Bundesministerium
Inneres

Bundeskriminalamt

Cybercrimereport 2024

Cybercrimereport 2024

Wien, 2025

Impressum

Medieninhaber und Herausgeber:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
www.bmi.gv.at
Autorinnen und Autoren: BMI II/BK – Bundeskriminalamt
Layout: BMI Referat I/C/10/a – Strategische Kommunikation und Kreation
Druck: Digitalprintcenter des BMI
Wien, 2025

Vorwort

Die Cyberkriminalität zählt seit Jahren zu den am schnellsten wachsenden Deliktsbereichen. Im Jahr 2024 wurde zwar erstmals ein leichter Rückgang verzeichnet, die Zahl der Anzeigen bleibt jedoch hoch und die Bedrohung signifikant. Internetkriminalität ist längst eine der größten Herausforderungen für die Sicherheit Österreichs – und im internationalen Kontext. Sie betrifft jede und jeden, unabhängig von Alter, Bildung oder Vorerfahrung, und gefährdet Bürgerinnen und Bürger ebenso wie Unternehmen und den Staat selbst.

Um dieser Gefahr wirksam zu begegnen, setzt das Bundesministerium für Inneres im Rahmen der Kriminaldienstreform auf einen massiven Ausbau von Technik, Organisation und Personal. Neue Trainingszentren, Ausbildungskooperationen wie mit den Cyber-Handelsakademien sowie verstärkte internationale Zusammenarbeit sind entscheidende Schritte. Gleichzeitig werden hochspezialisierte IT-Fachkräfte angeworben, um das Know-how im Wettlauf mit global agierenden Cyberkriminellen stetig zu erweitern. So entstehen im Zuge der Reform neue Arbeitsplätze zur weiteren Stärkung der Bereiche Cybercrime und organisierte Kriminalität. Im Hinblick auf den wachsenden personellen und technischen Bedarf im Bereich der Cybercrime-Bekämpfung ist ebenso eine organisatorische Änderung und Aufwertung des Cybercrime-Competence-Centers (C4) zu einer eigenen Abteilung im Bundeskriminalamt erfolgt, um auch allen zukünftigen Herausforderungen und internationalen Standards weiterhin gerecht werden zu können.

Ein weiterer Schwerpunkt liegt auf der Prävention. Da Cyberkriminalität alle treffen kann, gilt es, die Eigenverantwortung der Bevölkerung zu stärken und diese für einen sicheren Umgang mit digitalen Technologien zu sensibilisieren.

Nur durch konsequente Aufklärung, Kooperation und moderne Ermittlungswerkzeuge kann die notwendige Widerstandskraft aufgebaut werden. Dazu zählen die Beschaffung neuer Softwarelösungen, die Stärkung von IT-Forensik und IT-Ermittlungen sowie die gezielte Gewinnung von Expertinnen und Experten für den Polizeidienst. Der verantwortungsvolle Einsatz neuer Technologien – etwa Künstlicher Intelligenz – wird dabei ebenso wichtig sein wie die enge Zusammenarbeit mit Wissenschaft, Forschung und Wirtschaft.

Mag. Gerhard Karner,
Bundesminister für Inneres
© BKA/Andy Wenzel

Mag. Dr. Franz Ruf, MA,
Generaldirektor für die
öffentliche Sicherheit
© BMI/Gerd Pachauer

General
Mag. Andreas Holzer, MA,
Direktor des
Bundeskriminalamtes
© Fotostudio Semrad

Inhalt

1 Einleitung

Der vorliegende Bericht gewährt den alljährlichen Überblick in die Komplexität des Begriffs „Cybercrime“ und beschreibt die kriminalpolizeilichen Maßnahmen im Rahmen der in Österreich geltenden Definitionen und Abgrenzungen. Die Aufgaben der Cybersicherheit und der Cyberabwehr unterliegen den Verantwortungen anderer Organisationen beziehungsweise Organisationseinheiten.

Die Ergebnisse aus den Analysen basieren auf Informationen, die in der fachlichen Zentralstelle des Bundeskriminalamts, dem Cybercrime-Competence-Center (C4), zusammenlaufen, wie den gesammelten Meldungen, Anzeigen und Statistiken aus internationalen Kooperationen, dem Informationsaustausch mit Mitgliedsstaaten, den Ausbildungen, Positionspapieren sowie Studien von Dritten. Die Bestandsaufnahme der quantitativen Daten und qualitativen Inhaltsanalysen fand zu Beginn des Erscheinungsjahres statt, da auf die Verfügbarkeit der Daten von Jänner bis Dezember 2024 in der Polizeilichen Kriminalstatistik (PKS) Rücksicht genommen werden muss. Diese gibt trotz eines zu verbessernden Anzeigeverhaltens mit vermuteten hohen Dunkelziffern die strategischen Leitlinien der exekutiven Maßnahmen vor und dient der stetigen Weiterentwicklung beim Know-how-Aufbau und in der Kriminalitätsbekämpfung.

Im Jahresvergleich kann bei den Cybercrime-Delikten insgesamt eine Abnahme verzeichnet werden. Erfreulicherweise lässt sich auch ein leichter Anstieg der Aufklärungsquote feststellen.

Internetkriminalität	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
Jahr 2015	10.010	4.157	41,5 %
Jahr 2016	13.103	5.072	38,7 %
Jahr 2017	16.804	6.470	38,5 %
Jahr 2018	19.627	7.332	37,4 %
Jahr 2019	28.434	10.187	35,8 %
Jahr 2020	35.915	12.012	33,4 %
Jahr 2021	46.179	17.020	36,9 %
Jahr 2022	60.195	20.378	33,9 %
Jahr 2023	65.864	20.818	31,6 %
Jahr 2024	62.328	19.785	31,7 %
Veränderung zum Vorjahr	-5,4 %	-5,0 %	0,1 %-Punkte

Tabelle 1: Zehn-Jahres-Vergleich Internetkriminalität / Österreich 2015 bis 2024 (Jänner bis Dezember)

Die Personalrekrutierung von IT-Fachleuten für die Reform des C4 gestaltete sich auch im vergangenen Jahr mit den bestehenden Ressourcen als herausfordernd und führte zu einer Fokussierung im internen Wissensaufbau durch Präsenz- und Online-Schulungen.

Die Aufbauorganisation und ihre Abläufe sind aufgrund der technischen Komplexität und einhergehender Spezialisierung sehr flexibel gestaltet. Das Cybercrime-Competence-Center (C4) möchte mit der ausgeübten zentralen Fachaufsicht einen Einblick in Vorgehensweisen geben und das Anzeigeverhalten in der Bevölkerung verbessern. Es wird weiterhin auf vermehrte Eigenverantwortung der Bürgerinnen und Bürger und auf präventive Maßnahmen als Schwerpunkt gesetzt. Deshalb werden im Bericht die wichtigsten Phänomene im Detail genannt, fallweise mit vorbeugenden Handlungsempfehlungen ergänzt und das richtige Anzeigeverhalten beschrieben.

2 Entwicklungen, Trends und Beispiele

In der Meldestelle des Cybercrime-Competence-Centers wurden im Laufe des vergangenen Jahres vermehrt Angriffe auf Computersysteme oder Netzwerke mit Hilfe von Schadsoftware registriert. Ebenso kam es zu zahlreichen Erpressungsversuchen gegenüber Unternehmen, aber auch gegenüber Privatpersonen. Genaue Auswertungen und Analysen zur Polizeilichen Kriminalstatistik (PKS) 2024 finden sich in Kapitel 3 wieder.

Auch im Jahr 2024 machten Betrugshandlungen den größten Anteil an erstatteten Anzeigen aus. Insgesamt werden über die vergangenen Jahre vermehrt Anzeigen im Bereich von Internetbetrug über das Tatmedium Internet verzeichnet. Aufgrund zunehmender Arbeitsteilung und Vernetzung der Tätergruppen, vor allem im Ransomware-Bereich, wird eine erfolgreiche Strafverfolgung erschwert.

2.1 Internetbetrug

Die überwiegende Mehrheit der Betrugsfälle wird digital initiiert, wobei die Kriminellen das Internet zur Anbahnung und Ausführung der Tat nutzen. Die digitale Welt bietet Kriminellen ein breites Spektrum an Möglichkeiten, ihre Opfer zu täuschen. Die Betrugsarten haben sich auch im Jahr 2024 weiter diversifiziert und stellen eine anhaltende Herausforderung für die österreichische Exekutive dar. Dieses breit gefächerte Spektrum umfasst unter anderem betrügerische Anrufe, falsche Gewinnversprechen, betrügerische Investitionsangebote sowie Love Scams, Phishing-Attacken und betrügerische Aktivitäten im Onlinehandel. Neben einzelnen Kriminellen dominieren insbesondere organisierte Tätergruppen, die die Anonymität des Internets für ihre Zwecke ausnutzen. Mit minimalen Ressourcen erreichen diese Gruppen eine große Anzahl potenzieller Opfer und erzielen beträchtliche finanzielle Gewinne. Der Einsatz von Künstlicher Intelligenz zur Erstellung betrügerischer Deep Fakes sowie zur Automatisierung komplexer Betrugsmodelle zeichnete sich im Jahr 2024 bereits ab. Das im Bundeskriminalamt angesiedelte, datenbankgestützte Lagebild Betrug erfasst aktuelle Trends und neue Betrugsmethoden zeitnah und ist ein wesentlicher Baustein zielgerichteter und zeitkritischer Präventionsmaßnahmen.

Das Bundeskriminalamt setzt zur Bekämpfung dieser kriminellen Aktivitäten sowohl auf präventive als auch auf repressive Maßnahmen. Einerseits wird die Öffentlichkeit über aktuelle Betrugsphänomene informiert und sensibilisiert, andererseits wird die internationale Kooperation mit ausländischen Behörden intensiviert. Das Bundeskriminalamt steht in engem Austausch mit wissenschaftlichen und privaten Einrichtungen zur

Erarbeitung und Etablierung neuer Methoden zur Betrugsbekämpfung und Betrugsprävention. Als Beispiel kann hierzu das frei verfügbare Browser-Plug-in „Fake Shop detector“ genannt werden.

Die Polizeiliche Kriminalstatistik (PKS) des Jahres 2024 verzeichnet eine Abnahme der gemeldeten Fälle von Internetbetrug auf 31.768 was einem Rückgang von 6,8 Prozent gegenüber dem Vorjahr entspricht.

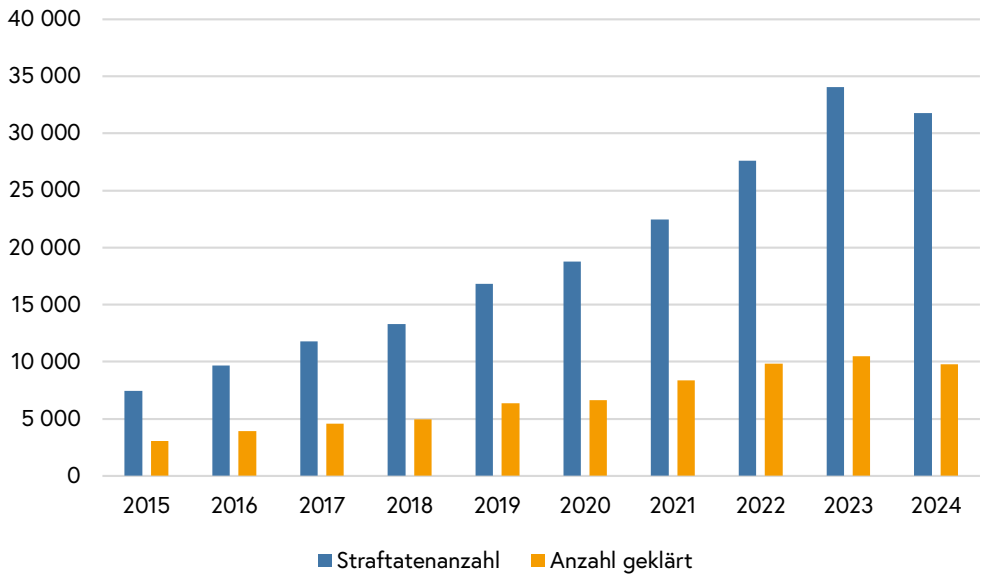

Abbildung 1: Zehn-Jahres-Vergleich Internetbetrug

Hervorzuheben sind die jährlich zunehmenden Fall- und Schadenszahlen im Bereich des Cyber Trading Frauds. Dabei werden potenzielle Anlegerinnen und Anleger für vermeintlich lukrative Investitionsgeschäfte im Internet angelockt und zu Geldzahlungen verleitet. Die Kontaktaufnahme geschieht vornehmlich über Online-Werbeanzeigen, soziale Medien oder Massenmails. Die Schadenssumme im Jahr 2024 belief sich hierbei allein auf zirka 120 Millionen Euro. Um diesem Deliktsfeld bundesweit koordiniert, international und zielgerichtet entgegentreten zu können, wurde im Bundeskriminalamt eine Ermittlungsgruppe zur Bekämpfung dieser Betrugsform installiert.
Auch Phishing-Angriffe per E-Mail oder SMS waren 2024 hoch im Kurs. Anzumerken ist, dass neben klassischen Phishing-Versuchen, die auf Bankkundinnen und Bankkunden und Kreditkarteninhaberinnen und Kreditkarteninhaber abzielten, auch vermehrt Phishing-Angriffe auf Kundinnen und Kunden alternativer Online-Zahlungsdienstleisterinnen und Zahlungsdienstleister und Inhaberinnen und Inhaber von Krypto-Börsen-Konten zu verzeichnen waren.

Das Bundeskriminalamt steht mit betroffenen Finanzinstituten in engem Austausch, um derartige Phishing-Angriffe zielgerichtet eindämmen und potenzielle Opfer zeitnah warnen zu können.

2.2 Crime as a Service

Die angebotenen Leistungen von „Crime as a Service"-(CaaS-)Diensten nehmen im Internet weiterhin zu. Dabei handelt es sich vorwiegend um Hackingtools und Schadsoftware, wie beispielsweise Verschlüsselungstrojaner, aber darüber hinaus auch um spezielle Dienstleistungen zur Geldwäsche, für Übersetzungen oder für den vermeintlichen „Opfer-Support". Auch die Nutzung von Bot-Netzwerken, die DDoS-Angriffen oder dem Versand von Spam-E-Mails dienen, kann vermehrt wahrgenommen werden. Ebenso wurde ein Anstieg beim Inverkehrbringen von Falschgeld, pornographischer Darstellung Minderjähriger, Kreditkartendaten und gefälschten Urkunden registriert.

Durch die im Darknet angebotenen Dienste konnten vor allem Massenerpressungsmails und gezielte Erpressungen durch Ransomware mit Bitcoin-Forderungen festgestellt werden. Die Täterschaft benötigt damit keinesfalls mehr tiefgreifendes Wissen zur technischen Durchführung, sondern wird mit den CaaS-Dienstleistungen in die Lage versetzt, das fehlende Wissen mit entsprechenden Diensten zukaufen zu können. Mit einem Ransomware-as-a-Service-Modell (RaaS) lassen sich nach wie vor beträchtliche Gewinne erzielen.

2.3 Residential Proxies

Das Internet ist ein Ort der Anonymität – eine Tatsache, die sich Kriminelle zunutze machen. Eine besonders arglistige Methode ist die Nutzung sogenannter Residential Proxies.

Ein Proxy-Server dient als Vermittler zwischen einer Nutzerin bzw. einem Nutzer und dem Internet. Er versteckt die ursprüngliche IP-Adresse und leitet den Datenverkehr über eine andere Quelle. Während Datacenter Proxies von Serverfarmen stammen und leicht zu blockieren sind, verwenden Residential Proxies echte Privatanschlüsse von Haushalten. Dadurch wirken ihre IP-Adressen legitim und sind kaum als Tarnung zu erkennen.

In vielen Fällen ahnen Nutzerinnen und Nutzer nicht, dass ihr Heimnetzwerk als Proxy missbraucht wird. Dies geschieht meist durch das Installieren von scheinbar harmloser Software, etwa kostenlosen VPNs oder Apps, die im Kleingedruckten die Nutzung des Geräts als Proxy erlauben. In anderen Fällen werden Geräte über Sicherheitslücken oder Malware kompromittiert.

Ein großer Risikofaktor sind veraltete Router und IoT-(Internet-of-Things-)Geräte. Viele Menschen nutzen jahrelang denselben Router, ohne zu wissen, dass dieser keine Sicherheitsupdates mehr erhält. Cyberkriminelle suchen gezielt nach solchen ungeschützten Geräten, um sie in Proxy-Netzwerke einzubinden. Ohne Updates bleiben bekannte Sicherheitslücken offen, durch die Angreiferinnen bzw. Angreifer das Gerät unbemerkt übernehmen können.

Cyberkriminelle setzen Residential Proxies gezielt für Betrug und illegale Aktivitäten ein, darunter Finanzbetrug, Identitätsdiebstahl, Account-Übernahmen, Cyberangriffe, Botnetze, illegale Inhalte und Darknet-Aktivitäten.

Um sich zu schützen, sollte man keine unbekannten oder kostenlosen VPN-Dienste nutzen, Software nur aus vertrauenswürdigen Quellen beziehen und vor allem darauf achten, dass Router und andere Netzwerkgeräte regelmäßig aktualisiert werden. Wer ein Gerät nutzt, das keine Sicherheitsupdates mehr erhält, sollte über einen Austausch nachdenken – denn gerade alte, unsichere Geräte sind eine Einladung für Cyberkriminelle.

2.4 Blockchain und Kryptowährungen

In Österreich verzeichnen Ermittlungsbehörden einen signifikanten Anstieg von Betrugsdelikten im Kryptowährungssektor. Besonders besorgniserregend ist die zunehmende Professionalisierung der Tätergruppen, die immer ausgereiftere Methoden entwickeln.

Ein dominierendes Phänomen sind gefälschte Trading-Plattformen, die durch ihr professionelles Erscheinungsbild selbst erfahrene Anlegerinnen und Anleger täuschen. Diese Plattformen werben mit unrealistischen Renditeversprechen von 200 bis 300 Prozent und täuschen durch gefälschte Live-Kurse sowie manipulierte Handelsdaten eine legitime Handelsaktivität vor. Nach erfolgter Einzahlung wird den Opfern typischerweise der Zugriff auf ihre Vermögenswerte verwehrt, oder Auszahlungen werden unter verschiedenen Vorwänden verhindert.

Besondere Aufmerksamkeit verdient das sogenannte Address-Poisoning, bei dem Angreiferinnen und Angreifer täuschend ähnliche Wallet-Adressen in die Transaktionshistorie eines Opfers einschleusen. Wenn das Opfer später eine Adresse aus der Historie kopiert, kann es versehentlich die gefälschte Adresse verwenden und Kryptowährungen an Betrügerinnen und Betrüger verlieren.

Ein Rug Pull ist eine betrügerische Praxis, bei der Projektentwicklerinnen und Projektentwickler zunächst ein scheinbar legitimes Krypto-Projekt aufbauen und Investorengelder sammeln. Sobald genügend Liquidität vorhanden ist, ziehen sie plötzlich das gesamte Geld aus dem Projekt ab („Pull the rug“) und verschwinden. Die Tokens der Investoren werden

dabei wertlos. Diese Betrugsform ist besonders häufig bei DeFi-Projekten und neuen Token auf dezentralen Börsen zu finden, da dort keine Regulierung existiert und die Entwicklerinnen und Entwickler meist anonym bleiben. DeFi-(Decentralized-Finance-)Projekte sind Anwendungen und Protokolle, die im öffentlichen Blockchain-Bereich angesiedelt sind und traditionelle Finanzdienstleistungen ohne zentrale Vermittler wie Banken anbieten.

Eine weitere bedeutende Entwicklung ist der Liquidity-Mining-Betrug, bei dem gefälschte DeFi-Protokolle hohe Liquiditätsprämien versprechen. Durch manipulierte Smart Contracts werden die eingezahlten Gelder direkt an die Kriminellen transferiert. Die technische Komplexität dieser Betrugsvariante macht es für Opfer besonders schwer, den Betrug zu erkennen.

Als Reaktion auf diese Entwicklungen haben Aufsichtsbehörden die Regulierung verschärft. Die EU-MiCA-Verordnung (Markets in Crypto-Assets Regulation) sowie strengere KYC-Anforderungen (Know Your Customer) sollen mehr Transparenz und Sicherheit schaffen.

2.5 Pig Butchering: Liebes- und Investmentbetrug

Ein nach wie vor zu beobachtender Modus Operandi ist das sogenannte Pig Butchering in Kombination mit dem klassischen Love-Scam. Der Begriff „Pig Butchering“ bezieht sich dabei auf eine Betrugsmasche, die darauf abzielt, Vertrauensbeziehungen zu potenziellen Opfern aufzubauen, um diese in weiterer Folge finanziell auszunutzen. Der Name leitet sich von der Analogie ab, dass die Betrügerinnen und Betrüger ihre Opfer gewissermaßen wie Schweine mästen, bevor die betrügerischen Absichten realisiert und den Opfern sämtliche Investitionen entzogen werden.

Der Betrug läuft in der Regel folgendermaßen ab: Es werden gefälschte Profile auf verschiedenen sozialen Medien und Dating-Plattformen erstellt. Anschließend werden zufällig ausgewählte Personen via Messenger-Dienste, WhatsApp oder LinkedIn kontaktiert, um mit den späteren Opfern über Wochen und Monate eine freundschaftliche oder sogar tiefergehende, romantische Beziehung aufzubauen.

