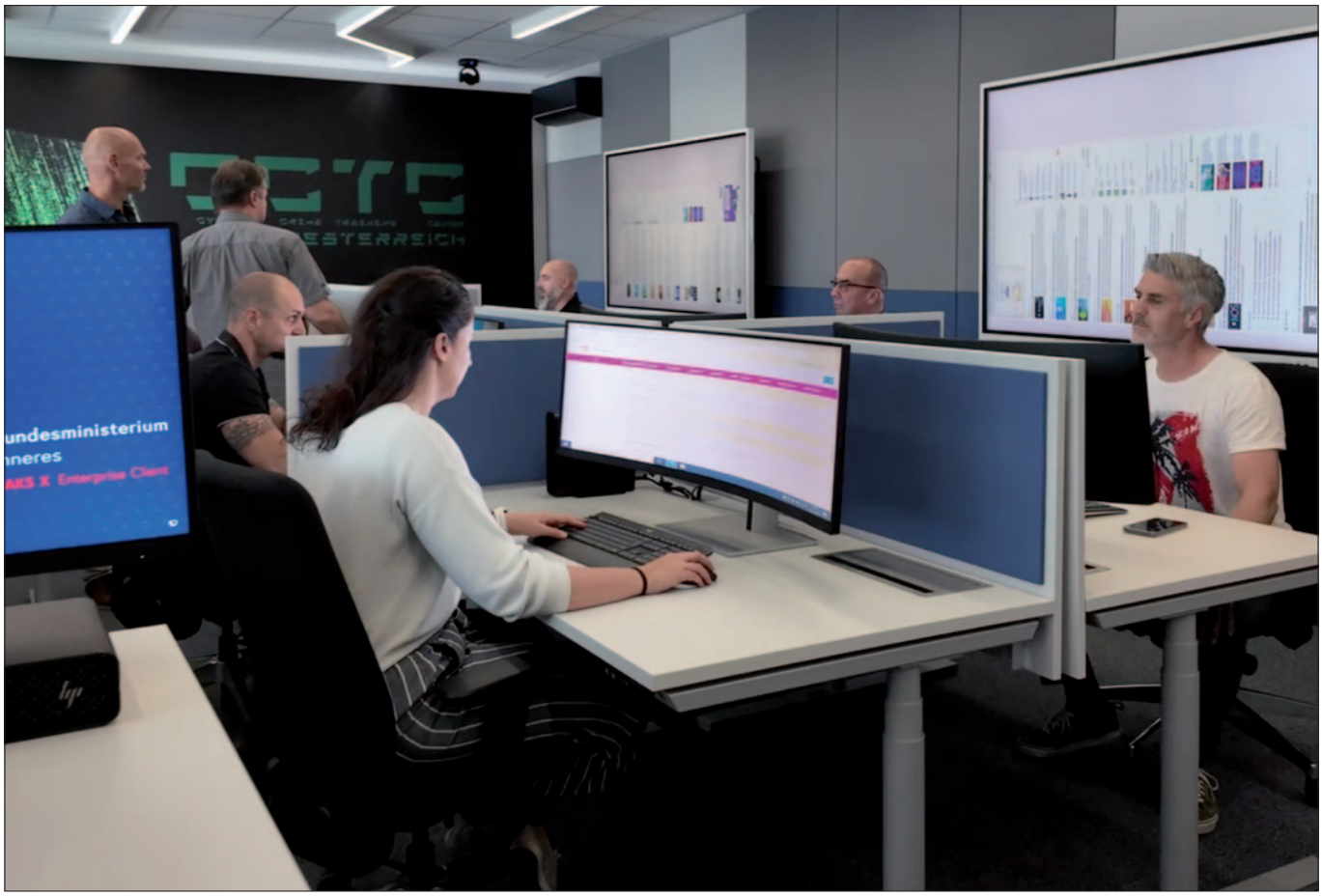


Kriminaldienstreform: einer der Schwerpunkte ist der Kampf gegen die Cyber-Kriminalität

Cybercrime auf hohem Niveau

Die Zahl der Cybercrime-Delikte sank zwar 2024 leicht, aber die Gesamtzahl der Straftaten bleibt auf einem hohen Niveau. Eine Herausforderung stellt die rasant wachsende Menge an digitalen Daten dar, die von den Ermittlungsbehörden gesichtet und ausgewertet werden müssen.

