schadsoftware, die mobile TANS für das Online-Banking abgreifen oder gleich die komplette Überweisung umleiten. 2023 traten vermehrt Phishing-Wellen auf: Es kursierten mehrere Spam-SMS-Kampagnen, die einen Hinweis auf eine angebliche Zustellbenachrichtigung und weiterführende Links enthielten. Die Vorweihnachtszeit ist die Blütezeit für Phishing-Mails von Versandunternehmen, sowie der Installation von Schadsoftware nach dem Download von Rechnungen und/oder Bestellbestätigungen (Fake-Pdfs, die ein Programm sind und Trojaner installieren).

Bei Ransomware handelt es sich um Schadsoftware, die für das Kopieren und verschlüsseln von Daten verwendet wird, um das Opfer mit den verschlüsselten Daten oder der Veröffentlichung der kopierten Daten zu erpressen. Waren Ransomware-Angriffe in der Vergangenheit breiter gestreut, so finden diese nunmehr gezielt gegen Unternehmen, kritische Infrastruktur bis hin zu Organisationen und Behörden statt. Der Ursprung eines solchen Angriffs findet sich oft in Sicherheitslücken der verwendeten Systeme und Programme, aber auch im nicht sorgsamen Umgang mit unbekannten Mail-Inhalten und heruntergeladenen „Fake"-Dateien (Rechnungen als Pdfs getarnt).

Ransomware-Angriffe auf Unternehmen richten weltweit große Schäden an und stellen aufgrund der zunehmenden Qualität der Angriffe die Polizei vor Herausforderungen. 2023 wurden 148 Fälle in Österreich angezeigt. Über ein Drittel der Angriffe fand auf Unternehmen statt, wobei es keine bestimmten Zielbranchen gab. Insgesamt konnten 35 unterschiedliche Angreifer identifiziert werden, wobei „Lock-Bit" in verschiedenen Ländern als aktivster genannt wird.

Laut dem Crypto-Crime-Report 2024 der Analysefirma Chainalysis wurde 2023 weltweit mehr als eine Milliarde Dollar an Lösegeld gezahlt. Der Schaden ist viel höher, wenn man die wirtschaftlichen Auswirkungen einrechnet, wie etwa Produktionsverluste und Reparaturkosten.

Erfolgreiche Zusammenarbeit. Die international agierende Gruppe „Lock-Bit" zeichnete für den Angriff auf acht österreichische Unternehmen verantwortlich und wurde Gegenstand der Ermittlungen des Referats IT-Ermittlungen des *C4* im Bundeskriminalamt. Nachdem auch gleichartige Fälle in anderen Ländern auftraten, schlossen sich Verbindungsbeamte von Österreich und Japan bei Europol zu einer Joint-Cybercrime-Action-Taskforce (J-CAT) zusammen. Japanische Cyber-Ermittler waren für eine Woche im *C4* in Wien zu Gast. Sie tauschten Erfahrungen aus und entschlüsselten einen erheblichen Teil des Datenmaterials, wodurch ein größerer Schaden verhindert werden konnte.

Kriminaldienstreform und zukünftige Herausforderungen. Die größte Polizeireform der letzten Jahrzehnte wird rund 700 neue Arbeitsplätze umfassen, davon 300 zur Bekämpfung von Cybercrime und der organisierten Kriminalität. Das *C4* wird zu einer eigenen Abteilung im Bundeskriminalamt, um Herausforderungen zu meistern, wie die fortschreitende Digitalisierung, die Entwicklung neuer krimineller Methoden und die Notwendigkeit einer ständigen Weiterentwicklung der technischen und personellen Ressourcen.

Durch die fortlaufende Weiterentwicklung und Fortbildung in diesem Bereich strebt die Polizei an, den Kriminellen entgegenzutreten. Die Bevölkerung soll durch verstärkte Präventionsmaßnahmen die Möglichkeit erhalten, sich vor Kriminalität im digitalen Raum zu schützen. *Romana Tofan*

FOTO: GERD PACHAUER