Sobald genug Vertrauen aufgebaut wurde, erwähnen die Betrügerinnen und Betrüger beiläufig eine Kryptoinvestitions-Website, auf der sie angeblich bereits hohe Rendite erwirtschaftet hätten, und überreden die potenziellen Opfer, nach und nach immer größere Summen über die genannte Webseite zu investieren. Diese Plattformen manipulieren die angezeigten Renditen und lassen es so aussehen, als hätten die Opfer jederzeit Zugriff auf ihre investierten Mittel. Für diesen Zweck kommen regelmäßig falsche und imitierte „Stablecoins“ wie beispielsweise USDT zum Einsatz, die eine regelmäßige Auszahlung der angeblich erwirtschafteten Rendite an das eigene Wallet vortäuschen sollen.

Stablecoins sind digitale Währungen, die den Wert eines anderen Assets abbilden. Dabei handelt es sich meistens um Fiatwährungen wie zum Beispiel Euro oder US-Dollar (USD). Ein Stablecoin kann also den Wert einer anderen Währung spiegeln. Der Tether USD (USDT) ist ein Stablecoin, der darauf abzielt, den Wert des US-Dollars nachzubilden.

Sobald das Potenzial der Opfer ausgeschöpft wurde, folgt oft der Versuch, diese zu überreden, Kredite aufzunehmen oder weitere Geldquellen zu erschließen. Wenn die Opfer misstrauisch werden oder keine weiteren Zahlungen leisten können, schränken Betrügerinnen und Betrüger den Zugang zu den Geldern ein und starten Erpressungsversuche. Sie drohen den Opfern mit rechtlichen Konsequenzen, Gewalt oder der Veröffentlichung ihrer intimen Kommunikation und intimen Bildmaterials.

2.6 Tochter-Sohn-Trick über WhatsApp-Nachrichten

Noch immer im Umlauf ist der Tochter-Sohn-Trick. Den Opfern wird über WhatsApp eine Nachricht, zum Beispiel „Hallo Mama, das ist meine neue Telefonnummer“, übermittelt. Die Betrügerinnen und Betrüger geben sich als Kind der Empfängerinnen und Empfänger aus und teilen mit, dass sie über eine neue Telefonnummer verfügen. Das alte Mobiltelefon wurde verloren oder sei durch einen Wasserschaden unbrauchbar. Da am neuen Telefon die Banking-App noch nicht funktioniere und deshalb eine dringende Zahlung nicht durchgeführt werden könne, wird um Hilfe gebeten. Die Opfer mögen doch einen zumeist vierstelligen Betrag an einen gewissen Empfänger überweisen. Das Geld werde so bald wie möglich zurückgezahlt. Die Empfänger sind zumeist Money Mules im europäischen Ausland.

2.7 Bezahldienst-Trick

Vorsicht ist auch bei Verkäufen auf Kleinanzeigenplattformen geboten. Betrügerinnen und Betrüger täuschen Kaufinteresse vor. Sie geben an, dass die Bezahlung für eine Ware erfolgt sei. Zum Erhalt der Ware müsse ein Link angeklickt werden. Das Opfer gibt sämtliche Bezahldetails wie Betrag, Bankkonto, Kreditkarten- und Verfügernummer an. Das Ergebnis ist jedoch, dass keine Bezahlung an das Opfer erfolgt, sondern über den Link eine oder wiederholte Zahlungen an die Kriminellen autorisiert werden.

2.8 Transportdienst-Trick

Ebenfalls auf Kleinanzeigenplattformen kursiert ein weiterer Trick. Die Kriminellen nehmen Kontakt auf und geben an, an der vom Opfer angebotenen Ware interessiert zu sein. Aufgrund des derzeitigen Aufenthaltsorts der vermeintlichen Käuferin beziehungsweise des vermeintlichen Käufers, die zumeist angeblich im Ausland weilen, kann die Ware nicht persönlich abgeholt werden. Es wird jedoch der Vorschlag gemacht, die Ware mit einem Shipping-Dienst (Transportdienst) abholen zu lassen. Den Kaufpreis hätte der Transportdienst in bar dabei, um diesen bei Abholung zu übergeben. Im Verlauf dieses angeblichen Kaufs erhält das Opfer vom angeblichen Transportdienst die Aufforderung per Link, eine Versicherung abzuschließen und die Kosten vorerst auszulegen. Bei der Abholung der Ware würden dann auch die Kosten für diese Versicherung von der Käuferin bzw. vom Käufer übernommen und somit bezahlt werden. Bei dieser Betrugsform bestätigen gutgläubige Opfer tatsächlich Zahlungen an die Kriminellen, ohne dass dieser je die Ware abholen lässt.

2.9 Phishing

Phishing (abgeleitet vom englischen Wort „fishing“ = angeln) ist eine betrügerische Methode, bei der Cyberkriminelle versuchen, persönliche Informationen wie Passwörter und Kreditkartendaten beispielsweise durch gefälschte E-Mails oder Webseiten zu stehlen. Betrügerinnen und Betrüger versuchen hierbei, ahnungslose Internetnutzerinnen und -nutzer zu täuschen, um an sensible Daten zu gelangen.

Phishing-E-Mails und -Webseiten traten im Laufe des Jahres 2024 gehäuft in Erscheinung. Alle größeren Bankinstitute in Österreich waren von Phishing von Zugangsdaten für eBanking betroffen, wobei mit schädlichen Android-Applikationen mobile TAN für das Online-Banking abgegriffen wurden. Besonders im Rahmen der Anubis-Android-Malware waren mehrere Phishing- und Malware-Verbreitungskampagnen im Umlauf. Der Link zur Phishing-Seite lässt sich nur per Android-Browser (Android User Agent) öffnen. Nach Eingabe der Daten erfolgt die Aufforderung zum Download einer sogenannten „Sicherheits-App“.

2.10 Ransomware

Ransomware ist eine Schadsoftware, die von Kriminellen verwendet wird, um den Zugriff auf Daten oder das gesamte Computersystem eines Opfers zu verhindern. Dabei werden die Daten auf dem Computer des Opfers verschlüsselt oder der Zugriff darauf wird blockiert. Die Angreifer fordern anschließend Lösegeld, um die Daten wieder freizugeben. Ransomware kann auf verschiedene Arten in ein System eindringen, zum Beispiel durch

das Öffnen von E-Mail-Anhängen, Social Engineering oder durch Herunterladen von infizierten Dateien aus dem Internet.

Ransomware-Angriffe treten weltweit in einer Vielzahl von Branchen auf. Cyberkriminelle richten ihre Angriffe oft gegen Organisationen und Branchen, die für sie finanziell lukrativ sind oder die durch einen Ausfall besonders stark beeinträchtigt werden können. Es ist wichtig zu beachten, dass Ransomware-Angriffe praktisch jede oder jeden treffen können. Die Motivationen der Angreiferinnen und Angreifer können von finanziellen Forderungen bis hin zu ideologischen Gründen reichen. In diesem Zusammenhang wird auf den „**Ransomware Report 2024**“ des Cybercrime-Competence-Centers im Bundeskriminalamt verwiesen.

Im Cybercrime-Competence-Center werden alle angezeigten Ransomware-Fälle zentral erfasst und auf Gemeinsamkeiten analysiert. Ausgenommen sind jene Fälle, die aufgrund der Geschäftseinteilung in den Zuständigkeitsbereich anderer Behörden und Dienststellen fallen (wie zum Beispiel der Direktion für Staatsschutz und Nachrichtendienst – DSN). Zusammengehörige Fälle (selbe Täterschaft, zusammenhängende Indikatoren der Kompromittierung etc.) werden zentral unter Einbeziehung der involvierten Polizeidienststellen koordiniert beziehungsweise erfolgt eine Unterstützung der jeweiligen Sachbearbeiterin oder des jeweiligen Sachbearbeiters. In bestimmten Fällen erfolgt auch eine Übernahme international durchzuführender Anfragen, ein Datenabgleich und die Koordination und Fallkooperation mit anderen Ländern.

Im Jahr 2024 wurden **109 Fälle** im gesamten Bundesgebiet zur Anzeige gebracht.

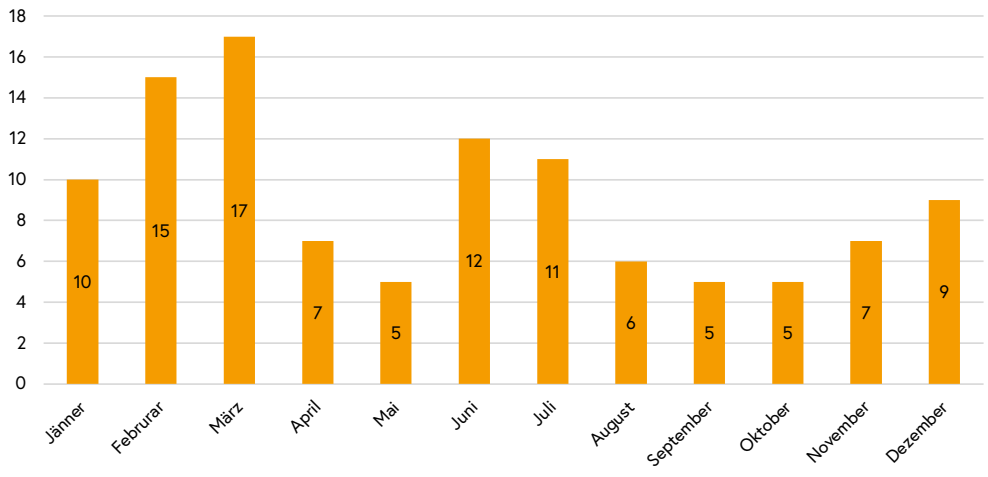

Abbildung 2: Monatliche Verteilung der Ransomware-Fälle 2024

Die Mehrheit der Angriffe erfolgte in der ersten Jahreshälfte, wobei erkennbar ist, dass ein großer Teil der Angriffe durch viele kleinere Akteurinnen und Akteure durchgeführt

wurde. Lediglich einige wenige Gruppierungen (zum Beispiel LockBit) sind für fortgesetzte Tathandlungen und mehrere Angriffe verantwortlich.

Wie im Vorjahr konnte etwa ein Drittel der Anzeigen nicht eindeutig einer bestimmten Ransomware-Gruppierung zugeordnet werden. Derartige Zuordnungen gestalten sich aufgrund unterschiedlicher Ursachen immer komplexer. IT-Systeme von Opfern werden einerseits noch vor Anzeigenerstattung verändert oder neu installiert, um so schnell wie möglich wieder einsatzbereit zu sein, wodurch wichtige Spuren verloren gehen können. Andererseits versuchen viele Ransomware-Akteurinnen und -Akteure ihre Identität zu verbergen, hinterlassen bewusst irreführende Spuren, setzen falsche Indikatoren, kooperieren oder teilen sich Ressourcen, Werkzeuge und Techniken. Neue Gruppierungen entstehen, bestehende durchlaufen Veränderungen, andere wiederum verschwinden. Ein weiterer Grund ist auch die schnelle Evolution von Malware. Die Methoden zur Durchführung von Ransomware-Angriffen entwickeln sich schnell weiter. Eine Akteurin bzw. ein Akteur kann leicht seine Taktiken, Techniken und Verfahren ändern.

Über ein Drittel der Angriffe fand auf Unternehmen statt. Dabei kann keine Konzentration auf bestimmte Zielbranchen festgestellt werden. **29 unterschiedliche Akteurinnen und Akteure** konnten als Angreifer identifiziert werden.

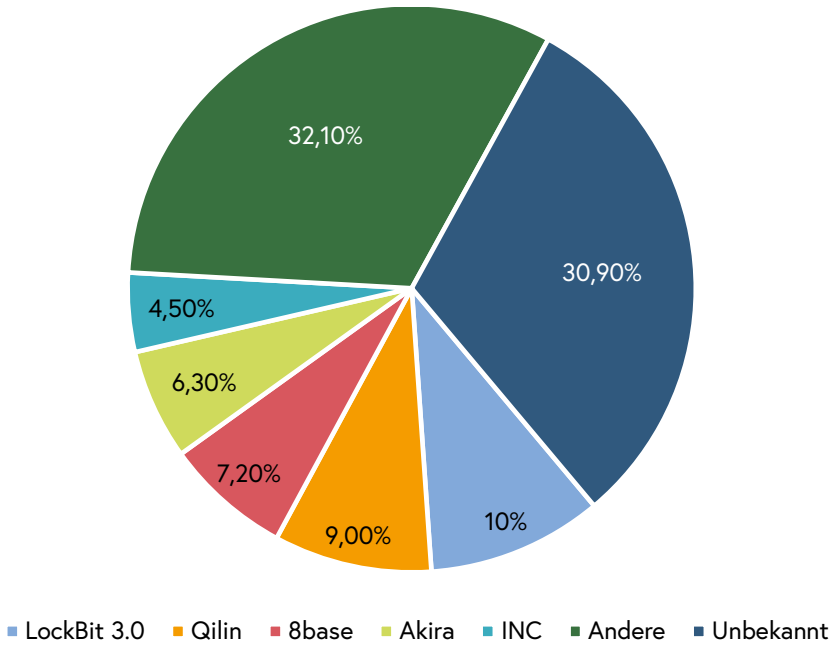

Abbildung 3: Ransomware-Akteure und prozentuelle Verteilung 2024

Der Ransomware-Akteur LockBit (in den Varianten - 1.0, 2.0 und 3.0) wird auch in verschiedenen Ländern als aktivster Angreifer genannt.

2.11 DDos-Angriffe

DoS/ DDoS (Denial of Service / Distributed Denial of Service) sind Angriffe auf die Verfügbarkeit eines Dienstes, um vorübergehend die Erbringung dieses Dienstes einzuschränken oder gänzlich zu unterbinden. Zu diesem Zweck wird das angegriffene System mit (sinnlosen) Anfragen überflutet, sodass die Ressourcen des angegriffenen Systems für die ordnungsgemäße Erbringung der vorgesehenen Funktionen nicht mehr ausreichen.

Im Jahr 2024 wurden in Österreich DDoS-Angriffe auf Unternehmen und Institutionen verzeichnet. Diese Angriffe führten zu erheblichen Störungen in verschiedenen Sektoren und erforderten verstärkte Sicherheitsmaßnahmen.

Die Angriffe richteten sich gegen verschiedene Wirtschaftsbereiche, darunter Medienunternehmen, E-Commerce-Plattformen, Tourismusbetriebe sowie kritische Infrastrukturen wie Informations- und Verkehrsdienste. Die Kriminellen verwendeten verschiedene Methoden, wobei sogenannte DNS-Reflection- und Layer-7-Angriffe die häufigsten Techniken darstellten.

DNS-Reflection ist eine Methode, bei der Angreiferinnen bzw. Angreifer Server dazu bringen, große Datenmengen an das Opfer zu senden, um dessen System zu überlasten. Zusätzlich wurden Kombinationen anderer Angriffsmuster beobachtet. Die Angriffe erfolgten meist durch automatisierte Botnetze, die gezielt Server überlasteten. In einigen Fällen konnten spezifische IP-Adressen aus dem Ausland identifiziert werden, die auf international agierende Kriminelle hinweisen.

Die Attacken führten zu temporären Ausfällen von Online-Plattformen, Verzögerungen im Geschäftsverkehr und erhöhten Sicherheitsmaßnahmen. Schätzungen zufolge verursachten diese Angriffe wirtschaftliche Schäden in Millionenhöhe, insbesondere durch Umsatzausfälle und zusätzliche IT-Sicherheitskosten.

Die Anonymität der Kriminellen stellt weiterhin eine große Herausforderung für die Strafverfolgung dar. Um zukünftige Angriffe zu verhindern, wird empfohlen, verstärkt in DDoS-Schutzmaßnahmen zu investieren, darunter Traffic-Filter, CDN-Dienste (Computer Network Defense) und erweiterte Firewall-Lösungen. Unternehmen sollten zudem ihre Incident-Response-Pläne regelmäßig aktualisieren.

2.12 RDDoS-Angriffe

Eine Sonderform von DDoS-Attacken stellten auch im vergangenen Jahr Ransom-DDoS-Angriffe (RDDoS-Angriffe) dar. Diese liegen vor, wenn Täter(gruppierungen) versuchen, eine Person oder Organisation zu erpressen, und zusätzlich mit einem DDoS-Angriff drohen oder Lösegeld verlangen. Beobachtungen zufolge führen manche Angreiferinnen bzw. Angreifer den DDoS-Angriff zuerst durch, um Lösegeld zu verlangen. Andere wiederum schicken zuerst eine Lösegeldforderung und drohen ihren Opfern darin mit einem DDoS-Angriff. Im zweiten Fall sind Angreiferinnen bzw. Angreifer möglicherweise technisch gar nicht in der Lage, den Angriff durchzuführen. Das Restrisiko kann in vielen Fällen jedoch kaum eingeschätzt werden. Von einer leeren Drohung auszugehen, bleibt meist riskant.

In diesem Zusammenhang gab es vereinzelt Attacken auf österreichische Unternehmen aus unterschiedlichen Wirtschaftsbereichen.

2.13 Online-Suchtmittelhandel

Innerhalb des vergangenen Jahrzehnts hat sich der verbotene Handel mit Suchtmitteln über Online-Plattformen zu einer bewährten Begehungsform der Suchtmittelkriminalität auch innerhalb Österreichs entwickelt. Genutzt werden diese Medien sowohl von Einzeltäterinnen und Einzeltätern als auch von kriminellen Organisationen, um durch diese organisierte Art des Suchtmittelhandels illegale Gewinne zu erzielen. Es kann davon ausgegangen werden, dass sowohl von den Händlerinnen und Händlern als auch von den Konsumentinnen und Konsumenten der hohe Grad an Anonymität, das Fehlen eines direkten Kontaktes und die durchgehende Verfügbarkeit geschätzt werden. Ferner bietet der Online-Handel auch eine Verfügbarkeit von Suchtmitteln aller Art an den abgelegensten Orten an.

Aus den Ermittlungen im Bereich dieser Begehungsform des Suchtmittelhandels kann abgeleitet werden, dass der Online-Drogenhandel den Straßenhandel nicht verdrängt oder ersetzt, sondern diesen vielmehr ergänzt. Gezeigt hat sich außerdem, dass über Online-Plattformen Suchtmittel höherer Qualität verkauft werden. Der Erwerb dieser hochwertigen Suchtmittel über Online-Plattformen dient fallweise auch dazu, sie im Straßenhandel gewinnbringend weiterzuverkaufen.

Außerdem ergänzt der Online-Handel mit Suchtmitteln den klassischen Straßenhandel, indem er ein diverseres, leicht zugänglicheres Angebot zu vor allem unüblichen synthetischen Suchtmitteln bietet.

Fand der Verkauf dieser illegalen Suchtmittel zu Beginn vorwiegend im Darknet statt – wo die gesamten Geschäftsgebarungen, angefangen von der Anbahnung über die

Verkaufsverhandlungen bis hin zur Bezahlung, über diese verschlüsselten Netzwerke abgewickelt werden – ist in der jüngeren Vergangenheit eine Verschiebung des Online-Handels ins Clearnet, zu Instant-Messenger-Apps mit End-to-End-Verschlüsselung und zu Social-Media-Kanälen zu beobachten.

Wie betroffen die Republik Österreich vom Suchtmittelhandel über Online-Plattformen ist, kann an den nachstehenden Zahlen abgelesen werden.

Durch das Zollamt Österreich wurden 1.179 Postsendungen mit Suchtmitteln sichergestellt. Dazu kommen weitere 237 sichergestellte Postsendungen mit Suchtmitteln internationaler Partner mit dem Ziel oder der Herkunft Österreich. Somit kam es im Jahr 2024 zu insgesamt 1.416 Sicherstellungen von Postsendungen mit illegalen Suchtmitteln mit Bezug zu Österreich.

Statistisch führt Deutschland, vor den Niederlanden und den innerösterreichischen Sendungen, die Liste der Herkunftsländer an. Es wird jedoch angenommen, dass zirka zwei Drittel der sichergestellten Sendungen ursprünglich aus den Niederlanden stammen, die teils zuvor nach Deutschland verbracht und dort in den Postweg eingebracht wurden.

Hinzu kommt eine neuartige, statistisch nicht erfasste Begehungsform bei der Übermittlung der Suchtmittel, der sogenannte Deaddrop. Hier werden die Suchtmittel nicht mehr per Post versendet, sondern an bestimmten Orten versteckt und die GPS-Koordinaten dem Empfänger übermittelt.

Um diesen Begehungsformen der Suchtmittelkriminalität entgegenzutreten, wurde ein spezialisiertes Referat im Büro zur Bekämpfung der Suchtmittelkriminalität im Bundeskriminalamt eingerichtet. Die Mitarbeiterinnen und Mitarbeiter dieses Referats befassen sich hauptsächlich mit Ermittlungen gegen in Österreich ansässige Online-Suchtmittelhändlerinnen sowie -händler und koordinieren die polizeilichen Maßnahmen zur strafrechtlichen Verfolgung der Käuferinnen und Käufer.

Zusätzlich zu den operativen Maßnahmen werden auch fortwährend neue Strategien entwickelt und analysiert.

Aufgrund der zunehmenden Internationalisierung dieser Begehungsformen ist auch die internationale Zusammenarbeit und Koordination mit Europol und anderen Drittstaaten eine zentrale Aufgabe dieses Fachreferats.