Cyber-Kriminalität ist eine Bedrohung für die Sicherheit in Österreich. Während im Jahr 2024 erstmals seit einem Jahrzehnt ein leichter Rückgang der Anzeigenzahl verzeichnet werden konnte, bleibt die Gesamtzahl der Straftaten auf einem hohen Niveau. Die Entwicklungen zeigen: Cybercrime ist ein dynamisches Feld, das sich ständig verändert und nicht nur die Ermittlungsbehörden, sondern auch die Gesellschaft vor Herausforderungen stellt.

„Internetkriminalität gehört nach wie vor zu den großen Herausforderungen für die Polizei in Österreich. Durch die Einrichtung von Kriminalassistenzdienststellen in den Bundesländern stehen Spezialisten im Bereich der Prävention, aber auch bei der Aufklärung von Straftaten den Menschen in den Regionen zur Verfügung“, sagt Innenminister Gerhard Karner.

Weniger Anzeigen. 2024 wurden 62.328 Straftaten zur Anzeige gebracht. Das bedeutet einen Rückgang um 5,4 Prozent im Vergleich mit dem Jahr davor (2023: 65.864). Auch wenn dieser Wert den niedrigsten der vergangenen zehn Jahre markiert, bewegt sich die Zahl der Anzeigen auf einem hohen Niveau: Wurden 2015 10.010 Delikte angezeigt, hat sich die Anzahl ein Jahrzehnt später mehr als versechsfacht.

Die Aufklärungsquote ist im Vergleich mit dem Vorjahr um 0,1 Prozentpunkte auf 31,7 Prozent gestiegen. Bei der Cybercrime-Meldestelle blieben die Eingänge mit über 15.000 Meldungen 2024 auf hohem Niveau.

Eine Herausforderung in der Cybercrime-Bekämpfung stellt die rasant wachsende Menge an digitalen Daten dar, die von den Ermittlungsbehörden gesichtet und ausgewertet werden müssen. In der elektronischen Beweismittelsicherung im *Cybercrime-Competence-Center (C4)* des Bundeskriminalamtes und in den Landeskriminalämtern wurden 2.075 Terabyte Daten im Berichtsjahr ausgewertet. Im Vergleich: 2023 belief sich die Menge noch auf 1.572 Terabyte.

Rückgang bei Cybercrime im engeren Sinn. Bei Cybercrime im engeren Sinn – also Angriffe, die sich direkt gegen Informations- und Kommunikationssysteme richten – wurde 2024 mit 20.246 Fällen ein Rückgang um 3,4 Prozent im Vergleich zum Vorjahr registriert. Die Zahl der Anzeigen wegen widerrechtlichen Zugriffs auf Computersysteme stieg von 1.858 auf 1.991 Fälle. Auch beim Missbrauch von Computerprogrammen oder Zugangsdaten gab es ei-

FOTO: RALF LORBEG

KI – insbesondere zur Erstellung von Deep Fakes – stellt eine neue Herausforderung für die Polizei dar

Screenshot: Metropolitan Police, FAMILY STOCK – stock.adobe.com

ne Zunahme von 305 auf 496 Anzeigen. Die Zahl an Datenbeschädigungen ging von 308 auf 241 Fälle zurück. Cybermobbing blieb mit 462 Anzeigen nahezu gleich.

Internetbetrug als Herausforderung. Im Berichtsjahr machten Betrügereien mit 31.768 Fällen wieder den größten Anteil der Anzeigen aus. Hier wurde zwar ein Rückgang von 6,8 Prozent gegenüber 2023 registriert, dennoch macht dieses Delikt mehr als die Hälfte aller Cybercrime-Straftaten aus. Besonders stark vertreten sind der Bestellbetrug und unbefugte Abbuchungen von Bankkonten. Durch den Einsatz minimaler Ressourcen können kriminelle Gruppen eine große Anzahl Opfer schnell und einfach erreichen, wodurch hohe finanzielle Gewinne erzielt werden können. 2024 wurde ein starker Anstieg der Zahl bei komplexen Fällen von Investitionsbetrugsformen registriert, besonders beim Cyber-Trading-Fraud, der im Berichtsjahr Schäden von 120 Millionen Euro verursachte.

Ebenso stellt der Einsatz von künstlicher Intelligenz – insbesondere zur Erstellung von Deep Fakes und zur Automatisierung komplexer Betrugsmodelle – eine neue Herausforderung dar. Phishing-Angriffe per E-Mail oder SMS waren ebenfalls ein beliebter Modus Operandi.