Nach wie vor zeigt sich jedoch, dass die effektivste Maßnahme zur Bekämpfung des Online-Suchtmittelhandels die Zerschlagung der Vertriebswege ist. Aus diesem Grund werden bereits seit 2020 in enger Kooperation mit der österreichischen Zollverwaltung Schwerpunktkontrollen der Postwege durchgeführt und auch im Jahr 2025 fortgesetzt.

2.14 Bildliches sexualbezogenes Kindesmissbrauchsmaterial / Darstellungen minderjähriger Personen

2024 – neues Rekordhoch an übermittelten NCMEC-Verdachtsmeldungen

Im Jahr 2024 kam es zur Übermittlung von insgesamt 18.276 Verdachtsmeldungen durch US-Internet-Service-Provider an das Bundeskriminalamt. Ein neuer Rekord an Meldungen, der den letztjährigen Spitzenwert in der langjährigen Kooperation zwischen dem National Center for Missing & Exploited Children (NCMEC) und dem Referat 3.2.7 abermals um 2.400 Meldungen übertrifft.

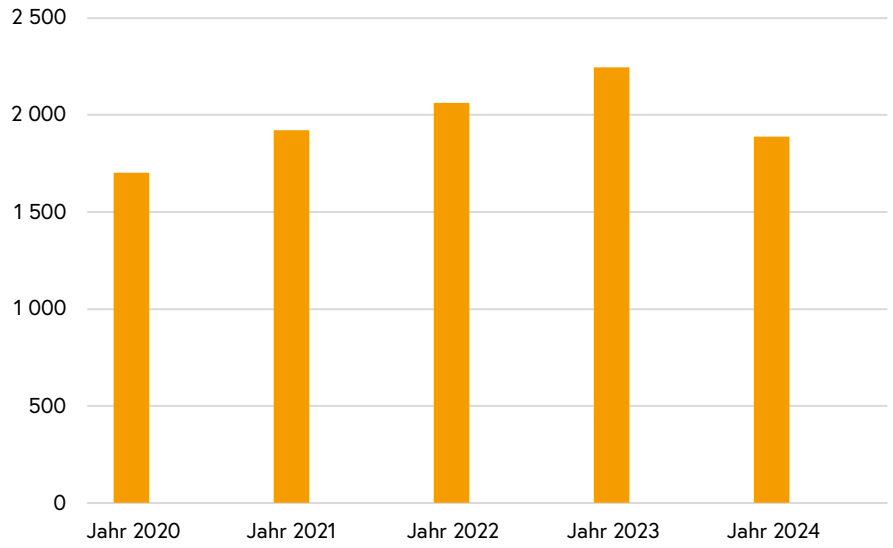

Abbildung 4: Fünf-Jahresvergleich der Anzeigen nach § 207a StGB

Die Inhalte der Benutzerinnen und Benutzer werden von den verschiedensten Internetserviceprovidern vor allem in den USA auf pornographische Inhalte überprüft. Inhalte, die der Tathandlung des „Kindesmissbrauch Online" zuzuordnen sind, werden bei einem entdeckten Fall gesichert und der betroffene Account wird gesperrt. Damit einhergehend erfolgt eine entsprechende Verdachtsmeldung an die zuständigen Strafverfolgungsbehörden des jeweiligen Landes, dem die Verursacherin bzw. der Verursacher zugeordnet werden kann.

Somit fungiert das **National Center for Missing & Exploited Children** als internationale Drehscheibe und stellt das Bindeglied zwischen den jeweiligen Anbietern und den Strafverfolgungsbehörden der einzelnen Staaten dar.

Ebenfalls im Zunehmen ist das Phänomen des so genannten Long Distant Child Abuse. So sieht sich das Referat II/BK/3.2.7 im Bundeskriminalamt mit einer stetig steigenden Anzahl von Fällen konfrontiert, in denen österreichische Kriminelle einen sexuellen Missbrauch von Kindern auf den Philippinen beauftragen und diesen anschließend online, in Echtzeit, konsumieren.

Hier ist positiv zu vermerken, dass es der spezialisierten Ermittlungseinheit im Bundeskriminalamt im Jahr 2024 möglich war, in Zusammenarbeit mit den Landeskriminalämtern und der österreichischen Polizeiattachée in Bangkok, einen Täter aus Österreich und insgesamt 15 minderjährige Opfer auf den Philippinen zu identifizieren. Dieser wurde zu vier Jahren Haft verurteilt, wobei das Urteil noch nicht rechtskräftig ist.

§ 207a StGB	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
Jahr 2015	465	409	88,0 %
Jahr 2016	681	602	88,4 %
Jahr 2017	733	650	88,7 %
Jahr 2018	1.161	1.037	89,3 %
Jahr 2019	1.666	1.541	92,5 %
Jahr 2020	1.702	1.528	89,8 %
Jahr 2021	1.921	1.775	92,4 %
Jahr 2022	2.061	1.889	91,7 %
Jahr 2023	2.245	2.053	91,4 %
Jahr 2024	1.889	1.753	92,8 %
Veränderung zum Vorjahr	-15,9 %	-14,6 %	1,4 %-Punkte

Tabelle 2: Zehn-Jahres-Vergleich der polizeilichen Anzeigen nach § 207a StGB

3 Jahresrückblick

3.1 Zahlen und Fakten im Überblick

Die nachfolgenden Zahlen und Daten stammen in bewährter Weise aus der öffentlich verfügbaren und offiziell verlautbarten Polizeilichen Kriminalstatistik (PKS). Im Jahr 2024 konnte erstmalig im Zehn-Jahresverlauf eine Abnahme der angezeigten Straftaten beobachtet werden.

Cybercrime im Fünf-Jahres-Vergleich			
Jahr	**Anzahl der angezeigten Straftaten**	**Anzahl der geklärten Straftaten**	**Aufklärungsquote (gerundet)**
2020	35.915	12.012	33,4 %
2021	46.179	17.020	36,9 %
2022	60.195	20.378	33,9 %
2023	65.864	20.818	31,6 %
2024	62.328	19.785	31,7 %

Veränderung der Aufklärungsquote im Vergleich zum Vorjahr			
	Jahr 2023: 31,6 %	**Jahr 2024: 31,7%**	**+ 0,1 %-Punkte**

Tabelle 3: Entwicklung der Anzeigen, geklärten Fälle und der Aufklärungsquote von Cybercrime 2020 bis 2024 (Fünf-Jahres-Vergleich)

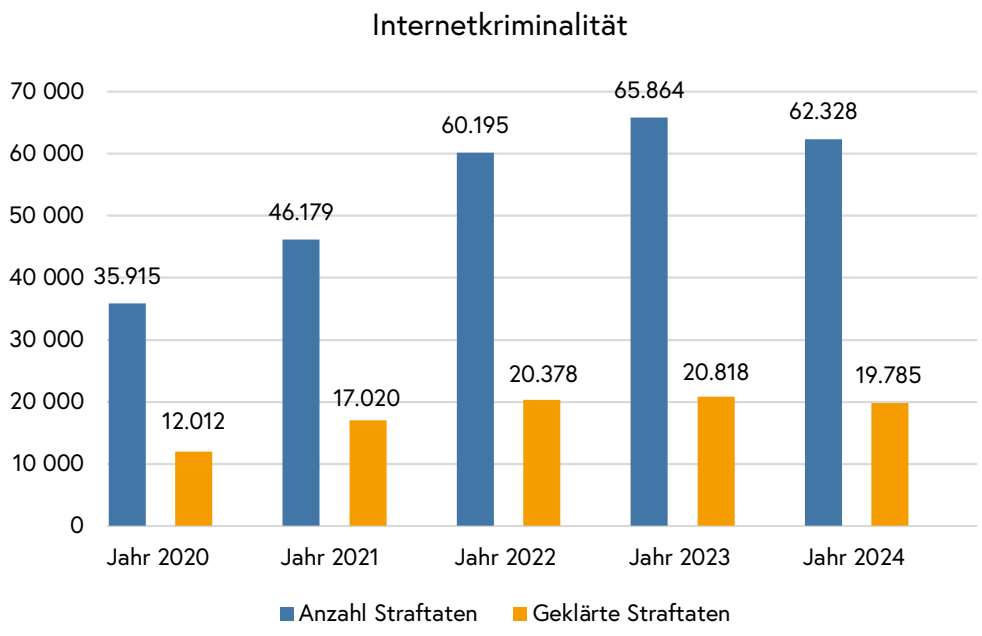

Abbildung 5: Entwicklung der Anzeigen und aufgeklärten Fälle von Cybercrime 2020 bis 2024

In der Polizeilichen Kriminalstatistik (PKS) wird im Sinne internationaler Vereinbarungen (in Anlehnung an die Budapester Konvention) eine Einteilung von Cybercrime vorgenommen, deren Überarbeitung auch national ein Thema von interministeriellen Diskussionen ist.

3.2 Cybercrime im engeren Sinn (IKT als Angriffsziel)

Cybercrime im engeren Sinne umfasst kriminelle Handlungen, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnologie (IKT) begangen werden. Die Straftaten sind gegen die Netzwerke selbst oder aber gegen Geräte, Dienste oder Daten in diesen Netzwerken gerichtet, wie zum Beispiel bei der Datenbeschädigung, dem Hacking oder sogenannten DDoS-Angriffen.

Im Jahr 2024 konnte bei den Tatbeständen zu Cybercrime im engeren Sinn ein leichter Rückgang der Anzeigen in Höhe von 3,4 Prozent gegenüber dem Vorjahr verzeichnet werden. Dies geht mit einer geänderten statistischen Erfassung im Hinblick auf § 148a StGB einher. Grund ist ein OGH-Urteil aus dem Jahr 2023. Der Oberste Gerichtshof (OGH) hat festgestellt, dass eine erfolgte Behebung mit einer fremden Bankomatkarte nicht den Tatbestand des § 148a StGB erfüllt. Diese wird nun als Einbruch protokolliert und statistisch erfasst. Dies hat zur Folge, dass Behebungen mit einer fremden Bankomatkarte nun als Einbruch statistisch erfasst werden.

Im Zuge der Analyse des Zahlenmaterials kann Folgendes festgestellt werden:

Die Zunahme der Anzeigen nach § 118a StGB beruht auf der steigenden Digitalisierung im Alltag. Immer mehr Menschen verwenden digitale Medien stets intensiver, was auch zu einem Anstieg der strafbaren Handlungen in diesem Bereich führt.

Die Gesamtzahl der angezeigten Delikte nach § 119 und § 119a StGB ist so gering, dass über die Ursachen einer geringen Zu- oder Abnahme keine aussagekräftige Begründung abgegeben werden kann.

Bei den Anzeigen nach § 126a, § 126b und § 126c StGB handelt es sich oftmals um strafbare Handlungen, die Wirtschaftsbetriebe treffen. Punktuell stieg die Zahl der Anzeigen beispielsweise bei § 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten).

Das sogenannte Cybermobbing (Fortdauernde Belästigung im Wege der Telekommunikation oder eines Computersystems, § 107c StGB) stellt weiterhin eine große Herausforderung dar, das mit 462 angezeigten Delikten ungefähr auf dem Niveau von 2023 ist.

Delikt	Angezeigte Fälle 2023	Angezeigte Fälle 2024	Geklärte Straftaten 2023	Geklärte Straftaten 2024
§ 107c StGB	458	462	365	355
§ 118a StGB	1.858	1.991	256	250
§ 119 StGB	13	12	9	10
§ 119a StGB	67	63	11	12
§ 126a StGB	308	241	82	58
§ 126b StGB	59	76	3	7
§ 126c StGB	305	496	40	67
§ 148a StGB	17.154	16.192	3.369	2.297
§ 225a StGB	729	713	183	237
Gesamt	20.951	20.246	4.318	3.293

§ 107c StGB (Fortdauernde Belästigung im Wege der Telekommunikation oder eines Computersystems)
§ 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem)
§ 119 StGB (Verletzung des Telekommunikationsgeheimnisses)
§ 119a StGB (Missbräuchliches Abfangen von Daten)
§ 126a StGB (Datenbeschädigung)
§ 126b StGB (Störung der Funktionsfähigkeit eines Computersystems)
§ 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten)
§ 148a StGB (Betrügerischer Datenverarbeitungsmissbrauch)
§ 225a StGB (Datenfälschung)

Tabelle 4: Angezeigte Fälle und geklärte Straftaten von Cybercrime im engeren Sinn nach Paragrafen des Strafgesetzbuches – Vergleich 2023 / 2024.

3.3 Cybercrime im weiteren Sinn (IKT als Tatmittel)

Hierunter werden Straftaten verstanden, bei denen die Informations- und Kommunikationstechnik als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt wird, wie zum Beispiel Betrugsdelikte, Drogenhandel im Darknet, Cybergrooming oder Cybermobbing. In der Polizeilichen Kriminalstatistik (PKS) umfasst Cybercrime im weiteren Sinne beispielsweise die Paragrafen des Internetbetrugs und der sonstigen Kriminalität im Internet.

Der **Internetbetrug** stellt zahlenmäßig den größten Faktor im Bereich der Cyberkriminalität dar und ist auch maßgeblich für die anhaltend hohe Anzahl der Delikte verantwortlich. Mehr als die Hälfte der Internetdelikte fallen auf Betrugsdelikte: 2024 wurden 31.768 Fälle von Internetbetrug angezeigt, ein Rückgang von 6,8 Prozent im Vergleich zum Vorjahr. Mit der fortschreitenden Digitalisierung verlagern sich Betrugsdelikte immer mehr ins Internet. Für die Kriminellen ist es ein Leichtes, aufgrund technischer Anonymisierung sowie Verschleierung der Finanzflüsse Betrugshandlungen unerkannt und damit „sicher“ durchzuführen. Zusätzlich können durch den weltweiten Zugang zum Internet immer

mehr Menschen als potenzielle Opfer angesprochen werden. Der Bestellbetrug, sowohl kauf- als auch verkaufsseitig, gehört hierbei zu den größten Bereichen, gefolgt von unbefugten Abbuchungen von Bankkonten der Opfer. Auch der Anrufbetrug (Stichwort „falscher Polizist“) und international agierende Callcenter trieben die Statistik in die Höhe, ebenso der digitale Investmentbetrug.

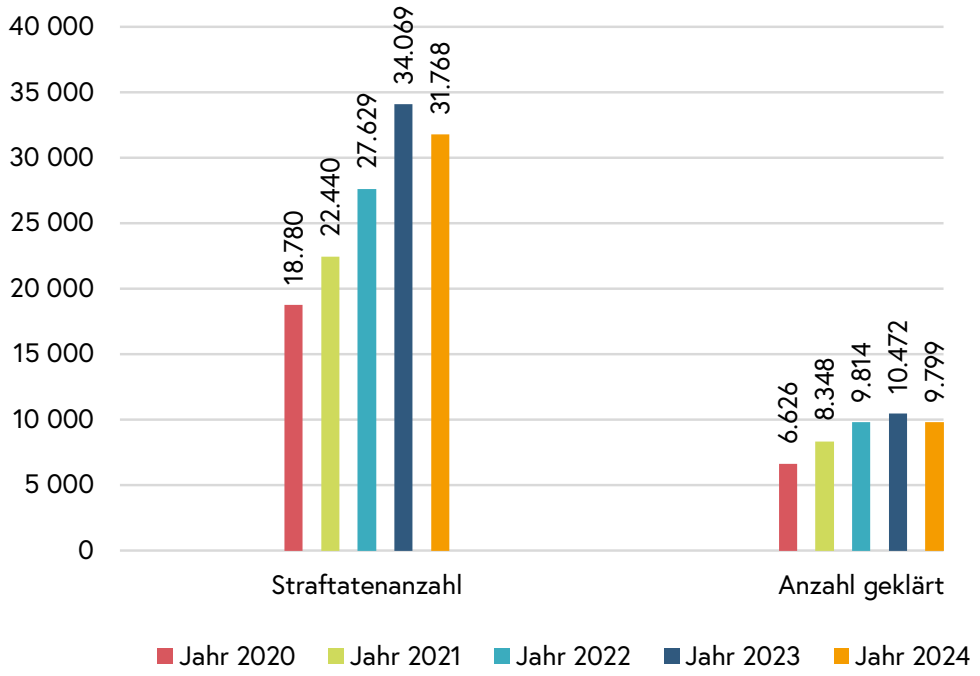

Abbildung 6: Fünf-Jahres-Vergleich Internetbetrug §§ 146–148 StGB (Örtlichkeit „Internet“)

Unter **sonstiger Kriminalität im Internet** versteht man Straftaten, die ihren Tatort im Internet haben. Ausgenommen sind Cybercrime im engeren Sinn, der Internetbetrug, bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellungen minderjähriger Personen (§ 207a StGB) und die Anbahnung von Sexualkontakten zu Unmündigen (§ 208a StGB). Im Bereich der sonstigen Kriminalität im Internet wurde im Jahr 2024 ein deutlicher Anstieg der Delikte verzeichnet. Eine zunehmende Verlagerung klassischer Strafrechtsdelikte ins Internet lässt sich seit Jahren beobachten. Gleichzeitig werden sogenannte „Crime as a Service“-Leistungen im Darknet angeboten. Dabei handelt es sich vorwiegend um Hacking Tools oder Erpressungstrojaner. Ebenso wird ein vermehrter Vertrieb von Falschgeld, Kinderpornografie und Kreditkartendaten wahrgenommen.

Zunahmen wurden beispielsweise bei § 107 StGB (Gefährliche Drohung, 1.472 Anzeigen) und § 283 StGB (Verhetzung, 309 Anzeigen) verzeichnet. Auch Anzeigen nach dem Verbotsgesetz (Wiederbetätigung) waren im Steigen begriffen (beispielsweise 1.222 Anzeigen nach § 3g VerbotsG).

SMS-Nachrichten wurden erneut zum Daten-Phishing verwendet: Es kursierten mehrere Spam-Kampagnen, die einen Hinweis auf eine angebliche „Zustellbenachrichtigung“ und weiterführende Links enthielten. Verstärkt sind hier Links von inexistenten Zahlungsdienstleisterinnen und Zahlungsdienstleistern verwendet worden. Gegen Jahresende – in der Vorweihnachtszeit – war wieder die saisonal beobachtbare Anzahl an kriminellen Webshops (Fake- und Phishing-Shops) deutlich angestiegen. Auch waren zahlreiche Spamwellen mit Erpressermails (Sextortion) und E-Mails zum Phishing von Bankdaten im Umlauf. Ebenso wurde vielfach versucht, WhatsApp-Accounts zu stehlen, um damit weitere Betrugshandlungen durchzuführen.

Nach wie vor wurden durch organisierte Tätergruppierungen vermehrt sowohl E-Mails als auch SMS zum Daten-Phishing verwendet. So erhielten Betroffene Phishing-E-Mails im Namen der vermeintlichen Hausbank mit einem beigefügten Link. In dieser Nachricht wurden die Opfer von angeblich widerrechtlich vorgenommenen Abbuchungen auf deren Konten informiert oder aufgefordert, ihre Legitimation für Online-Banking zu verlängern.

Phishing-Betrug auf Kleinanzeigenplattformen trat auch im Jahr 2024 auf. Opfer möchten private Gegenstände auf Kleinanzeigenplattformen verkaufen. Kriminelle stellen den Kontakt zu den Opfern her und bekunden scheinbares Kaufinteresse. Die Kriminellen wirken seriös und ernsthaft interessiert. Schließlich wird von den Betrügerinnen und Betrügern vorgeschlagen, die Zahlung und die Übergabe der Ware mit einem Kurierdienst abzuwickeln.

Den Opfern wird ein Link zugeschickt, der sich in weiterer Folge als Phishing-Link herausstellt und die Konsumentinnen und Konsumenten auf eine gefälschte Webseite weiterleitet. Auf diesem gefälschten Portal wird der Eindruck vermittelt, die verkaufte Ware sei bereits bezahlt. Die Opfer werden weiter aufgefordert, ihre Kreditkartendaten einzugeben, damit der Betrag zurücküberwiesen werden kann. Mit dem Bestätigen der Freigabe wird schließlich kein Geld überwiesen. In Wirklichkeit geben die Betroffenen eine Zahlung frei und überweisen Geld an die Betrügerinnen und Betrüger.

Der sogenannte Tochter-Sohn-Trick ist dem Bundeskriminalamt seit dem Jahr 2021 bekannt. Kriminelle verschicken per SMS oder WhatsApp eine Nachricht an die Geschädigten. Darin geben sie sich als angebliche Tochter oder Sohn aus und erklären, eine neue Nummer zu haben. In weiterer Folge werden aufgrund von vorgetäuschten Spontangebrechen oder Notfällen dringende Geldforderungen kommuniziert. Zumeist werden ausländische Konten als Zahlungsempfänger übermittelt. Die Opfer überweisen im Glauben, der Tochter oder dem Sohn Gutes zu tun. Zumeist erfolgt der Transfer in Echtzeit. Mittels Installierung einer Ermittlungsgruppe, koordiniert durch die Abteilung 7.2 des Bundeskriminalamts und durch entsprechende Präventionsarbeit wird versucht, dieses Phänomen einzudämmen.

Ebenso konnte festgestellt werden, dass Hacker Künstliche Intelligenz (KI) für die Programmierung von Malware nutzen. Da es sich bei der KI um ein lernendes System handelt, ist anzunehmen, dass in Zukunft stets komplexere Schadsoftware damit erstellt wird. Neben Malware könnte die Software beim Erstellen von Darknet-Marktplätzen oder Phishing zum Einsatz kommen.

Ebenso konnte beobachtet werden, dass Anschlussdelikte nach einem Diebstahl oder Verlust von Bankomatkarten mit NFC-Funktion steigen. Derzeit können mit diesen Karten fünf Bezahlvorgänge bis 50 Euro ohne Eingabe einer PIN durchgeführt werden.

Erpressungen im Internet (§§ 144, 145 StGB)

Im Jahr 2024 war mit 2.931 angezeigten Erpressungen im Internet ein Rückgang der Anzeigen um 24,7 Prozent zu verzeichnen. Gleichzeitig konnte die Aufklärungsquote um 2,7 Prozent, von 5 Prozent im Jahr 2023 auf 7,8 Prozent im Jahr 2024, gesteigert werden.

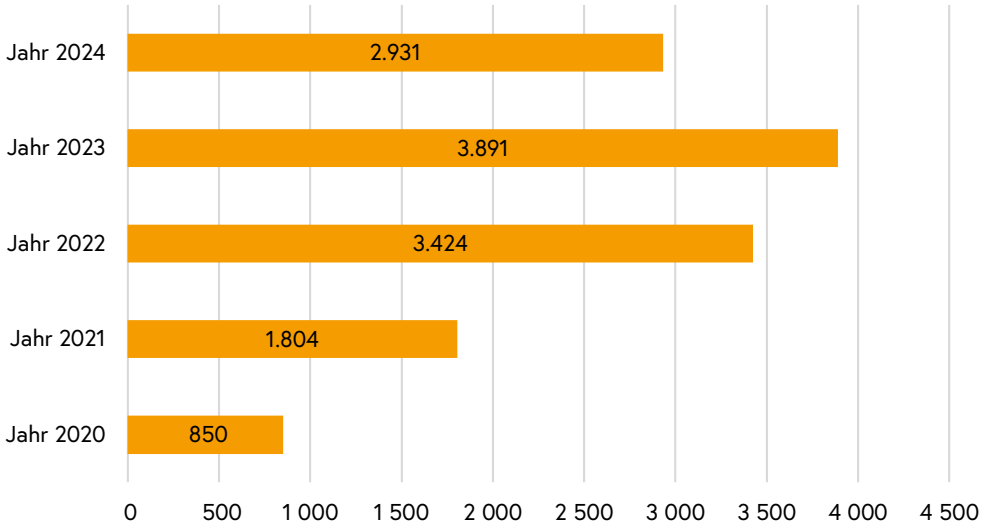

Abbildung 7: Erpressung im Internet – § 144 StGB (Erpressung), § 145 StGB (Schwere Erpressung)

Erpressung im Internet ist nach wie vor ein gängiges Geschäftsmodell krimineller Gruppierungen. Organisierte Tätergruppen sind dabei nicht nur durch das Versenden von Massenerpressungsmails, sondern auch durch Sextortion (Sex-Erpressung) im großen Stil überregional und transnational aktiv. Ein neues Phänomen in diesem Zusammenhang ist die Erpressung mittels sogenannter Police-Fake-Mail. Hier wird als „Fake"-Absender eine Polizeieinheit (Bundeskriminalamt, Polizei Wien und dergleichen) vorgetäuscht und mit einem Strafverfahren, beispielsweise wegen Kinderpornografie, gedroht, sollte der geforderte Geldbetrag nicht bezahlt werden. Das Bundeskriminalamt hat auf diese Entwicklung reagiert und gemeinsam mit den Landeskriminalämtern eine einheitliche und

strukturierte Vorgehensweise zur Bekämpfung der Gruppierungen hinter den genannten Kriminalitätsphänomenen festgelegt.

Delikt	Angezeigte Fälle 2023	Angezeigte Fälle 2024	Geklärte Straftaten 2023	Geklärte Straftaten 2024
		Internetbetrug		
§ 146 StGB	28.975	26.578	8.287	8.101
§ 147 StGB	3.579	4.404	1.168	1.332
§ 148 StGB	1.515	786	1.017	366
Gesamt	34.069	31.768	10.472	9.799

	Sonstige Kriminalität im Internet			
§ 105 StGB	373	341	206	235
§ 106 StGB	307	187	113	142
§ 107 StGB	1.209	1.472	1.040	1.303
§ 107a StGB	470	419	432	386
§ 111 StGB	0	15	0	13
§ 115 StGB	48	60	42	46
§ 207b StGB	0	0	0	0
§ 218 StGB	0	0	0	0
§ 223 StGB	150	125	119	95
§ 224 StGB	41	64	20	33
§ 228 StGB	1	2	1	2
§ 229 StGB	0	2	0	1
§ 231 StGB	63	44	19	12
§ 232 StGB	36	38	35	37
§ 241a StGB	2	3	0	1
§ 283 StGB	135	309	123	302
§ 297 StGB	0	10	0	10
§ 27 SMG	785	762	600	570
§ 28 SMG	12	8	10	7
§ 28a SMG	64	54	55	44
§ 30 SMG	34	45	33	40
§ 31 SMG	1	0	1	0
§ 31a SMG	0	0	0	0
§ 32 SMG	0	0	0	0

§ 3a VerbotsG	2	1	2	1
§ 3b VerbotsG	0	0	0	0
§ 3d VerbotsG	12	7	12	6
§ 3e VerbotsG	0	1	0	0
§ 3g VerbotsG	729	1.222	717	1.186
§ 3h VerbotsG	59	50	58	48
§ 4 NPSG	76	129	65	102
Sonstige Kriminalität im Internet Summe	**4.609**	**5.370**	**3.703**	**4.622**

Tabelle 5: Jahresvergleich 2023/2024 angezeigte Fälle von Cybercrime im weiteren Sinn nach Paragrafen

3.4 Dunkelziffer und Anzeigeverhalten

Die Dunkelziffer im Bereich der Internetkriminalität ist, wenn man internationale Studien berücksichtigt, besonders hoch. Viele Betroffene scheuen die Anzeige bei der nächsten Polizeidienststelle, teils aus Scham, Angst vor Reputationsverlust oder weil angenommen wird, dass der Fall ohnehin nicht verfolgt werden könnte oder der Schaden der einzelnen Opfer oftmals gering ist.

Jedoch kann mit jedem angezeigten Vorfall die Beweismittellage zu verdächtigen Tätergruppen weiter verdichtet werden. Außerdem verbessert die Anzahl der Anzeigen die frühere Erkennung von neuen Massenphänomenen für die ermittelnden Strafverfolgungsbehörden. Ebenso können Präventionsmaßnahmen zeitnaher gesetzt werden. Mit zielgerichteten Warnhinweisen an die Bevölkerung kann die Anzahl der Geschädigten reduziert werden. Eine Wiedererlangung abhanden gekommener Vermögenswerte gelingt jedoch selbst nach internationaler Ausforschung der Kriminellen nur in den seltensten Fällen. Die Verhinderung von Straftaten erfolgt durch verstärkte Bewusstseinsbildung der Bürgerinnen und Bürger und gleichzeitig erhöht Aufklärung die Aufmerksamkeit für Internetbetrug. Die Kriminellen nutzen menschliche Schwächen wie Gier und Sehnsüchte nach Anerkennung oder Beziehungen aus, um sich selbst zu bereichern. Auch im Jahr 2024 blieb Social Engineering ein maßgeblicher Angriffsvektor.

4 Ermittlungserfolge (Beispiele)

4.1 LoopX

Im Zeitraum von Dezember 2017 bis Februar 2018 bot eine Tätergruppe unter dem Vorwand, eine neue Kryptowährung namens LoopX einzuführen, zehn Millionen Token zum Verkauf an, die ausschließlich über Bitcoin und Ethereum erworben werden konnten. Nachdem weltweit hunderte Investoren in diese Token investiert hatten, löschten die Verdächtigen ihre Online-Präsenzen und verschwanden mit den Einlagen der Opfer – ein Vorgehen, das als „Exit Scam" bezeichnet wird.

Unter der Leitung der Wirtschafts- und Korruptionsstaatsanwaltschaft (WKStA) analysierten Ermittlerinnen und Ermittler des Cybercrime-Competence-Centers (C4) im Bundeskriminalamt (BK) zwischen Dezember 2022 und März 2024 die Transaktionen der Kryptowährungen und stellten fest, dass die Gruppe hauptsächlich in Österreich agierte, mit Verbindungen nach Deutschland, Tschechien, Thailand und Zypern.

In Zusammenarbeit mit Eurojust und den Behörden der beteiligten Länder wurden europäische Haftbefehle erwirkt. Im Herbst 2023 fanden koordinierte Aktionen in Linz, Graz, Prag und Zypern statt – unterstützt durch das Einsatzkommando Cobra sowie IT-Expertinnen und IT-Experten von Europol, die zu mehreren Hausdurchsuchungen, Sicherstellungen und drei Festnahmen führten. Bis Anfang 2024 wurden insgesamt sechs Personen festgenommen, darunter österreichische Staatsbürger im Alter von 29 bis 40 Jahren sowie ein 34-jähriger tschechischer Staatsangehöriger.

Die Ermittlungen führten zur Sicherstellung von rund 750.000 Euro in verschiedenen Währungen, zwei Fahrzeugen und einer Immobilie im Wert von knapp 1,4 Millionen Euro. Die Gesamtschadenssumme beläuft sich auf etwa sechs Millionen Euro.

Weiterführende Informationen: https://www.europol.europa.eu/media-press/newsroom/news/austrian-scammers-escape-investors-not-law-enforcement?mtm_campaign=newsletter

4.2 LabHost

Strafverfolgungsbehörden aus 19 Ländern haben eine der weltweit größten Phishing-as-a-Service-Plattformen, bekannt als LabHost, zerschlagen. Die einjährige Operation, die international von Europol koordiniert wurde und an der auch das Cybercrime-Competence-Center des Bundeskriminalamts beteiligt war, führte zur Kompromittierung der Infrastruktur von LabHost.

Insgesamt wurden weltweit 70 Adressen durchsucht, was zur Festnahme von 37 Verdächtigen führte. Darunter waren auch vier Personen in Großbritannien, die mit dem Betrieb der Website in Verbindung stehen, sowie die ursprünglichen Entwicklerinnen und Entwickler des Dienstes.

Die LabHost-Plattform, die zuvor offen im Internet verfügbar war, wurde abgeschaltet. Die internationale Untersuchung wurde von der britischen London Metropolitan Police geleitet und vom Europäischen Zentrum für Cyberkriminalität (EC3) von Europol und der Joint Cybercrime Action Taskforce (J-CAT) unterstützt.

Abbildung 8: Screenshot – © Europol https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost

Europol arbeitete an diesem Fall bereits seit September 2023. In der Zentrale wurde ein operativer Sprint mit allen beteiligten Ländern organisiert, damit nationale Ermittlerinnen und Ermittler Informationen über Nutzerinnen und Nutzer sowie Opfer in ihren eigenen Ländern sammeln und auswerten konnten.

Cybercrime as a Service hat sich zu einem rasant wachsenden Geschäftsmodell in der kriminellen Landschaft entwickelt. Dabei vermieten oder verkaufen Bedrohungsakteurinnen und Bedrohungsakteure Tools, Fachwissen oder Dienstleistungen an andere Cyberkriminelle, um ihre Angriffe durchzuführen. Dieses Modell ist bei Ransomware-Gruppen etabliert und wird auch in anderen Bereichen der Cyberkriminalität, beispielsweise bei Phishing-Angriffen, eingesetzt.

LabHost hat sich zu einem wichtigen Werkzeug für Cyberkriminelle weltweit entwickelt. Gegen ein monatliches Abonnement bot die Plattform Phishing-Kits, Infrastruktur zum Hosten von Seiten, interaktive Funktionen für die direkte Interaktion mit Opfern sowie Kampagnenübersichtsdienste.

Die Untersuchung deckte mindestens 40.000 Phishing-Domänen auf, die mit LabHost verknüpft waren und weltweit rund 10.000 Benutzerinnen und Benutzer hatten.

Gegen eine monatliche Gebühr von durchschnittlich 249 US-Dollar bot LabHost eine Reihe illegaler Dienste an, die individuell anpassbar und mit wenigen Klicks einsatzbereit waren. Je nach Abonnement stand Kriminellen eine wachsende Auswahl an Zielen zur Verfügung, darunter Finanzinstitute, Postdienste und Telekommunikationsanbieter. LabHost bot seinen Nutzerinnen und Nutzern eine Auswahl von über 170 gefälschten Websites mit überzeugenden Phishing-Inhalten an.

Weiterführende Informationen: https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost

4.3 OP Synergia II

Eine globale Interpol-Operation namens Synergia II, die vom 1. April bis 31. August 2024 durchgeführt wurde, führte zur Abschaltung von über 22.000 kriminell genutzten IP-Adressen und Servern, die mit Cyberbedrohungen wie Phishing, Ransomware und Informationsdiebstahl in Verbindung standen. An der Operation beteiligten sich 95 Interpol-Mitgliedsländer sowie Partnerinnen und Partner aus dem Privatsektor. Insgesamt wurden etwa 30.000 verdächtige IP-Adressen identifiziert, von denen 76 Prozent deaktiviert wurden. 59 Server wurden beschlagnahmt und weitere elektronische Geräte sichergestellt. Die Operation führte zur Verhaftung von 41 Personen, gegen 65 weitere wird ermittelt.

Interpol betonte die Notwendigkeit einer globalen Antwort auf die weltweite Natur der Cyberkriminalität und hob hervor, dass durch die gemeinsame Anstrengung nicht nur kriminelle Infrastrukturen zerschlagen, sondern auch hunderttausende potenzielle Opfer vor Cyberkriminalität geschützt wurden.

4.4 OP VICTORIA

Die Zentralstelle zur Bekämpfung der Rip-Deal-Kriminalität des Landeskriminalamtes Wien (Rip-Deal-Unit Vienna) feiert im Jahr 2025 ihr fünfjähriges Bestandsjubiläum. Ziel ist, den Aktivitäten organisierter, meist europaweit agierender Clans bezüglich der Modi Operandi hinsichtlich Rip Deal und Rip Deal 2.0 entgegenzuwirken.

Dies geschieht insbesondere durch Struktur- und Szeneermittlungen, kriminalpolizeiliche Ermittlungen auch operativer Natur und durch Ermittlungen im IT- und Krypto-Bereich. So gelingt es, Angriffswellen zu erkennen, diese zu Fallkomplexen zusammenzufassen und in weiterer Folge zentral zu bearbeiten.

Rip-Deal-Betrügerinnen und -Betrüger operieren oftmals in internationalen Netzwerken. Sie tarnen sich als reiche Geschäftsleute oder Investoren und bieten den Opfern scheinbar lukrative Geschäftsmöglichkeiten an. So geben sie beispielsweise vor, hochpreisige Güter kaufen zu wollen und schädigen ihre Opfer oft um hunderttausende Euro, indem sie bei der Bezahlung echtes Geld gegen Falschgeld tauschen. Die Betrügerinnen und Betrüger gehen hierbei meist arbeitsteilig vor.

Bei Rip Deal 2.0 wird mit Kryptowährung statt mit Bargeld gearbeitet. Die Opfer glauben oft, dass sie gehackt wurden. Die Kriminellen hacken jedoch nicht, sondern spähen die Passwörter aus.

Im konkreten Fall erstattete Ende September 2023 ein österreichischer Immobilienentwickler bei einer Wiener Polizeiinspektion Anzeige wegen eines Rip Deals 2.0 (Rip Deal mit Kryptowährung). Es war geplant, Fremdkapital für die Finanzierung von Luxusimmobilien zu lukrieren, um dies geschäftsüblich abwickeln zu können. Die Tätergruppierung trat an das Opfer über seriöse Plattformen heran und suggerierte die Bereitstellung einer Finanzierungssumme in Höhe von 23 Millionen Euro für die Objekterrichtung. Es folgten wochenlange Korrespondenzen, um Geschäftsmodalitäten sowie persönliche Treffen im Ausland abzuhandeln – um die Professionalität der Täterschaft zu untermauern. Für die Abwicklung der Finanzierungssumme wurde seitens der Kriminellen eine Provisionssumme in ETH (Kryptowährung Ethereum) gefordert, die jedoch nicht transferiert, sondern lediglich über eine Non-Custodial-Wallet gehalten und in der Blockchain nachgewiesen werden sollte.

Trotz örtlicher Trennung gelang es den Kriminellen, die Kryptovermögenswerte in deren Verfügungsmacht zu ziehen. Die Kriminellen haben technische Sicherheitslücken in Non-Custodial-Wallet-Applikationen erkannt und diese für die Tatausführung genutzt. In diesem Fall wären Opfer auch bei vorhandenem technischem Know-how machtlos gewesen.

Bild 1: Hintergrund der Startseite einer Fake-Homepage, die von vermeintlichen Investoren aufgesetzt wurde (Ermittlungsakt LKA Wien)

Am Tag der Erstinformation über den Betrugssachverhalt wurde durch die Rip-Deal-Unit Vienna im Sinne von technischen Sofortmaßnahmen das Cybercrime-Competence-Center des Bundeskriminalamts (Ermittlungsgruppe Blockchain) verständigt. Alle notwendigen Parameter wurden übermittelt. Ein sofort eingerichtetes 24/7-Monitoring führte schlussendlich dazu, dass fast die komplette Schadensumme (umgerechnet 265.000 Euro in ETH) auf den Seychellen eingefroren und der Vermögenssicherung zugeführt werden konnte.

Die Ermittlungen entwickelten sich rasant über mehrere europäische Mitgliedsstaaten und brachten eine Vielzahl an justiziellen Rechtshilfen und europäischen Ermittlungsanordnungen mit sich. Unter Einbindung des österreichischen Außenministeriums (BMEIA) wurde der justizielle Weg nach Afrika erfolgreich bestritten, um die Kryptovermögenswerte zu erlangen. Die Hauptverantwortlichen Rip Dealer, die gegenüber dem Opfer persönlich in Erscheinung traten, wurden ausgeforscht und 2024 in Belgien

festgenommen. In enger Kooperation der Rip-Deal-Unit Vienna und des Cybercrime-Competence-Centers mit belgischen Spezialermittlungsgruppen konnten den Kriminellen nach erfolgten Hausdurchsuchungen in Belgien rund 20 gleichgelagerte Fälle nachgewiesen werden. Die Kriminellen wurden zum Teil bereits in Belgien zu mehrjährigen unbedingten Freiheitsstrafen verurteilt beziehungsweise nach Österreich ausgeliefert.

Bild 2: Vermeintlicher Nachweis vorhandener finanzieller Mittel (Ermittlungsakt LKA Wien)

5 Aufbauorganisation und Abläufe

5.1 Nationale und internationale Koordinierungs-, Ermittlungs- und Meldestelle

Das Cybercrime-Competence-Center (C4) wurde 2011 zur Bekämpfung von Computerkriminalität als eigene Einheit innerhalb der Abteilung „Kriminalpolizeiliche Assistenzdienste“ des Bundeskriminalamts etabliert. Es ist zugleich nationale und internationale Koordinierungs-, Ermittlungs- und Meldestelle im Zusammenhang mit Cybercrime im engeren Sinn sowie für die elektronische Beweismittelsicherung und deren Auswertung zuständig. Das Cybercrime-Competence-Center (C4) dient aber auch allen Polizeidienststellen als wichtiger Koordinationspunkt bei landesweiten und international auftretenden Phänomenen und damit zusammenhängenden Ermittlungen.

Es gliedert sich mit seinen Schnittstellen zur **Direktion Staatsschutz und Nachrichtendienst (DSN)** als wesentlicher Bestandteil in die Strategie des Bundeskanzleramts ein. In diesem Zusammenhang ist das C4 Teil des **Inneren Kreises der operativen Koordinierungsstrukturen (IKDOK)**. Weiterführende Informationen zur Cybersicherheit können unter https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment.html nachgelesen werden.

5.2 C4-Meldestelle

Die Meldestelle zur Bekämpfung der Internetkriminalität ist seit über zehn Jahren im C4 etabliert und in einem 24/7-Betrieb rund um die Uhr erreichbar. Durch die Meldestelle kann gewährleistet werden, dass bei cyberrelevanten Vorfällen umgehend die erforderlichen Maßnahmen zur Gefahrenabwehr eingeleitet werden können.

Anfragen erhält die Meldestelle von den behördeneigenen Dienststellen und zunehmend auch Mitteilungen von Bürgerinnen und Bürgern, Unternehmen sowie nationalen und internationalen Polizeidienststellen.

Im **Jahr 2024** erreichten **14.594 Anfragen** die Meldestelle, wobei **8.119** davon einen Bezug zu Cybercrime hatten. Spam-Mails traten über das ganze Jahr verteilt auf, schwerpunktmäßig jedoch in den Monaten Jänner und Februar 2024 (gesamt 5.001). Damit kann eine Abnahme der eintreffenden Meldungen im Vergleich zum Vorjahr festgestellt

werden, die sich einerseits auf verstärkte Präventionstätigkeiten seitens der Kriminalpolizei und nichtstaatlicher Organisationen sowie auf ein vermehrtes Bewusstsein in der Bevölkerung zurückführen lässt, andererseits aber auch auf eine Diversifizierung der Meldemöglichkeiten für Unternehmen und Bevölkerung.