Neben den klassischen Phishing-Versuchen, die auf Bankkunden oder Kreditkarteninhaber abzielten, wurden vermehrt Angriffe auf Kunden alternativer Online-Zahlungsdienstleister sowie Inhaber von Kryptobörsen-Konten verzeichnet.

„Lab-Host“. Die internationale Ermittlungsoperation gegen die Phishing-Plattform „Lab-Host“ gilt als Erfolg in der Bekämpfung von Cybercrime im Jahr 2024. Lab-Host war als „Phishing-as-a-Service“-Modell organisiert und eine der weltweit größten Anbieter auf diesem Sektor. Den Nutzern wurde gegen eine monatliche Gebühr eine professionelle Infrastruktur angeboten und täuschend echte Phishing-Seiten zur Verfügung gestellt, die unter anderem Banken, Post- und Telekommunikationsunternehmen imitierten. Zusätzlich konnten die Täter mit interaktiven Tools direkt mit ihren Opfern kommunizieren, um diese zum Eingeben von sensiblen Daten wie Passwörtern oder Kreditkarteninformationen zu bewegen.

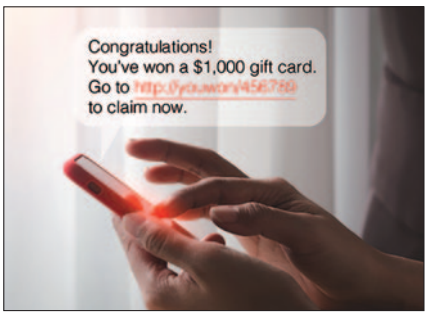
Auf der Plattform „Lab-Host“ wurden gefälschte Websites und andere Dienste für Phishingversuche angeboten

Strafverfolgungsbehörden aus 19 Ländern haben in der einjährigen Operation, die von Europol koordiniert wurde und an der auch *das Cybercrime-Competence-Center (C4)* des Bundeskriminalamtes teilnahm, die Infrastruktur von Lab-Host offengelegt. Die Ermittlerinnen und Ermittler konnten nachweisen, dass über 40.000 Phishing-Domains mit Lab-Host verknüpft waren und rund 10.000 Nutzer das Service regelmäßig in Anspruch nahmen.

Die Professionalität spiegelte sich im Geschäftsmodell wider: Für 249 US-Dollar pro Monat erhielten Krimi-

nelle Zugang zu illegalen Diensten, die individuell anpassbar und mit wenigen Klicks einsatzbereit waren. Weltweit wurden 70 Objekte durchsucht und 37 Verdächtige festgenommen, darunter die mutmaßlichen Betreiber.

Entwicklungen. In der sonstigen Kriminalität im Internet zeigte sich ein deutlicher Anstieg: 5.370 Fälle wurden angezeigt, ein Plus von über 16 Prozent (2023: 4.609). Hierzu zählen unter anderem gefährliche Drohungen (§ 107 StGB, von 1.209 auf 1.472), Verhetzung (§ 283 StGB, von 135 auf 309 Anzeigen) und Verstöße gegen das Verbotsgesetz, die von 729 auf 1.222 stiegen. Bei der Online-Erpressung zeigt die Statistik eine deutliche Veränderung: 2024 wurden 2.931 Fälle von Online-Erpressungen angezeigt – ein Rückgang von 25 Prozent. Gleichzeitig stieg die Aufklärungsquote von 5 auf 7,8 Prozent. Die Tätergruppen setzen weiterhin auf Sextortion-Mails und gefälschte Polizeimitteilungen, in denen Geldzahlungen gefordert werden. Trotz der positiven Entwicklung bleibt dieses Delikt ein lukratives Geschäftsmodell für internationale Tätergruppen.