Beispielhaft können in diesem Zusammenhang folgende Seiten erwähnt werden:

https://www.onlinesicherheit.gv.at/Themen/Erste-Hilfe/Meldestellen.html
https://www.watchlist-internet.at/
https://www.ombudsstelle.at/
https://www.wko.at/it-sicherheit/cyber-security-hotline
https://zara.or.at/de/beratungsstellen
https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/Beschwerde_Meldung.de.html
https://www.stopline.at/de/home
https://dsn.gv.at/402/

In ihrer zentralen Funktion als Cybercrime-Schnittstelle innerhalb polizeiinterner Strukturen sowie als Meldestelle für Bevölkerung und Wirtschaft agiert die Unit als Koordinierungs- und Informationszentrum für diesen Themenkreis. Zusätzlich umfasst diese Tätigkeit auch proaktive und präventive Maßnahmen. Dabei auftretende Phänomene, insbesondere im Bereich von Phishing-Attacken, werden auch ministeriumsübergreifend koordiniert sowie notwendige Maßnahmen eingeleitet. Die deutlich erkennbare Sensibilisierung und Bewusstseinsbildung zum Thema Cybercrime erfolgt auch durch die fortlaufende Kooperation mit unterschiedlichen Institutionen aus dem Bereich der Wirtschaft und Vereinen, wie beispielsweise der WKO oder der Initiative „Watchlist Internet“. Ebenso führen Erstanalysen der eingehenden Meldungen zu schnellen Informationsweitergaben aktueller Phänomene, damit akute, negative Auswirkungen minimiert werden können. Für diese Aufgaben ist ein technischer Journaldienstbetrieb eingerichtet, der in dringenden Fällen organisationsübergreifende Informations- und Sofortmaßnahmen einleiten kann.

Da die Meldestelle auch als Drehscheibe zu anderen internationalen Dienststellen und Polizeieinheiten – wie dem Interpol Digital Cyber Center (IDCC), dem Europäischen Cybercrime Center (EC3) und den jeweiligen High Tech Crime Units anderer Staaten (NCPs) fungiert – konnte im Bereich der internationalen Anfragen und Unterstützungen, insbesondere im Hinblick auf Vorabsicherungen von Daten und diesbezügliche Ermittlungen im Sinne der Budapester Cybercrime Convention, ein entsprechender Anstieg der Anfragen und damit verbundene Ermittlungsaufgaben vermerkt werden.

Kontakt:
Bundeskriminalamt – Meldestelle Cybercrime
E-Mail: against-cybercrime@bmi.gv.at

Berichts-monat	Anzahl der relevanten E-Mail-Meldungen	Anzahl der relevanten Telefonmeldungen	Relevante Web-Frontend Meldungen	Summe aller Meldungen
2024 01	610	65	134	2.248
2024 02	454	73	97	1.217
2024 03	504	56	71	1.008
2024 04	523	66	132	1.146
2024 05	545	50	74	1.173
2024 06	616	39	20	1.221
2024 07	642	51	24	1.086
2024 08	567	42	12	1.061
2024 09	530	30	16	903
2024 10	560	64	14	1.057
2024 11	630	51	38	1.191
2024 12	628	59	32	1.283

Tabelle 6: Monatliche Übersicht aller Meldungen an die C4-Meldestelle

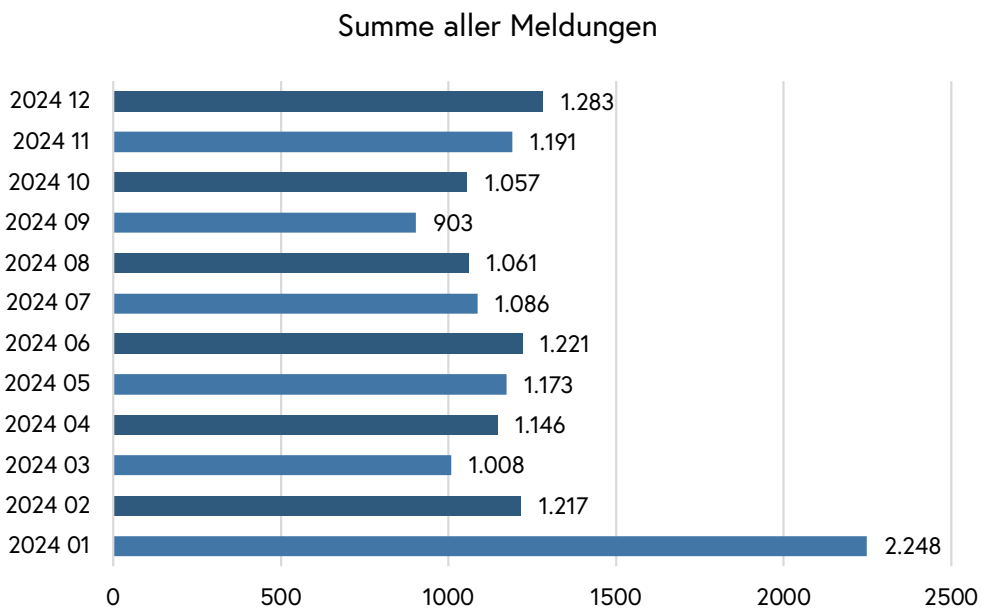

Abbildung 9: Gesamtanzahl der Meldungen an die C4-Meldestelle nach Monaten (Jahresverlauf)

5.3 Digitales Beweismittelmanagement (DBM)

Der Bereich „Digitales Beweismittelmanagement“ (DBM) im C4 besitzt die Kompetenzen, die für eine zeitgemäße kriminalpolizeiliche Bearbeitung komplexer Fälle mit großen Datenmengen notwendig sind. Das umfasst die technische Aufbereitung sichergestellter digitaler Beweismittel für eine systematische Indizierung und nachfolgende Bereitstellung für die Ermittlungsbereiche im Bundeskriminalamt oder in den Landeskriminalämtern sowie das Fallmanagement als Schnittstelle zwischen Forensik, Ermittlungen, Technik und der Justiz.

Die Auswahl, Inbetriebnahme und laufende Betreuung moderner Auswertesoftware gehören ebenso zu den Aufgaben des Bereichs wie die zeitnahe, fallspezifische Adaptierung einer flexiblen digitalen Arbeitsumgebung für die kooperative Fallbearbeitung von Kriminalfällen mit erhöhter technischer Komplexität.

Dabei werden folgende Aufgaben und Ziele verfolgt:

- modernes Fallmanagement für technisch komplexe Kriminalfälle,
- zeitnahe Bereitstellung einer fallspezifisch angepassten digitalen Arbeitsumgebung für Ermittlungen sowie Forensik,
- Etablierung einer Schnittstelle zwischen beteiligten kriminalpolizeilichen Fachbereichen zur optimierten, reibungsfreien Fallbearbeitung sowie
- Auswahl und Einsatz moderner Software und performanter Hardware, um große digitale Beweismittelmengen überhaupt erst durchsuchbar und bearbeitbar zu machen.

Bild 3: Serverlandschaft des C4

Mithilfe spezieller Programme zur Sichtung großer Datenmengen wurden 2024 insgesamt 61 neue Fälle mit einem Analyseausgangsdatenvolumen von über 64 Terabyte erstellt. Zusätzlich wurden über 130 separate virtuelle Maschinen zur Beweismittelsichtung und fallbezogenen Recherche in Betrieb genommen, womit insgesamt über 1.000 Ermittlerinnen und Ermittler im Bundeskriminalamt und den LKAs Zugriff auf eine moderne Arbeitsumgebung zur Strafverfolgung erhalten haben. Im größten Einzelfall kooperieren mehr als 350 Ermittlerinnen und Ermittler sowie Dolmetscherinnen und Dolmetscher.

2024 war wie auch im Vorjahr die Modernisierung der vorhandenen Speicher- und Rechenkapazität sowie die Verbesserung der Vernetzung mit weiteren Dienststellen eine wesentliche Herausforderung. Darüber hinaus wurden einige Verbesserungen im Bereich der IT Security zur Reduzierung von Risiken im Umgang mit Schmutzdaten umgesetzt. Daneben wurde die enge Zusammenarbeit mit dem Team des Projekts SeILE (Schaffung einer IKT-Lösung für kriminalpolizeiliche Ermittlungen)

fortgeführt sowie mit technischen Proof of Concepts unterstützt. Des Weiteren wurde die technische Mitarbeit bei operativen Fallbearbeitungen im Cybercrime-Competence-Center intensiviert.

5.4 C4-Forensik

Die Auswertung von IT und Speichermedien stellte die betroffenen Forensikerinnen und Forensiker anhaltend vor große Herausforderungen. Nach wie vor sind unzählige Geräte mit beträchtlichen Datenmengen aufzubereiten, um ressourcenintensive Unterstützung zu gewährleisten. Wie aus der Statistik ersichtlich, war die IT-Forensik im Jahr 2024 erneut mit einer starken Zunahme der auszuwertenden Datenmenge konfrontiert. Dies lässt sich durch den Umstand erklären, dass die Zahl der Hausdurchsuchungen und der hiermit einhergehenden Auswertungen deutlich anstieg.

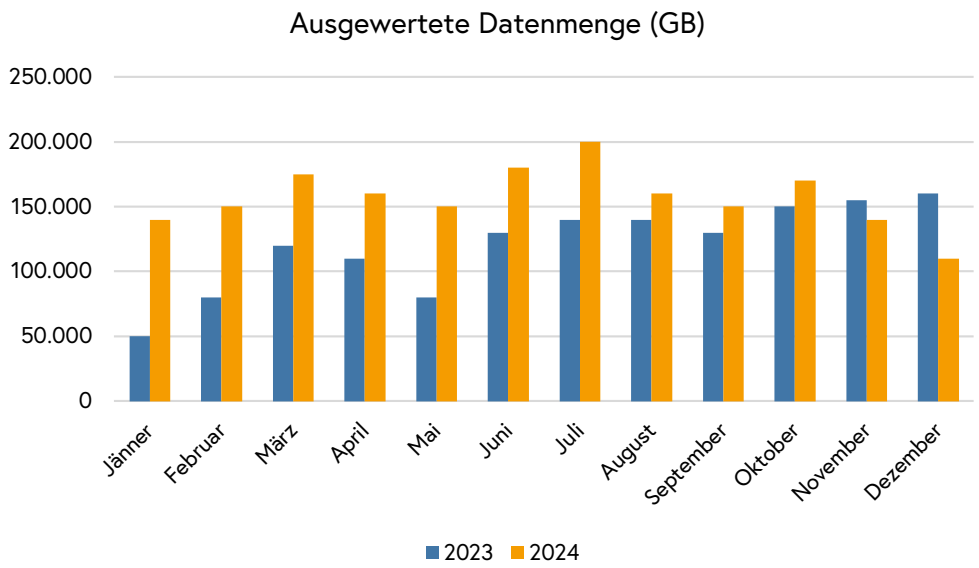

Abbildung 10: IT-Forensik – Ausgewertete Datenmengen in GB

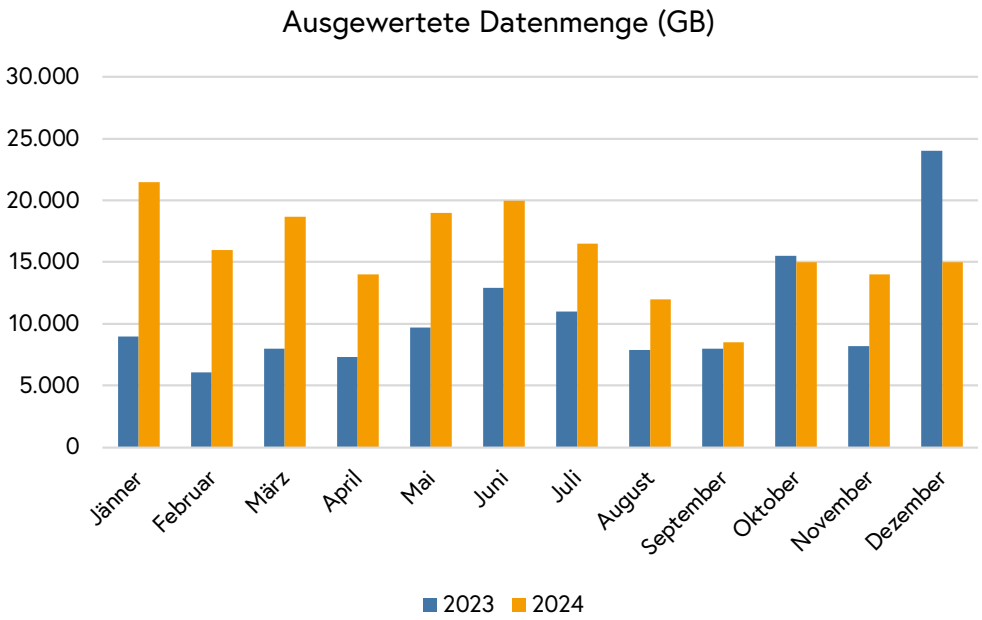

Abbildung 11: Mobile Forensik – Ausgewertete Datenmengen in GB

Aufgrund der rasanten technischen Entwicklungen und der eingesetzten Schutzmechanismen wird die Auswertung diverser Medien immer schwieriger. Herstellerspezifische Systeme mit ausgeprägten Verschlüsselungsverfahren stellen die elektronische Beweismittelsicherung fortwährend vor große Herausforderungen. Sowohl im Bereich der mobilen Forensik wie auch der IT-Forensik werden Datensicherungen und Auswertungen immer komplexer. Das C4 sieht sich zunehmend mit umfassenden Auswertungen von Smartphones und Clouds konfrontiert, um den Assistenzbereich AB06 ITB des Landeskriminalamts zu unterstützen. Die auszuwertenden Datenmengen (Festplatten, Netzwerkdaten und Mobiltelefone) bleiben auf hohem Niveau.

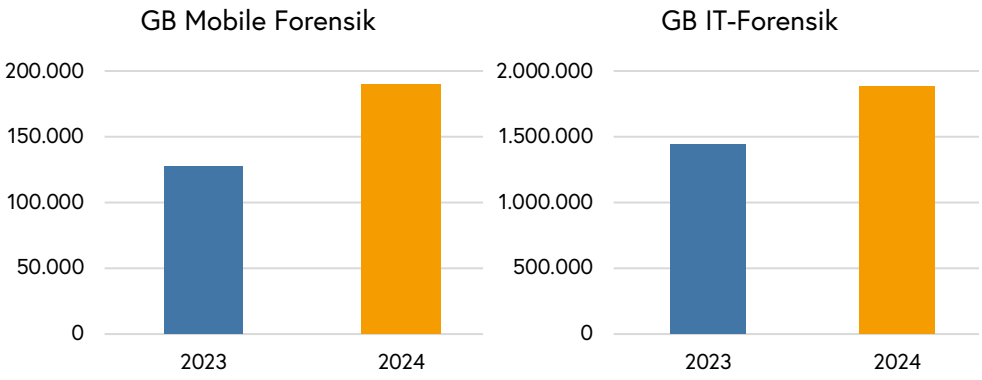

Abbildung 12: Mobile-Forensik und IT-Forensik – Gegenüberstellung der ausgewerteten Datenmengen der Jahre 2023 und 2024.

Das zeit- und ressourcenaufwendige Chip-Off-Verfahren, bei dem Memory-Chips von ihrer Hardware physisch entfernt werden sowie der Bereich KFZ-Forensik, können nur zentral im Cybercrime-Competence-Center (C4) durchgeführt werden. Im Jahr 2024 konnten 128 Chip-Off-Verfahren abgeschlossen werden.

Bei einigen schweren Straftaten – sowie im Bereich der organisierten Kriminalität oder bei der grenzüberschreitenden Schwerkriminalität – besteht ein direkter oder indirekter Bezug zu einem Kraftfahrzeug, indem dieses als Transport- und/oder Tatmittel verwendet wurde. Dem Kraftfahrzeug kommt ein hoher Stellenwert als Beweismittel zu. Die Informationen werden während des Betriebes automatisch generiert und gespeichert. Sie können bei entsprechend fachgerechter Auswertung und Aufbereitung für kriminalpolizeiliche Ermittlungen aber auch für das Strafverfahren von enormer Bedeutung sein. Durch die Bediensteten des Fachbereichs Automotive IT des Cybercrime-Competence-Centers werden bundesweit gerichtsverwertbare Beweisaufnahmen für alle Dienststellen des Bundesministeriums für Inneres und der Landespolizeidirektionen durchgeführt. Darüber hinaus wirken die Bediensteten der Automotive IT aktiv an Schwerpunktaktionen und operativen Einsätzen mit, wenn die sofortige Sicherung von Beweismitteln notwendig erscheint und Anordnungen der Staatsanwaltschaften vollzogen werden müssen. Insgesamt wurden 228 Fahrzeuge in der Berichtsperiode Jänner bis Dezember 2024 ausgewertet. Aufgrund ihrer besonderen Expertise werden sie häufig bei internationalen Ermittlungen zur Auswertung von Fahrzeugdaten hinzugezogen.

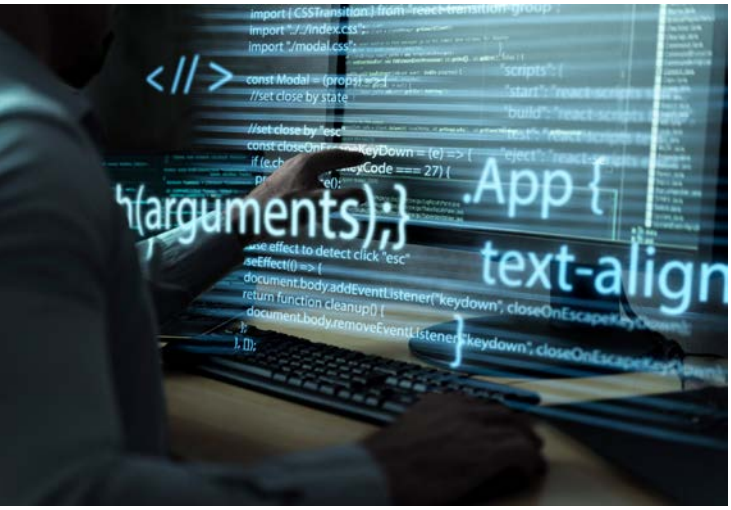

Bild 4: Entwicklung neuer Tools (© www.freepik.com)

5.5 Entwicklung und Innovation

Sowohl bei den aktuell pro Fall auftretenden Datenmengen als auch bei der Komplexität der darin enthaltenen Zusammenhänge sowie der von der Täterschaft verwendeten Technologien ist es immer häufiger nötig, bei der Fallbearbeitung nicht nur auf die bewährten Fähigkeiten im Ermittlungsbereich zurückzugreifen, sondern auch wissenschaftliche Unterstützung hinzuzuziehen.

Eine der Aufgaben des Büros 5.4 – Entwicklung und Innovation – ist, genau diese Unterstützung zu leisten. Dies umfasste im Jahr 2024 komplexe mathematische Analysen von Geldflüssen in diversen Kryptowährungen, Analysen von forensischen Artefakten, Entschlüsselungen von Daten und Datenträgern und zahlreiche andere Hilfestellungen. In mehreren Fällen wurden die Ermittlungen durch die Erstellung von Scripts und Tools unterstützt.

Dabei sind das Erkennen und Nachweisen der zumeist hochkomplexen Zusammenhänge in enger Zusammenarbeit mit den Ermittlerinnen und Ermittlern nicht die einzige Herausforderung. Ebenso wichtig ist, die gewonnenen Erkenntnisse in einer übersichtlichen Form darzustellen, damit sie auch Personen ohne technische Ausbildung in geeigneter Weise präsentiert werden können.

Eine weitere Aufgabe des Büros 5.4 ist die Beobachtung und Analyse neuer Technologien auf ihre Bedeutung für die kriminalpolizeiliche Arbeit. Hier wurde einer der Schwerpunkte auf Künstliche Intelligenz gelegt. Speziell zu diesem Thema, aber auch in vielen anderen Bereichen, ist die Zusammenarbeit mit nationalen und internationalen Polizeiorganisationen und auch mit Forschungseinrichtungen entscheidend. Deshalb wurde sowohl in mehreren nationalen als auch internationalen Projekten, Arbeitsgruppen und Gremien mitgearbeitet.

Gerade im Cybercrime-Bereich gewinnt die Präventionsarbeit immer mehr an Bedeutung, da sich zum Beispiel sehr viele Betrugsdelikte durch entsprechende Bewusstseinsbildung und daraus folgende Vorsicht verhindern ließen. Deshalb wurden auch im Jahr 2024 zahlreiche diesbezügliche Veranstaltungen von Ministerien, der Wirtschaftskammer und weiteren relevanten Organisationen mit Expertise unterstützt.

5.6 Wissensvermittlung durch Ausbildung und internationalen Austausch

Cyberkriminalität ist zu einer der größten Bedrohungen für die Gesellschaft geworden und erfordert eine entsprechende Reaktion seitens der Strafverfolgungsbehörden. Eine zentrale Komponente in diesem Kampf ist die Ausbildung von Polizeibediensteten im Bereich der Cyberkriminalitätsbekämpfung. Diese Ausbildungen sind von entscheidender Bedeutung, um die Fähigkeiten der Polizei zu stärken und sicherzustellen, dass sie effektiv auf die sich ständig wandelnden Bedrohungen reagieren kann.