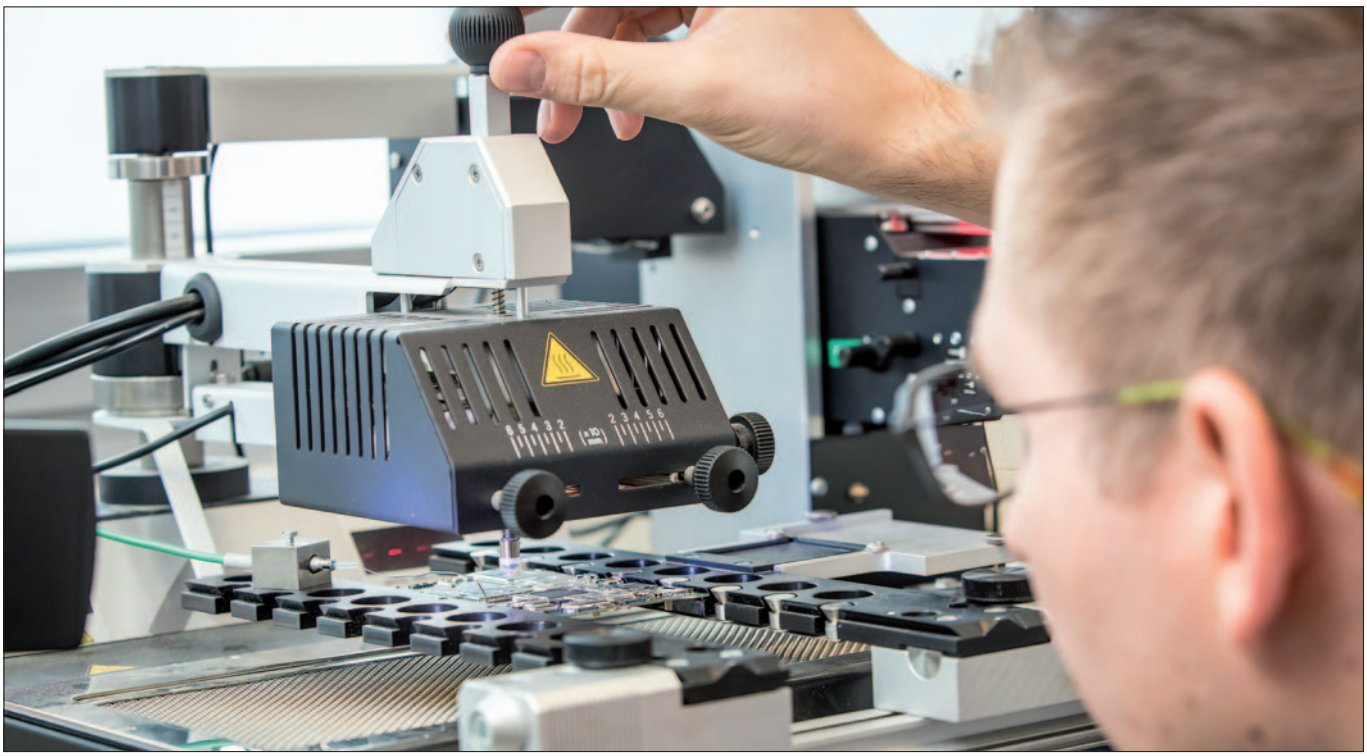


Internetbetrug macht mehr als die Hälfte aller Cybercrime-Straftaten aus

Mehr Anfragen an Online-Plattformen. Die zentrale Anfragestelle für Social Media und Online-Service-Provider (ZASP) hat sich 2024 erneut als unverzichtbares Bindeglied zwischen den Ermittlungsbehörden und Internetplattformen erwiesen. Im Berichtsjahr stieg die Zahl der Anfragen weiter an: 3.343 Anträge wurden über ZASP abgewickelt und dabei 5.432 Accountanfragen gestellt (2023: 3.331 Anträge; 4.913 Accountanfragen). Zu den Tatbeständen zählten Betrug (3.043), Erpressung (970), Nötigung/gefährliche Drohung (268), Cybercrime im engeren Sinn (221) und Verletzung der sexuellen Integrität (143). Durch die Zentralisierung und Vereinheitlichung der Anfragen wurde die Antwortquote gesteigert. So langten im Berichtsjahr von *Facebook* zu 84 Prozent, *Instagram* zu 88 Prozent, *WhatsApp* zu 89 Prozent, *Microsoft* zu 78 Prozent und von *Tiktok* zu 63 Prozent ein Ergebnis auf eine Accountanfrage ein.

Rekordhoch bei NCMEC-Verdachtsmeldungen. Besonders sensibel ist der Bereich des sexuellen Missbrauchs von Kindern im Internet. Im Jahr 2024 gingen beim Bundeskriminalamt 18.276 Verdachtsmeldungen von US-Internet-Service-Providern ein – ein Wert, der den letztjährigen Spitzenwert in der Kooperation zwischen dem *National Center for Missing & Exploited Children (NCME)* und dem Bundeskriminalamt um 2.400 Meldungen übersteigt. Gleichzeitig ist die Zahl der Anzeigen nach § 207a StGB (bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellungen minderjähriger Personen) erstmals gesunken: von 2.245 auf 1.889 Fälle. Die Aufklärungsquote liegt mit 92,8 Prozent weiterhin auf hohem Niveau. Neu in den Fokus rückte das Phä-

FOTO: TETE_ESCAPE - STOCK.ADOBE.COM/ER



Elektronische Beweismittelsicherung: Im Bundeskriminalamt und in den Landeskriminalämtern wurden 2.075 Terabyte Daten 2024 ausgewertet

nomen des „Long-Distant-Child-Abuse“. Hier beauftragen Täter aus Österreich über das Internet den Missbrauch von Kindern im Ausland und verfolgen die Taten per Livestream. Ermittlungen führten 2024 unter anderem zur Identifizierung von 15 minderjährigen Opfern auf den Philippinen und zur Festnahme eines österreichischen Täters.

Online-Suchtmittelhandel. Der Handel mit illegalen Suchtmitteln über das Internet hat sich in den vergangenen Jahren zu einem Dauerbrenner der organisierten Kriminalität entwickelt. Während in der Vergangenheit vor allem Darknet-Marktplätze genutzt wurden, zeigt sich in jüngster Zeit eine Verschiebung in das Clearnet sowie in verschlüsselte Messengerdienste und soziale Netzwerke. Im Berichtsjahr wurden in Österreich 1.416 Postsendungen mit Bezug zu Suchtmitteln sichergestellt. Es wird angenommen, dass ein erheblicher Teil der Lieferungen aus den Niederlanden stammt, auch wenn sie oftmals über Deutschland weitergeleitet werden, um die Herkunft zu verschleiern.

Deaddrop. Neben dem Versand per Post kommt eine neue Methode immer öfter vor: der „Deaddrop“. Hierbei werden Suchtmittel nicht mehr verschickt, sondern an geheimen Orten im öffentlichen Raum deponiert. Die Käufer erhalten die GPS-Koordinaten und können die Ware dort anonym abholen.

Ransomware-Angriffe blieben 2024 Thema. Mit 109 gemeldeten Fällen sank die Zahl zwar, dennoch verursachten die Angriffe erhebliche Schäden. Besonders aktiv war die Gruppe „Lock-Bit“, bei mehr als einem Drittel der Anzeigen konnte keine spezifische Gruppierung erkannt werden, was die Ermittlungen erschwerte. 90 Prozent der Angriffe fand auf Unternehmen statt. Hier wurde keine bestimmte Zielbranche identifiziert. 29 unterschiedliche Akteure wurden als Angreifer identifiziert. *R. T.*

KRIMINALPRÄVENTION

Schutz vor Cybercrime

• Seien Sie misstrauisch! Hinter Versprechungen und verlockenden Angeboten stecken meist betrügerische Absichten.
• Schützen Sie Computer und Handy. Halten Sie Ihre Geräte, Systeme und Programme wie z. B. Betriebssystem, Firewall immer auf aktuellem Stand.
• Sichern Sie Ihre Datenübertragung! Verwenden Sie verschlüsselte Internetseiten. Sie erkennen diese an einem Schloss-Zeichen in der Adressleiste. Meiden Sie öffentliches WLAN.
• Wählen Sie sichere Passwörter! Wählen Sie lange Passwörter mit Sonderzeichen und Zahlen oder verwenden Sie Passwortmanager. Halten Sie Ihre Passwörter geheim.
• Sichern Sie regelmäßig Ihre Daten! Wichtige Daten sollten Sie mittels Backup-Software auf externe Festplatten oder Datenträgern sichern. Trennen Sie diese danach vom System.
• Folgen Sie keinen Zahlungsaufforderungen.
• Öffnen Sie keine Links oder Anhänge von unbekannten Absendern.
• Brechen Sie sofort jeglichen Kontakt mit Erpressern ab und blockieren Sie diese, wenn möglich, im sozialen Netzwerk. Melden Sie die Fake-Accounts an die Seitenbetreiber.
• Sichern Sie relevante Beweismittel: Screenshots des Accounts, das Chat-Protokoll, den E-Mail-Verkehr.
• Erstatten Sie im Schadensfall eine Anzeige bei der Polizei.

Weitere Tipps und Informationen: *www.bundeskriminalamt.at*

FOTO: GERD PACHAUER