Ein grundlegendes Verständnis der Technologie ist für alle Polizeibediensteten unerlässlich, da ein Großteil der begangenen Delikte einen Cyberbezug aufweist. Dieses Verständnis umfasst nicht nur Kenntnisse über Computersysteme und Netzwerke, sondern auch über Verschlüsselungstechnologien, Forensik und digitale Beweismittelsicherung, um im Anlassfall die notwendigen Ermittlungen einleiten und Beweismittelsicherungen durchführen zu können. Eine fundierte Ausbildung ermöglicht es, die zur Verfügung stehenden Werkzeuge und Techniken voll auszuschöpfen, um Kriminelle zu identifizieren und Beweise zu sammeln, die vor Gericht auch verwertbar sind.

Das Cybercrime-Competence-Center des Bundeskriminalamts führte bis 2024 eine umfassende Ausbildung für Bezirks-IT-Ermittlerinnen und -Ermittler durch. Mittlerweile

unterstützen mehr als 462 speziell ausgebildete Kolleginnen und Kollegen durch fachgemäße Erstmaßnahmen und Ermittlungen auf lokaler Ebene.

Die Cybercrime-Ausbildungen der Polizeibediensteten in den Bundesländern sind ab 2025 Zuständigkeit der Cybercrime-Training-Center (CCTC) der Landeskriminalämter, wodurch eine noch größere Reichweite gewährleistet werden soll. Das Cybercrime-Competence-Center des Bundeskriminalamts wird ab 2025 unterschiedliche Spezialausbildungen und Expertenschulungen anbieten.

Das Thema Cybercrime wird zielgruppengerecht weiterhin im Rahmen der kriminaldienstlichen Aus- und Fortbildung sowie in den Grundausbildungslehrgängen zugänglich gemacht.

Bereits 2023 wurde in enger Abstimmung mit dem Bundesministerium für Justiz (BMJ) eine eigene Ausbildungsreihe für Staats- und Bezirksanwältinnen und -anwälte sowie für Richterinnen und Richter entwickelt und durchgeführt, die sich im Sinne einer zielgerichteten Strafverfolgung speziell auf technische Hintergründe und hiermit einhergehende Ermittlungsmöglichkeiten im Cyber-Bereich fokussierte. Ziel war, einem möglichst großen Personenkreis Cybercrime-Grundkompetenzen zu vermitteln. Die Ausbildungen fanden jeweils in Form von Webinaren statt, wodurch es möglich war, einschlägiges kriminalpolizeiliches Fachwissen bundesweit an Staatsanwältinnen und Staatsanwälte, Bezirksanwältinnen und Bezirksanwälte sowie Richterinnen und Richter weiterzugeben. Die Kooperation mit dem BMJ wurde auch 2024 weitergeführt.

Elftes Internationales Symposium „Neue Technologien“ in Fürstenfeldbruck, Deutschland

Rund 250 internationale Expertinnen und Experten von Sicherheitsbehörden sowie aus Wissenschaft und Wirtschaft kamen zusammen und diskutierten über das Thema „Künstliche Intelligenz – Polizeiarbeit und Gesellschaft der Zukunft. Chancen und Herausforderungen“. Am 6. und 7. November 2024 fand im Churfürstensaal der Hochschule für den öffentlichen Dienst in Bayern (HföD) das Internationale Symposium „Neue Technologien“ statt. Bereits zum elften Mal veranstalteten das Cybercrime-Competence-Center (C4) des Bundeskriminalamts Österreich, das Bayerische Landeskriminalamt, das Landeskriminalamt Baden-Württemberg und die Schweizer Bundespolizei fedpol dieses länderübergreifende Symposium.

Bild 5: Symposium „Neue Technologien“ (NT 2024) in Fürstenfeldbruck, Bayern
(© Landeskriminalamt Bayern)

Künstliche Intelligenz (KI) hat sich von einem Nischenthema zu einer zentralen Technologie entwickelt. KI hat das Potenzial, auf beinahe alle Aspekte des Lebens und der Gesellschaft Einfluss zu nehmen. Es zeichnet sich bereits ab, dass KI auch für Behörden im Allgemeinen und die Polizei im Speziellen ein besonders wichtiges Zukunftsthema sein wird. Ziel des Symposiums war, neben der Vorstellung von laufenden Projekten marktreife Ergebnisse aus Forschung und Entwicklung sowie technische Herausforderungen und Bedürfnisse im polizeilichen Kontext zu präsentieren. Zudem war es beabsichtigt, eine Möglichkeit zu bieten, aktuelle gesellschaftspolitische Herausforderungen im Zusammenhang mit KI aus verschiedenen Perspektiven vorzustellen und zu diskutieren. Die Veranstaltung umfasste zahlreiche interessante Themen. Expertinnen und Experten aus unterschiedlichen Disziplinen präsentierten ihre Erkenntnisse und vertieften diese in Diskussionsrunden. Neben dem fachlichen Austausch bot das Symposium auch ein Forum für umfassende länderübergreifende Vernetzung und Kooperation.

Fachtagung der IT-Ermittlerinnen und -Ermittler sowie IT-Forensikerinnen und -Forensiker in Wien

Neueste Entwicklungen im Cyber-Bereich wurden bei der siebten Fachtagung für IT-Beweismittelsicherung (ITB) am 10. April 2024 fachlich erörtert.

Rund 220 IT-Ermittlerinnen und -Ermittler sowie Forensik-Expertinnen und -Experten vom Assistenzbereich 06 der Landeskriminalämter, aus den Bezirkspolizeikommanden und den Fachabteilungen des Bundeskriminalamts sowie Vertreterinnen und Vertreter weiterer Strafverfolgungsbehörden nahmen an der eintägigen Veranstaltung teil. Diese wurde vom Cybercrime-Competence-Center (C4) organisiert und fand im Festsaal des Bundeskriminalamts statt.

Bild 6: Fachtagung IT-Beweismittelsicherung (ITB) in Wien © BK 5

Themen waren die neuesten Entwicklungen im Cyber-Bereich und die damit einhergehende, zielgerichtete Bekämpfung der Cyberkriminalität. Diese stellt einen wesentlichen Schwerpunkt in der Sicherheitsstrategie des Innenministeriums dar. Der technologische Wandel schreitet stetig voran, unterschiedliche elektronische Services werden in nahezu allen Lebensbereichen angeboten und vielfach genutzt. Die neuen technischen

Möglichkeiten eröffnen aber auch unzählige Gelegenheiten für Missbrauch. Kriminelle gehen vermögens- und zielorientiert vor, was sich beispielsweise bei Phänomenen wie Ransomware, Caller-ID-Spoofing und dem von Jahr zu Jahr steigenden Internetbetrug zeigt.

Die Themensetzung im Rahmen der Tagung war mannigfaltig – angefangen bei Strategien zur Bekämpfung der Darknet-Kriminalität, Ermittlungsansätzen beim Missbrauch von SIM-Karten und eID, Künstlicher Intelligenz, Deep Learning und Deepfakes und der Vorstellung C4-eigener Ermittlungstools.

Ebenso wurden operative Fälle präsentiert, bspw. eine erfolgreich abgeschlossene Ermittlung in Zusammenhang mit einem über das Darknet erfolgten Mordauftrag. Rechtliche Hintergründe im Hinblick auf die Sicherstellung und Verwertung von Kryptowährungen sowie die Sicherstellung von Datenträgern wurden von der Staatsanwaltschaft Wien – Kompetenzstelle Cybercrime – erörtert.

5.7 ZASP – Zentrale Anfragestelle für Social-Media- und Online-Service-Provider

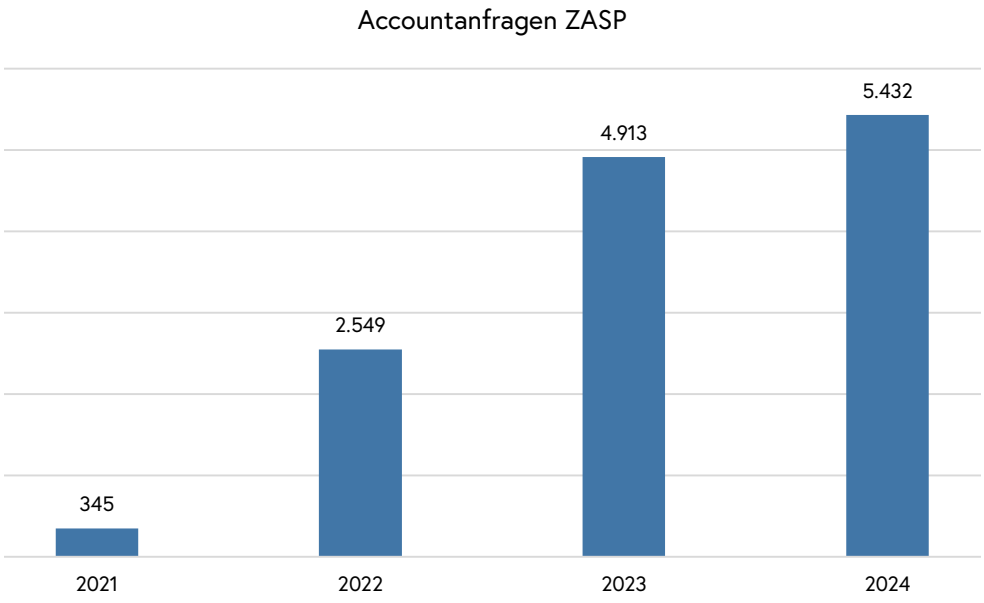

Abbildung 13: Accountanfragen im Jahresverlauf

Bei vielen Ermittlungen sind internationale Anfragen an Social-Media-Plattformen und ausländische Diensteanbieterinnen und Dienstanbieter im Internet erforderlich. Im Jahr 2024 wurden insgesamt 3.343 Anträge über die ZASP abgewickelt und dabei 5.432 Accountanfragen gestellt. Im gleichen Zeitraum langte von Facebook zu 84 Prozent, von

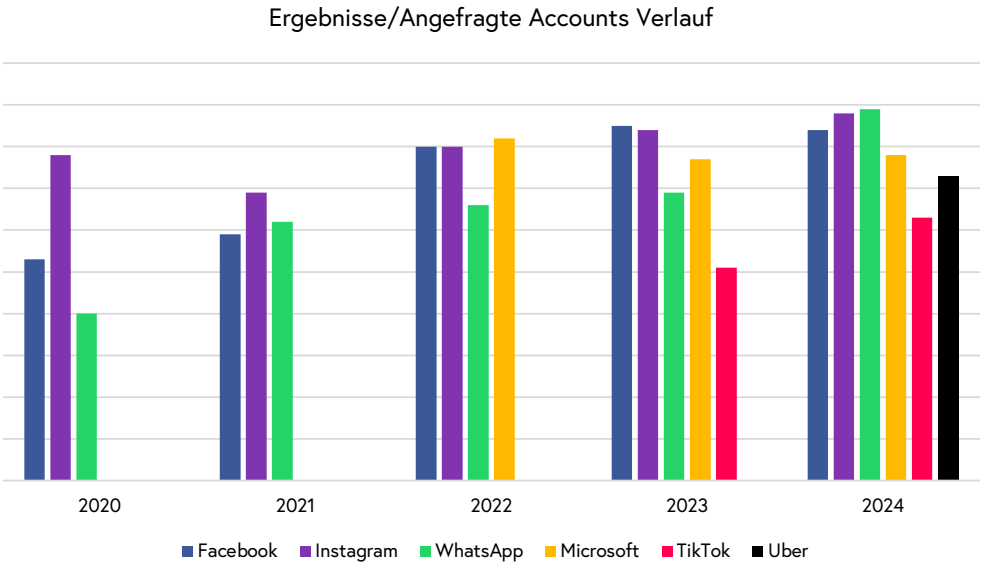

Abbildung 14: ZASP-Erfolgsquote im Jahresvergleich

Nach Etablierung der ZASP kann diese kriminalpolizeiliche Einheit als ein erfolgreiches Beispiel für zukunftsgerichtete Kooperationen zwischen Behörden und Kommunikationsplattformen angesehen werden. Durch die Zentralisierung und Vereinheitlichung der Anfragen konnte die Antwortquote enorm gesteigert werden.

Im März 2024 leistete die ZASP erfolgreich Unterstützung bei einer Fahndung nach einer Vergewaltigung und trug wesentlich zur Festnahme bei. Im Juni 2024 konnten Hinweise zu einem unbekannten Kriminellen nach einer Bombenanschlagsdrohung über soziale Medien ermittelt werden, nachdem durch die ZASP Anfragen an mehrere Diensteanbieterinnen und Dienstanbieter durchgeführt wurden.

In Zukunft kann davon ausgegangen werden, dass Anfragen an weitere Social-Media- und Service-Provider über die ZASP zentral für ganz Österreich abgewickelt werden. Hierdurch soll Cyberkriminalität noch effizienter, gezielter und schneller bekämpft werden.

6 Oberösterreich: Cybercrime-Training-Center-Jahresbericht

6.1 Zahlen und Fakten

Schulungsbetrieb und Teilnehmerzahlen im Überblick

In Oberösterreich wurde das Cybercrime-Training-Center (CCTC) mit einem Trainerteam von insgesamt 50 Personen eröffnet. Etwa 60 Prozent dieser Trainerinnen und Trainer stammen aus den Bezirkspolizeikommanden und üben dort neben ihrer Hauptfunktion auch Tätigkeiten als IT-Forensikerinnen und -Forensiker oder Cybercrime-Ermittlerinnen und -Ermittler aus. Die restlichen Trainer gehören zum Assistenzbereich AB06 – IT & Cybercrime des Landeskriminalamts Oberösterreich.

Der Schulungsbetrieb begann am 24. Juni 2024. In dieser initialen Phase nahmen vorwiegend Mitarbeiterinnen und Mitarbeiter des Landeskriminalamts sowie der Landespolizeidirektion teil. Diese erste Durchführungsphase diente primär dazu, die Umsetzbarkeit der ausgearbeiteten Inhalte zu testen und den Trainerinnen und Trainern, von denen manche bisher wenig Vortragserfahrung hatten, die Möglichkeit zu geben, sich mit ihrer neuen Rolle vertraut zu machen. Dank der sorgfältigen Vorbereitung des Schulungsprogramms kam es nur zu geringfügigen Unstimmigkeiten – etwa in Form von inhaltlichen Überschneidungen oder technisch aufwändigen Übungen mit begrenztem Mehrwert. Diese konnten durch die Flexibilität des Trainerinnen- und Trainerteams problemlos kompensiert werden. Aus diesem Grund wurden auch diese Pilotdurchgänge als vollwertige Grundmodul-Schulungen gewertet. (Anmerkung: Die festgestellten Unstimmigkeiten wurden im Zuge der Überarbeitung des Trainerhandbuchs im Dezember 2024 beseitigt. Zudem wurden aktuelle Themen wie zum Beispiel Künstliche Intelligenz ergänzt.)

In der Testphase wurden insgesamt 63 Personen einberufen, von denen 59 das Grundmodul vollständig absolvierten.

Mit dem 2. September 2024 begann der reguläre Schulungsbetrieb für die eigentliche Zielgruppe: Exekutivbedienstete von Polizeiinspektionen sowie Staatsanwältinnen und Staatsanwälte der Oberstaatsanwaltschaft Linz. Bis zum Jahresende 2024 nahmen 135 Personen am Grundmodul teil, von denen 124 die Schulung vollständig abschlossen.

Unter den Absolventinnen und Absolventen befanden sich sieben Staatsanwältinnen und Staatsanwälte aus Linz und Salzburg.

Um die für Vertreterinnen und Vertreter der Staatsanwaltschaft vorgesehenen Plätze optimal zu nutzen, wurden im Jahr 2025 – auf Ersuchen der Oberstaatsanwaltschaft Wien – auch Staatsanwältinnen und Staatsanwälte aus diesem Sprengel einbezogen, sofern durch Absagen oder kurzfristige Ausfälle Plätze frei wurden. Bis zum 25. April 2025 nahmen weitere 149 Personen am Grundmodul teil, darunter acht weitere Staatsanwälte aus den Staatsanwaltschaften Linz, Wels und Wien. 135 dieser Personen konnten das Modul erfolgreich abschließen.

Insgesamt wurden zwischen dem 24. Juni 2024 und dem 25. April 2025 somit 347 Personen für das Grundmodul einberufen, von denen 318 – darunter 15 Staatsanwältinnen und Staatsanwälte – die Schulung vollständig absolvierten. Drei der entsandten Staatsanwältinnen und Staatsanwälte kamen aus Wien.

Umfrageergebnisse zum Grundmodul im Cybercrime-Training-Center

Im Zeitraum vom 24. Juni 2024 bis zum 8. Mai 2025 wurde die Teilnahme am Grundmodul des Cybercrime-Training-Centers (CCTC) durch eine standardisierte Onlinebefragung evaluiert. Die Ergebnisse basieren auf den Rückmeldungen von 72 Exekutivbediensteten aus unterschiedlichen Organisationseinheiten und Dienstverrichtungen. Der Großteil der Teilnehmenden (69 Prozent) war auf Polizeiinspektionen tätig, wobei insbesondere Streifendienstbedienstete (68 Prozent) vertreten waren – und somit genau jene Zielgruppe, für die das Grundmodul konzipiert wurde.

Die Inhalte des Moduls wurden im Durchschnitt mit vier von fünf Punkten hinsichtlich ihrer Relevanz für die tägliche Praxis bewertet. 84 Prozent der Befragten gaben an, dass sie das im Kurs vermittelte Wissen bereits einmalig oder mehrfach im dienstlichen Kontext anwenden konnten. Besonders positiv wurde der praxisnahe Aufbau des Trainings hervorgehoben. So bewerteten 61 Prozent der Teilnehmenden die praktischen Übungen – etwa das Nachstellen von Hausdurchsuchungen oder den Aufbau von Netzwerkinfrastrukturen – als die effektivste Lehrmethode. Auch das im CCTC eingesetzte Team-Teaching wurde mehrheitlich positiv beurteilt: 95 Prozent bewerteten die Zusammenarbeit der Vortragenden mit „sehr gut“ oder „gut abgestimmt“.

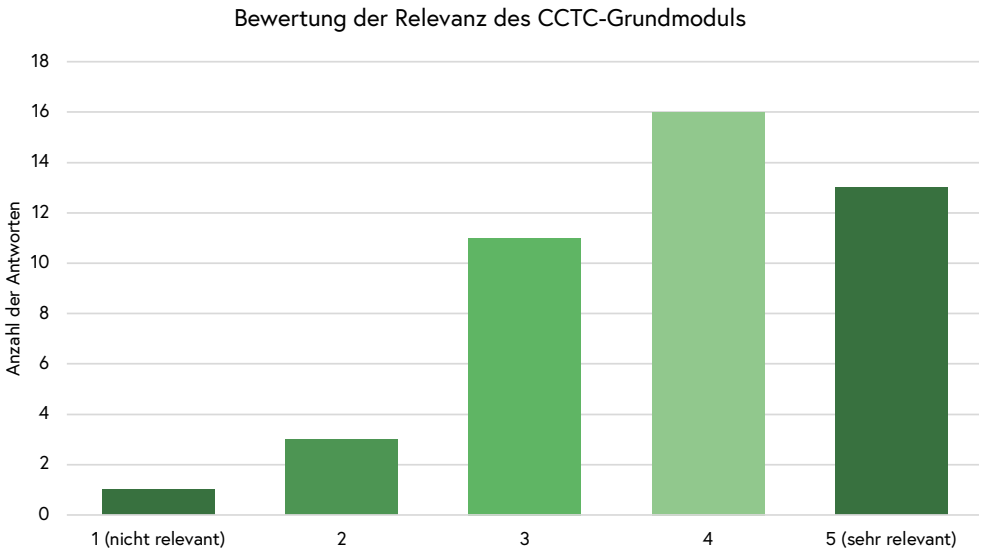

Abbildung 15: Bewertung der Relevanz des Grundmoduls

Inhaltlich wurden die Themen „Beweismittelsicherung“, „Hausdurchsuchung und Tatortverhalten“ sowie „Sicherung und Auswertung von Mobilgeräten“ als besonders relevant für den dienstlichen Alltag eingestuft. Gleichzeitig wurde vereinzelt der Wunsch geäußert, die Schulungsinhalte künftig um rechtliche Grundlagen zur Deliktszuordnung und praktische Hinweise zur Erstaufnahme bei Polizeiinspektionen zu ergänzen.

Die Lehrmethoden wurden insgesamt sehr positiv beurteilt. 61 Prozent nannten praktische Übungen als sinnvollste Methode, gefolgt von interaktivem Anschauungsmaterial (21 Prozent).

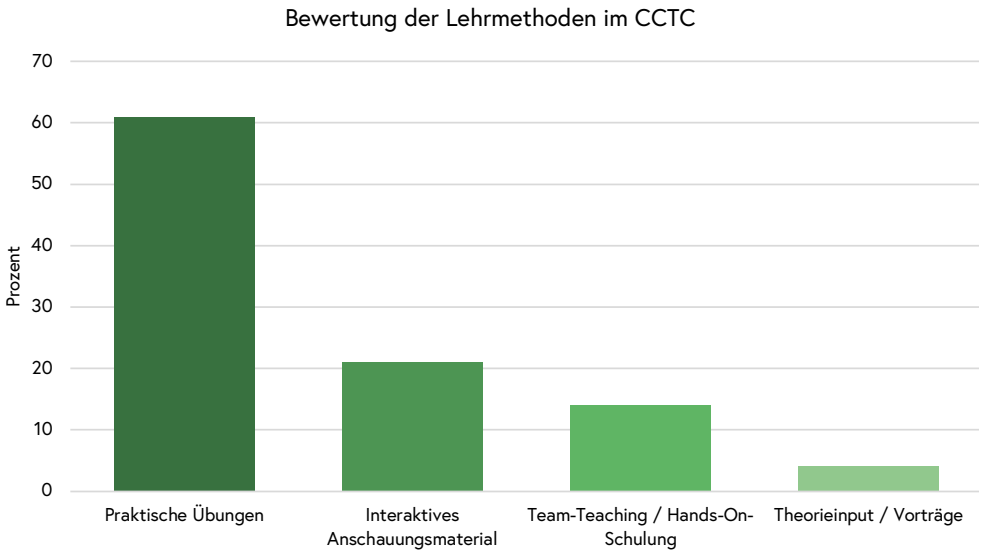

Abbildung 16: Bewertung der eingesetzten Lehrmethoden

Die Frage nach der eigenen Handlungssicherheit nach der Schulung zeigt ebenfalls ein klares Bild: 87 Prozent der Befragten fühlten sich nach Absolvierung des Grundmoduls besser oder sogar sehr gut gewappnet für die Aufnahme und Erstbearbeitung von Cybercrime-Anzeigen.

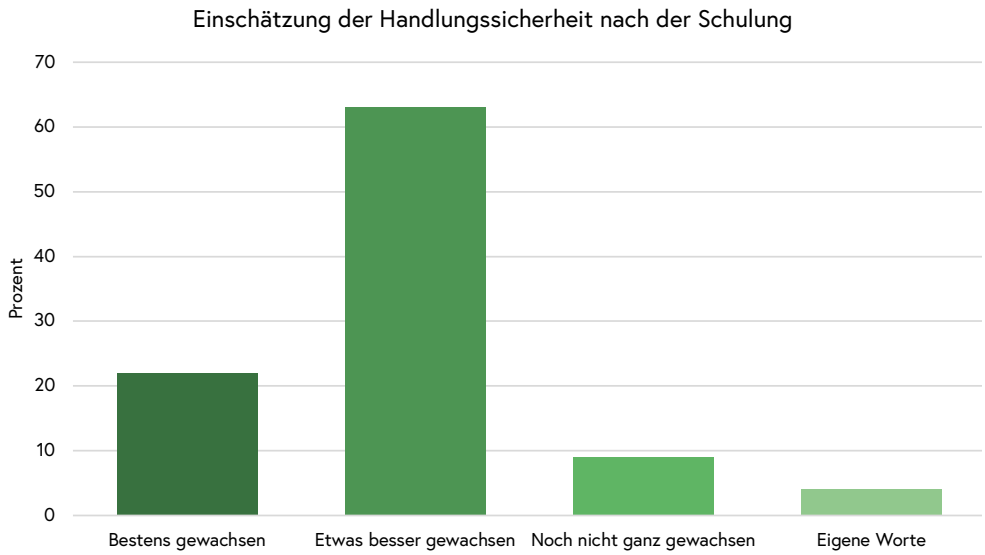

Abbildung 17: Einschätzung der Handlungssicherheit nach der Schulung

Insgesamt bestätigen die Ergebnisse nach wie vor, dass das Grundmodul im CCTC ein wirkungsvolles und zielgruppenadäquates Weiterbildungsformat darstellt.

6.2 Herausforderungen

Technische Hürden

Ein im Oktober 2024 erstellter Evaluierungsbericht stützt sich auf die gesammelten Erfahrungen während der Aufbauphase und des laufenden Betriebs des Cybercrime-Training-Centers. Zentrale Aspekte der Analyse bildeten dabei vor allem technische Herausforderungen sowie die Rückmeldungen der Schulungsteilnehmenden zur praktischen Anwendbarkeit der Infrastruktur.

Kompatibilitätsprobleme zwischen den eingesetzten Systemen (BAKS, Medientechnik, offene PC-Struktur) sowie nicht ideal auf den Schulungskontext abgestimmte Hard- und Softwarekomponenten stellten anfangs eine Herausforderung dar. Diese konnten jedoch durch das engagierte Vorgehen der Technikerinnen und Techniker des Assistenzbereichs AB06 erfolgreich gelöst werden. Darüber hinaus trugen gezielte, kostenbewusste Zusatzbeschaffungen wesentlich dazu bei, kleinere Störungen zu beheben und einen stabilen Schulungsbetrieb sicherzustellen.

Organisatorische Komplexität
Eine der zentralen organisatorischen Herausforderungen stellt die personelle Ressourcenplanung dar. Für einen durchgehenden Betrieb des Grundmoduls im CCTC mit monatlichem (maximal einmaligem) Einsatz jeder Trainerin beziehungsweise jedes Trainers werden mindestens 32 Vortragende benötigt, um die Kontinuität des Schulungsbetriebs gewährleisten zu können.

In Oberösterreich steht zwar ein Trainerinnen- und Trainerpool von rund 50 Personen zur Verfügung, dennoch stellen kurzfristige Ausfälle teilweise eine Belastung für die Organisation dar. Derzeit können diese überwiegend durch Mitarbeiterinnen und Mitarbeiter des Assistenzbereichs AB06 des Landeskriminalamts kompensiert werden. In kleineren Bundesländern, in denen die personellen Kapazitäten begrenzter sind, stellt sich diese Problematik vermutlich in verschärfter Form dar.

6.3 Ausblick

Curriculare Weiterentwicklung
Angesichts der rasanten Entwicklungen im Bereich Cybercrime und IT ist eine laufende Anpassung sowohl des Curriculums als auch der Trainerhandbücher unabdingbar. Derzeit rücken insbesondere Themen wie das taktisch richtige Verhalten am Tatort sowie der Einsatz Künstlicher Intelligenz in den Fokus – sei es im Zusammenhang mit Deep Fakes oder als unterstützendes Werkzeug in verschiedenen Einsatzlagen. Die inhaltliche Aufbereitung durch das Trainerinnen- und Trainerteam sowie die bundesweite Abstimmung der Inhalte werden aktiv vorangetrieben.

Aufbaumodule in Vorbereitung
Aufgrund der aktuellen Strafprozessänderungen ist innerhalb der Kollegenschaft ein verstärkter Bedarf an vertiefenden Schulungsinhalten, insbesondere zur digitalen Beweismittelauswertung, erkennbar. Eine Grundkonzeption entsprechender Aufbaumodule wurde bereits erstellt. Derzeit befinden sich erste Entwürfe in Ausarbeitung, die in den kommenden Wochen fertiggestellt werden sollen.

7 Rechtliche Herausforderungen aus Sicht der Kriminalpolizei

7.1 Anpassung des Cyberstrafrechts

Bei kriminalpolizeilichen Ermittlungen in Zusammenhang mit Cybercrime-Delikten kommt es immer wieder zu Ermittlungshindernissen beziehungsweise Erschwernissen, die zum Teil auf die derzeitigen eng gefassten materiellen strafrechtlichen Bestimmungen zurückzuführen sind. So ist zum Beispiel ein Datendiebstahl, der nicht durch „Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem" erfolgt, nach wie vor gerichtlich nicht strafbar. Das Bundeskriminalamt spricht sich daher für eine Angleichung des „digitalen" Cyber-Strafrechts an das „analoge" Strafrecht, wie zum Beispiel in Zusammenhang mit Strafbestimmungen beim Diebstahl, aus. Die Strafdrohungen bei Cybercrime-Delikten im engeren Sinn sind mittlerweile zum Teil angehoben. So wurde die Strafdrohung beispielsweise bei § 118a StGB Widerrechtlicher Zugriff auf ein Computersystem („Hacking") von sechs Monaten auf zwei Jahre angehoben. Dies eröffnet den Weg für Ermittlungen auf internationaler Ebene. Zum Beispiel kann der EU-Haftbefehl erst ab einer Mindeststrafdrohung von einem Jahr ausgestellt werden.

7.2 Datenschutz-Grundverordnung und „WHOIS"-Abfragen

Domainnamen wie „www.bundeskriminalamt.at" machen Informationen im Internet leichter auffindbar. Die dafür benötigten Domänen können bei Registries und Registraren angemietet werden. „WHOIS"-Abfragen im Internet führten in der Vergangenheit häufig noch direkt zum Inhaber oder zur Inhaberin einer Domäne und zu einer technischen Kontaktperson. Diese Domainnamen zählen zu den Grundbausteinen des Internets. Personenbezogene Auskünfte sind für weiterführende Ermittlungen von hoher Bedeutung und waren bis zum Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 auch öffentlich zugänglich. Durch die Vielzahl von Registries und Registraren, die für die Verwaltung von Domainnamen zuständig sind, ergeben sich weitere Herausforderungen bei den Nachforschungen. Waren vormals nur einfache Abfragen in öffentlichen Datenbanken erforderlich, müssen bei Auskunftsersuchen an internationalen Standorten verwaltungstechnisch höchst aufwändige Prozesse durchlaufen werden. Diese erheblichen Ermittlungshürden werden als Folge der DSGVO auch in technischen

und rechtlichen Gremien mit der Dachorganisation der Domänenverwaltung ICANN behandelt. Bis dato konnten keine von diesen Organisationen in Aussicht gestellten Konzepte final umgesetzt werden.

7.3 Carrier-Grade-NAT-Problematik

Aufgrund der häufigen Nutzung der Carrier-Grade-NAT-Technologie, bei der mehreren Internetnutzerinnen und Internetnutzern zeitgleich identische IP-Adressen vom Netz-Provider zugewiesen werden, können viele Straftaten nicht geklärt und auch die Verfasserinnen und Verfasser von Hasspostings sowie Fake News nicht ausgeforscht werden. Dies führt im Rahmen der Ermittlungen zu erheblichen Problemen bei der Zuordnung und Identifizierung krimineller Userinnen und User, wenn vom Netzanbieter die üblichen Protokollierungen von Userinnen und Usern beispielsweise aufgrund der fehlenden rechtlichen Rahmenbedingungen nicht gespeichert werden dürfen und daher nicht übermittelt werden können. Überdies gibt es international und auch auf europäischer Ebene selbst zwischen den einzelnen Mitgliedstaaten sehr große Unterschiede in deren rechtlichen Rahmenbedingungen zu dieser Thematik.

7.4 Pseudoanonyme Transaktionen von virtuellen Währungen

Kryptowährungen wie Bitcoins sind unter anderem auch ein beliebtes Mittel für Finanztransaktionen und Käufe illegaler Waren im Internet, ebenso wie bei der Geldwäsche. Jeder kann selbst anonym eigene Wallets erstellen, die wie eine digitale Geldbörse zur Aufbewahrung und wie ein Bankkonto für den Versand und Empfang von virtuellen Währungen genutzt werden. Der Einsatz von Computerprogrammen ermöglicht es zudem, eine Vielzahl von Schritten beim Zahlungsverkehr zu automatisieren. Das reicht von der Generierung dieser Wallets bis zu eigenständigen, maschinellen Überweisungen von Geldbeträgen. Durch die Flut an anonymen Überweisungen werden Strafverfolgungsbehörden vor Herausforderungen gestellt, die bei den notwendigen Erhebungen nur sehr schwer bewältigt werden können.

Eine diesbezügliche rechtliche Anpassung erfolgte seitens der EU mit der sogenannten Verordnung für Märkte für Kryptowerte (MiCA-Verordnung) und der dritten Geldtransfer-Verordnung, die Teile des sogenannten Digital Financial Package (AMLA-Paket 2021) sind. Diese Rechtsakte traten am 30. Dezember 2024 in Kraft. Durch diese soll die Kryptobranche innerhalb der EU stärker reguliert werden. Die MiCA-Verordnung enthält eine zentrale Legaldefinition des Begriffs „Kryptowerte“ sowie Anforderungen an das öffentliche Angebot und die Zulassung zum Handel mit Kryptowerten. Die dritte Geldtransfer-Verordnung dehnt die bereits bestehenden Geldwäschepräventionspflichten

für Zahlungsdienstleisterinnen und Zahlungsdienstleister auf Kryptodienstleisterinnen und Kryptodienstleister aus. Diese sind künftig im Zusammenhang mit Kryptotransfers verpflichtet, konkrete Angaben zum Zahler und Zahlungsempfänger einzuholen, wodurch die Rückverfolgbarkeit des Zahlungsflusses von Kryptowerten und somit auch die Strafverfolgung erleichtert werden soll.

7.5 Sicherstellung von Mobiltelefonen ohne richterliche Bewilligung verfassungswidrig

Der Verfassungsgerichtshof hat in seinem Urteil vom 14. Dezember 2023 festgestellt, dass die Sicherstellung von Mobiltelefonen in Strafverfahren ohne eine vorhergehende richterliche Bewilligung verfassungswidrig ist. Das verstoße gegen das Datenschutzgesetz und das Recht auf Privatleben. Grundrechtseingriffe müssen verhältnismäßig sein. Die Schwere des Eingriffs darf nicht größer sein als die Bedeutung des Ziels, das erreicht werden soll. Grundsätzlich sei es ein legitimes Ziel, Datenträger sicherzustellen und auszuwerten, um Straftaten zu verfolgen. Auch stellt die rasche Verbreitung neuer Kommunikationstechnologien die Kriminalitätsbekämpfung vor besondere Herausforderungen, doch entsprechen die angefochtenen Bestimmungen der Strafprozessordnung nicht den Anforderungen von § 1 Datenschutzgesetz und Artikel 8 der Europäischen Menschenrechtskonvention. Der Verfassungsgerichtshof ist der Ansicht, dass eine so weitgehende Maßnahme wie eine Sicherstellung von Datenträgern einer richterlichen Bewilligung bedarf. Nur so kann überprüft werden, ob die gesetzlichen Voraussetzungen für die Sicherstellung und Auswertung vorliegen und ob die Sicherheitsbehörden ihre Befugnisse einhalten.

Der Gesetzgeber hat auf dieses Urteil reagiert und eine entsprechende Anpassung der Strafprozessordnung (StPO) vorgenommen. Ab 1. Jänner 2025 gelten in Österreich neue Regelungen zur Sicherstellung von elektronischen Beweismitteln. Die neue Ermittlungsmaßnahme ist in den §§ 115f ff StPO zu den Bestimmungen über die Beschlagnahme von Datenträgern und Daten verankert. Die Beschlagnahme von elektronischen Datenträgern und Daten ist nunmehr durch die Staatsanwaltschaft aufgrund einer gerichtlichen Bewilligung anzuordnen (Richtervorbehalt) und von der Kriminalpolizei durchzuführen. Die Anordnung ist auf bestimmte Datenkategorien und Inhalte zu begrenzen. Die Aufbereitung und Auswertung der Daten erfolgt strikt getrennt voneinander und ist entsprechend zu dokumentieren. Außerdem sieht die Neuregelung neben Vernichtungsanordnungen und Verwendungsverboten einen besonderen Rechtsschutz vor, der dem oder der Rechtsschutzbeauftragten obliegt (Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung der Beschlagnahme von Datenträgern und Daten).

7.6 Vorratsdatenspeicherung

Mittlerweile ist es über zehn Jahre her, dass der Europäische Gerichtshof (EuGH) im Jahr 2014 entschieden hat, dass die Vorratsdatenspeicherung gegen das Grundrecht auf Achtung des Privatlebens und den Schutz personenbezogener Daten verstößt. Die Vorratsdatenspeicherung ist die gesetzliche Verpflichtung von Telekommunikationsanbietern, bestimmte Kommunikationsdaten ihrer Kundinnen und Kunden für einen bestimmten Zeitraum zu speichern. Davon betroffene Daten sind üblicherweise Telefonnummern, Zeitpunkte und die Dauer der jeweiligen Kommunikation sowie IP-Adressen betreffend Internetverbindungen. Solche Daten sind für polizeiliche Ermittlungen im Bereich Cybercrime für die Täterinnen- und Täterausforschung jedoch essenziell. Der EuGH hält in seinem Urteil zwar fest, unter welchen Umständen eine solche nationale Regelung die Vorratsdatenspeicherung betreffend zulässig wäre, jedoch ist das Problem aufgrund der Umstrittenheit rechtlich weder in Österreich noch auf EU-Ebene gelöst. Eine solche Regelung ist aus kriminalpolizeilicher Sicht jedenfalls zu begrüßen, da die derzeitige rechtliche Situation ohne Vorratsdatenspeicherung zweckmäßige und zielführende Ermittlungen de facto nicht zulässt.

Mittlerweile sieht der EuGH in einem jüngeren Urteil C-470/21 vom 30. April 2024 von seiner bisherigen diesbezüglichen Rechtsprechung jedoch ab. In diesem weitet er den Spielraum für eine präventive Speicherung von IP-Adressen auf die Bekämpfung von allen Straftaten aus. Alle Mitgliedstaaten haben daher nun die Möglichkeit, nationale Regelungen zu erlassen, durch die Kommunikationsdienstanbieterinnen und Kommunikationsdienstanbieter zum Zwecke der Bekämpfung von Straftaten verpflichtet werden, IP-Adressen auf Vorrat zu speichern, sofern keine Rückschlüsse auf das Privatleben einer Person gezogen werden können.

8 Exkurs: Widerrechtlicher Zugriff auf Computersysteme

Der widerrechtliche Zugriff auf Computersysteme stellt ein zunehmendes Problem dar. § 118a StGB kriminalisiert unbefugtes Eindringen in IT-Systeme und unterstreicht die gesellschaftliche und rechtliche Relevanz dieses Delikts.

Aktuelle Statistiken zeigen einen kontinuierlichen Anstieg der Anzeigen in diesem Bereich. Cyberkriminelle nutzen zunehmend raffinierte Methoden, um in fremde Systeme einzudringen, personenbezogene Daten zu stehlen und finanzielle Schäden zu verursachen. Besonders schadhaft sind Angriffe auf prioritäre Benutzerkonten sowie Konten, auf denen Zahlungsinformationen hinterlegt sind. Diese sind bevorzugte Ziele für Angreiferinnen und Angreifer, da sie direkten finanziellen Schaden anrichten können. Zudem ist zu beobachten, dass regelmäßig neue Begehungsformen aufscheinen, mit denen Kriminelle Sicherheitsmaßnahmen umgehen.

Bei der Analyse der Begehungsformen zu § 118a StGB fällt auf, dass sich die Schwerpunkte der Angriffe verändern. Während der widerrechtliche Zugriff auf Social-Media-Accounts sowie Server, PCs und Router (Hardware) im vergangenen Jahr rückläufig ist, nehmen die Angriffe auf E-Mail-Accounts, digitale und unbare Zahlungsmittel sowie Marktplatz-Accounts deutlich zu.

Gerade E-Mail-Accounts sind ein bevorzugtes Ziel, da sie oft als zentraler Zugangspunkt für viele weitere Online-Dienste dienen. Ein erfolgreicher Angriff kann weitreichende Folgen haben, da Cyberkriminelle auf diese Weise Passwörter zurücksetzen oder sensible Informationen abgreifen können. Ebenso steigt der Missbrauch von digitalen Zahlungsmitteln – insbesondere durch gestohlene Kreditkarteninformationen oder kompromittierte Zahlungsdienste – was zu erheblichen finanziellen Schäden führen kann.

Ein besonders starkes Wachstum ist im Bereich der Marktplatz-Accounts zu verzeichnen. Bekannte Plattformen geraten zunehmend ins Visier von Angreiferinnen und Angreifern, die betrügerische Bestellungen tätigen, Zahlungsdaten abgreifen oder Fake-Angebote einstellen, um ahnungslose Käuferinnen und Käufer zu täuschen.

Parallel dazu zeigt sich, dass die Bedrohung für Social-Media-Accounts vor allem auf Plattformen wie Facebook und Instagram bestehen bleibt, wenn auch in etwas abgeschwächter Form. Diese Accounts werden häufig für Identitätsdiebstahl und Betrugsmaschen genutzt, beispielsweise indem gehackte Profile dafür missbraucht werden, betrügerische Nachrichten an Freunde und Familie zu senden.

Ein besonderes Risiko stellen Datenlecks und schwache Sicherheitsvorkehrungen dar. Immer wieder gelangen große Mengen an Zugangsdaten durch Hackerangriffe oder unsichere Datenbanken an die Öffentlichkeit. Cyberkriminelle nutzen diese geleakten Informationen, um sich mithilfe von Credential-Stuffing-Angriffen Zugang zu weiteren Konten zu verschaffen.

Zusätzlich stellen Phishing, Social Engineering und Malware erhebliche Bedrohungen dar.

- **Phishing-Angriffe** werden immer raffinierter und nutzen täuschend echte E-Mails oder Nachrichten, um Nutzerinnen und Nutzer zur Preisgabe sensibler Daten zu verleiten. Besonders gefährlich sind Spear-Phishing-Attacken, bei denen Einzelpersonen oder Unternehmen gezielt angegriffen werden.

- **Social Engineering** nutzt psychologische Manipulation, um Menschen dazu zu bringen, vertrauliche Informationen preiszugeben oder schädliche Aktionen durchzuführen. Betrügerinnen und Betrüger geben sich oft als Kolleginnen bzw. Kollegen oder Bank- sowie Support-Mitarbeiterinnen und -Mitarbeiter aus.

- **Malware und Ransomware** verbreiten sich über infizierte Anhänge oder manipulierte Webseiten. Während Malware oft unbemerkt im Hintergrund Daten ausspioniert, verschlüsselt Ransomware komplette Systeme und fordert Lösegeld für die Freigabe der Daten.

- **SIM-Swapping** ist eine zunehmend verbreitete Methode, bei der Angreiferinnen und Angreifer die Kontrolle über Mobilfunknummern übernehmen, um Zwei-Faktor-Authentifizierungscodes abzufangen und so Zugriff auf Bankkonten oder E-Mail-Accounts zu erhalten.

- **Man-in-the-Middle-Angriffe (MITM)** ermöglichen es Hackern, sich in Datenübertragungen einzuklinken und vertrauliche Informationen abzufangen, beispielsweise in unsicheren WLAN-Netzwerken.

9 Kriminalprävention im digitalen Zeitalter

9.1 Cybercrime gemeinsam bekämpfen

Mit der fortschreitenden Digitalisierung steigen die Bedrohungen durch Cyberkriminalität stetig an. Sowohl Privatpersonen als auch Unternehmen und staatliche Institutionen sehen sich einer Vielzahl von Risiken ausgesetzt – von Phishing und Ransomware bis hin zu Social-Engineering-Angriffen. Um diesen Herausforderungen zu begegnen, setzt Österreich auf umfassende Präventionsmaßnahmen, die durch gezielte Kooperationen und Kampagnen umgesetzt werden.

Cybercrimeprävention ist ein entscheidender Aspekt der modernen Sicherheitsstrategie. Angesichts der stetig wachsenden Risiken im digitalen Raum ist es notwendig, dass Behörden, Institutionen und die Bevölkerung zusammenarbeiten, um effektive Schutzmaßnahmen zu entwickeln und umzusetzen. Die Kooperation zwischen verschiedenen Institutionen wie Polizei, Bildungseinrichtungen, Interessenvertretungen etc. ermöglicht eine ganzheitliche Prävention und eine schnelle Reaktion auf neue Bedrohungen.

Besonders wichtig ist die Aufklärung über die Risiken beim Online-Einkauf, da Betrugsformen wie Phishing, Fake-Shops oder Identitätsdiebstahl für Internetnutzerinnen und Internetnutzer oftmals schwieriger zu erkennen sind. Bei Vorträgen und Beratungen durch Präventionsbedienstete werden sowohl Bürgerinnen und Bürger als auch Verbraucherinnen und Verbraucher sensibilisiert, wie sie sich vor diesen Gefahren am besten schützen können. Ein Schwerpunkt im Jahr 2024 wurde auf maßgeschneiderte Vorträge für Senioren gelegt, um über die Risiken und Schutzmaßnahmen im Internet aufzuklären. Diese Zielgruppe ist besonders anfällig für Online-Betrügereien und verschiedene Telefonbetrugsformen, wie beispielsweise „Falscher Polizist“, „Enkel- oder Neffentrick“, „Angehörige in Not“ oder „Technische-Service-Dienste“.

Die Themen der Cybercrime-Prävention sind vielfältig und betreffen verschiedene Zielgruppen. Dementsprechend werden die Inhalte den aktuellen Kriminalitätsfeldern angepasst, aufgearbeitet und dementsprechend sensibilisiert. Um diesem breiten Adressatenkreis gerecht zu werden, ist es wichtig, eine umfassende Themenpalette anzubieten, die auf die unterschiedlichen Bedürfnisse und Kriminalitätsfelder eingeht.

Kooperation mit „Kriminalprävention“
Die Kriminalprävention stellt einen zentralen Bestandteil der Polizeitätigkeit dar, um der Bevölkerung die Möglichkeiten zu bieten, sich vor Straftaten zu schützen.

Ein Schwerpunkt ist die Schulung für Präventionsbedienstete zum „Lagebild Cybercrime“, die regelmäßig angeboten wird. Diese Schulung umfasst:

- **Lagebild Cybercrime**: Teilnehmerinnen und Teilnehmer erhalten einen Überblick über die aktuelle Bedrohungslage in Österreich. Dabei werden Statistiken, Fallbeispiele und Trends analysiert, um die Dynamik der Cyberkriminalität besser zu verstehen.
- **Aktuelle Phänomene**: Die Schulung behandelt die neuesten Methoden von Cyberkriminellen, darunter Phishing-Angriffe, Ransomware-Attacken und Social-Engineering-Betrug. Auf neue Entwicklungen, die durch technologische Innovationen und gesellschaftliche Veränderungen entstehen, wird besonders eingegangen.
- **Praxisnahe Tipps für Schutz und Prävention**: Den Teilnehmerinnen und Teilnehmern werden effektive Maßnahmen vermittelt, um sich und ihre Organisationen zu schützen. Dazu zählen sichere Passwörter, die Nutzung der Zwei-Faktor-Authentifizierung, ein achtsamer Umgang mit verdächtigen E-Mails sowie regelmäßige Software-Updates.

Diese Schulungen tragen dazu bei, das Bewusstsein für Cyber-Risiken zu schärfen und die Eigenverantwortung der Bürgerinnen und Bürger zu stärken.

Kooperation mit „Watchlist Internet“
Die „Watchlist Internet“ ist eine unabhängige Informationsplattform, die sich der Aufklärung von Online-Betrug und Internetfallen widmet. Sie bietet Verbraucherinnen und Verbrauchern wertvolle Tipps, um sich vor betrügerischen Websites, Phishing-Mails und anderen digitalen Bedrohungen zu schützen.

Ein wichtiger Meilenstein in der Zusammenarbeit war die **Beiratssitzung im November 2024**, die im Cybercrime-Competence-Center (C4) stattfand. Im Rahmen dieses Treffens wurden:

- Einblicke in aktuelle Ermittlungsansätze und Entwicklungen ausgetauscht,
- Strategien zur Verstärkung der Zusammenarbeit zwischen Polizei und „Watchlist Internet“ entwickelt und
- Präventionsprojekte für die kommenden Jahre geplant.

Die „Watchlist Internet“ bleibt eine essenzielle Anlaufstelle für die Prävention von Cybercrime und die Aufklärung der Öffentlichkeit.

Teilnahme an der Interpol-„Awareness Campaign“
Als Teil der internationalen Bemühungen zur Bekämpfung von Cybercrime beteiligt sich Österreich an der Interpol-„Awareness Campaign“. Diese weltweite Initiative hat das Ziel, das Bewusstsein für Cyber-Risiken zu erhöhen und globale Präventionsstrategien zu fördern.

Im Rahmen dieser Kampagne werden

- **Aufklärungskampagnen** gestartet, um öffentliche Aufmerksamkeit auf spezifische Cyberbedrohungen zu lenken,
- **Best Practices** und Erfolgsgeschichten im internationalen Kontext geteilt,
- **kooperative Maßnahmen** entwickelt, die den grenzüberschreitenden Charakter der Cyberkriminalität adressieren sowie
- eine **Webinarreihe konzipiert**, um aktuelle Kriminalitätsfelder schnell zu erkennen und darauf reagieren zu können, um die Bevölkerung für aktuelle Kriminalitätsformen sensibilisieren zu können.

Durch regelmäßige Schulungen bleiben die Polizeibediensteten stets auf dem neuesten Stand und können in ihrer Arbeit gezielt gegen Cyberkriminalität vorgehen.

Teilnahme an der „Counter Ransomware Initiative“ (CRI)
Ein weiteres bedeutendes Projekt ist die Teilnahme an der Counter Ransomware Initiative (CRI). Österreich ist seit Oktober 2021 auch Teilnehmer der „Counter Ransomware Initiative“ der USA. Die Partner sind an einer Ausweitung der Zusammenarbeit bei der Strafverfolgung interessiert, um gemeinsame, internationale Operationen im Zusammenhang mit Ransomware zu ermöglichen und Informationen auszutauschen.

Ziele der CRI sind:

- sowohl ein **Erfahrungsaustausch** als auch ein Austausch **bewährter Praktiken**,
- **die Entwicklung von Strategien** und Maßnahmen, die sowohl die Prävention als auch die Reaktion auf Ransomware-Angriffe verbessern und
- die Förderung eines **Informationsaustauschs** zwischen Ransomware-Opfern, Strafverfolgungsbehörden und Cyber-Notfallteams (CERTs), um effektive Gegenmaßnahmen zu erarbeiten.

Ein zentraler Bestandteil der Initiative war der CRI-Workshop, bei dem führende Expertinnen und Experten aktuelle Erkenntnisse und Technologien präsentierten, die im Kampf gegen Ransomware genutzt werden können. Im Fokus standen dabei auch gemeinsame Übungen zur Reaktion auf Angriffe und die Verbesserung der internationalen Zusammenarbeit.

Medienkampagnen
Durch Medienkampagnen können Informationen breiter gestreut werden, wobei gezielt auf Kooperationspartnerinnen und Kooperationspartner zurückgegriffen wird, um die Reichweite der Informationsverbreitung zu erhöhen und die Zielgruppen besser zu erreichen.

- Eine Kampagne zum Thema „**Sicher Einkaufen im Internet**“ weist auf die Gefahren des Online-Handels hin und vermittelt praktische Tipps zur Erkennung von Risiken und zum Ergreifen von Maßnahmen, um Gefährdungen zu minimieren.

- Zudem konnte die Online-Kampagne „**Überprüfe dein Wissen zu aktuellen Kriminalitätsphänomenen**“ mittels **Gamification-Ansatzes** (zum Beispiel Kahoot) zu verschiedenen aktuellen Kriminalitätsfeldern umgesetzt werden, die auf der Website des Bundeskriminalamts abrufbar ist. Durch das Spielen mittels Kahoot wird der Lernprozess spielerisch und interaktiv gestaltet und wirkt somit nachhaltiger. Dabei werden Betrugsformen wie Phishing, Smishing, Fake-Shops etc. durch Abbildung von aktuellen Fällen dargelegt und auf die Gefahren beziehungsweise Präventionstipps hingewiesen.

- Die Kampagne **#10TageGegenPhishing** fördert die Bereitschaft von Kundinnen und Kunden, sich über die neuesten Phishing-Techniken zu informieren. Sie wird vom Bundeskriminalamt, „Watchlist Internet“, der Payment Service Austria GmbH (PSA) und österreichischen Banken durchgeführt. Die Verbreitung geschieht sowohl über klassische Medien als auch über soziale Netzwerke. Das gemeinsame Ziel dieser Kampagne ist, einen Überblick über die aktuellen Phishing-Formen zu geben, diese zu erkennen und sich dementsprechend zu schützen.

Geplante Präventionskampagne „Account Sicherheit“
Für das Jahr 2025 plant Österreich die nationale Präventionskampagne „Account Sicherheit“. Diese Kampagne zielt darauf ab, die Bürgerinnen und Bürger über die Bedeutung der Kontosicherheit aufzuklären. Schwerpunkte der Kampagne sind:

- **Sichere Passwörter**: Tipps zur Erstellung starker und individueller Passwörter.
- **Zwei-Faktor-Authentifizierung**: Erläuterung, warum diese Methode eine effektive Schutzmaßnahme ist.
- **Maßnahmen im Schadensfall**: Schnelles Handeln im Schadensfall kann größere Schäden abwenden.

Diese Kampagne soll das Bewusstsein für die Eigenverantwortung beim Schutz digitaler Identitäten schärfen und die Anzahl der Account-Kompromittierungen reduzieren.

Ausbildung von Präventionsbediensteten
Ein weiterer Schwerpunkt liegt auf der Ausbildung von Präventionsbediensteten im Bereich Künstliche Intelligenz (KI). KI stellt sowohl eine Chance als auch ein Risiko für die Cybersicherheit dar. Aus- und Weiterbildungen für Präventionsbedienstete sowie Polizistinnen und Polizisten sind notwendig, um den sicheren Umgang mit KI zu gewährleisten und potenzielle Missbrauchsgefahren zu erkennen. Diese Schulungen helfen Fachkräften, KI als Werkzeug zur Bekämpfung von Cyberkriminalität effektiv einzusetzen und sich gleichzeitig vor Angriffen zu schützen, die auf KI-Technologien basieren.

Fazit
Durch die enge Zusammenarbeit mit der Kriminalprävention und „Watchlist Internet", die Teilnahme an internationalen Kampagnen und nationalen Präventionsprojekten setzt Österreich ein klares Zeichen im Kampf gegen Cyberkriminalität. Die Kombination aus Aufklärung, Ausbildung und gezielten Maßnahmen trägt dazu bei, die digitale Sicherheit von Bürgerinnen und Bürgern nachhaltig zu stärken.

Prävention ist dabei ein kontinuierlicher und essenzieller Prozess, der ständige Anpassungen an neue Bedrohungen erfordert. Weitere Kampagnen und Maßnahmen sind bereits in Planung, um den Herausforderungen der digitalen Welt weiterhin wirksam begegnen zu können.

Präventionstipps:
- „Gesundes Misstrauen" im Netz
- Seien Sie sich bewusst – auch im Internet ist nichts gratis
- Halten Sie Ihren Virenschutz / Ihre Firewall stets aktuell
- Vorsicht, wenn Sie jemand unter Druck setzen will
- Verschicken Sie niemals Ausweiskopien

9.2 Cybercrime-Anzeigenerstattung

Wenn Sie Opfer einer Straftat aus dem Feld der Cyberkriminalität geworden sind, haben Sie die Möglichkeit, diesen Sachverhalt in jeder Polizeidienststelle prüfen zu lassen beziehungsweise gegebenenfalls anzuzeigen.

Um sich hierfür optimal vorzubereiten, helfen Ihnen folgende Tipps:

Wenn es um einen konkreten aktuellen Notfall geht (Angriff auf Leib oder Leben), dann rufen Sie den Polizeinotruf 133 an.

Stellen Sie bitte fallrelevante(s) Beweismittel / Datenmaterial wie beispielsweise E-Mails, Chat-Verläufe, Zahlungsbelege, Screenshots, digitale Fotos oder Videos und vieles mehr entsprechend zusammen. Wenn bestimmte Inhalte nicht abgespeichert werden können, erstellen Sie Screenshots oder fotografieren Sie den Bildschirm notfalls ab.

Stellen Sie sicher, dass sich die Unterlagen und Daten, die Sie der Polizei zur Verfügung stellen, im Originalzustand befinden. Das bedeutet: keine Manipulation, keine Ergänzungen oder Ähnliches. Bei E-Mails würde das bedeuten, diese nicht einfach weiterzuleiten, sondern die Original-Mail abzuspeichern und die gespeicherte Kopie als Anhang zu übermitteln.

Häufig haben Sie auch selbst die Möglichkeit, bei den von Ihnen betroffenen Accounts Informationen zu erfragen, die für eine Täterausforschung notwendig sind. Exemplarisch sind dies IP-Adressen über widerrechtliche Zugriffe inklusive Zeitstempel, Logdaten etc. Überprüfen Sie am besten selbst, wo genau die für die Tathandlung relevanten Daten beim jeweiligen Account-Anbieter beziehungsweise Online-Service-Provider gespeichert werden beziehungsweise können Sie dort deren Bekanntgabe anfordern.

Im Falle einer komplexen Tathandlung **dokumentieren Sie den Tathergang** in chronologischer Weise und stellen Sie sicher, dass die Geschehnisse zeitlich richtig eingeordnet sind.

Wenn Sie Probleme haben, die Beweismittel technisch zu sichern beziehungsweise abzuspeichern, bitten Sie eine Person Ihres Vertrauens, diese Beweise mit Ihnen gemeinsam zu sichern.

Stellen Sie **die gesicherten Daten** den aufnehmenden Polizeibediensteten nach Absprache mit diesen **in geeigneter Form** zur Verfügung (beispielsweise über https://cryptshare.bmi.gv.at). Die Daten zur Verfügung zu stellen, ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.

Bitte haben Sie Verständnis dafür, dass Sie bei einem ersten Gespräch mit der Polizei nicht unmittelbar auf spezialisierte Cybercrime-Ermittlerinnen und -Ermittler treffen und deshalb in den meisten Fällen erst in einem zweiten Schritt an eine spezialisierte Fachdienststelle weitergeleitet werden oder von dort Rückfragen erhalten.

Darüber hinaus kann Ihnen die Meldestelle für Cybercrime professionelle Auskunft über die weitere Vorgangsweise bei Cybercrime-Vorfällen erteilen. Für die formelle Anzeigenerstattung sind in der Regel die örtlich und sachlich zuständigen Polizeidienststellen zuständig. Derzeit ist eine formelle Anzeigenerstattung über die Meldestelle nicht vorgesehen.

E-Mail: against-cybercrime@bmi.gv.at

10 Strategie und Ausblick

Cyberkriminalität ist ein sich schnell verändernder Deliktsbereich, der großes Know-how aller involvierten Kolleginnen und Kollegen verlangt. Folglich muss in den kommenden Jahren die Ausbildung im Cyber-Bereich weiter forciert werden, das Know-how bei allen Strafverfolgungsbehörden und Polizeidienststellen verbessert und die Gesellschaft im Umgang mit neuen Technologien zur Wahrung ihrer Sicherheit sensibilisiert werden. Im Rahmen der Kriminaldienstreform sind sowohl auf Landes- als auch auf regionaler Ebene die entsprechenden organisatorischen Anpassungen zur verbesserten Bekämpfung der Cyberkriminalität vorgesehen und die Einrichtung mehrerer Cybercrime-Trainingscenter geplant. Das Vorhaben ist aktuell (2025) in Umsetzung. Oberstes Ziel ist, die Kriminalitätsbekämpfung weiterzuentwickeln und den Dienst zu modernisieren. Der Bereich der Cyberkriminalität bildet einen Arbeitsschwerpunkt.

Ein strategischer Schwerpunkt umfasst wie auch in den Vorjahren die Stärkung der nationalen und internationalen Zusammenarbeit zwischen staatlichen Behörden, maßgeblichen Organisationen und relevanten Unternehmen. Die Einsatzmöglichkeiten künstlicher Intelligenz sollen im Bereich der Strafverfolgungsbehörden weiter ausgelotet werden. Eine besondere Herausforderung hierbei sind die rechtlichen Vorgaben der EU (beispielsweise AI-Act), speziell im Hinblick darauf, dass viele forensische Werkzeuge auf den Einsatz von KI setzen und daher diese Vorgaben berücksichtigen müssen.

Da künstliche Intelligenz zunehmend eine wichtige Rolle im Kampf gegen Cyberkriminalität spielt (KI-generierte Phishing-Versuche, Coding mit KI-Unterstützung etc.), ist geplant, die vorhandenen Ressourcen in diese Richtung verstärkt zu entwickeln. Insbesondere die Mitarbeit bei der Erarbeitung von rechtlichen Rahmenbedingungen sowie die kontinuierliche Weiterentwicklung von Fachexpertise der im C4 tätigen Kolleginnen und Kollegen sind vorgesehen. Die weiterschreitende Vernetzung (Internet der Dinge) erfordert die Entwicklung neuer Ermittlungsmethoden und Ermittlungsansätze. In diesem Bereich soll verstärkt Expertise aufgebaut werden.

Die Novellierung der Strafprozessordnung in Österreich bezüglich der Beschlagnahme von Datenträgern und Daten stellt das Cybercrime-Competence-Center vor neue Herausforderungen und erfordert eine entsprechende Neuausrichtung der IT-Beweissicherung. Die neuen Bestimmungen differenzieren klar zwischen den Phasen der Beschlagnahme, der technischen Aufbereitung und der inhaltlichen Auswertung der Daten. Das C4 muss seine Prozesse entsprechend anpassen und sicherstellen, dass diese Phasen transparent und nachvollziehbar dokumentiert werden. Insbesondere ist eine klare Trennung zwischen den ermittelnden Einheiten und dem assistierenden Büro 5.2 gefordert und gesetzlich geboten. Die notwendige Dokumentation in der Phase der Datenaufbereitung wurde

in Absprache mit der Justiz adaptiert. Die erforderlichen Aufbereitungsformulare der IT-Beweissicherung wurden geändert.

Auf Ebene des C4 wurden im Jahr 2024 sowohl der Bereich der IT-Ermittlungen wie auch jener der digitalen Beweismittelsicherung (IT-Forensik) personell verstärkt. Die Umstrukturierung des Büros 5.2 zur Abteilung 5 „Cybercrime-Competence-Center“ ist bereits erfolgt.

Der Aufbau einer österreichweiten, modernen technischen Infrastruktur für die Kriminalpolizei ist seit längerem im Gange. Bereits 2021 wurde ein Projekt unter dem Namen „SeILE“ (Schaffung einer IKT-Lösung für besondere kriminalpolizeiliche Ermittlungen) unter Einbindung des Justizministeriums gestartet und entsprechend den Empfehlungen des Rechnungshofes ausgerichtet. Im Rahmen dieses Projektes wird die Errichtung einer IKT-Lösung für all jene kriminalpolizeilichen Ermittlungs- und Forensik-Tätigkeiten angestrebt, die aus berechtigten Sicherheitsüberlegungen nicht in der aktuellen digitalen Umgebung des BMI ausgeführt werden können.

11 Strategy and Outlook

Cybercrime covers a wide range of rapidly changing offences that require a high level of expertise from all employees involved. Consequently, cyber training has to be further enhanced in the years to come and know-how has to be improved at all levels of law enforcement, down to every police station. In addition, awareness among society about the safe use of new technologies has to be raised. The criminal policing reform aims at making appropriate organisational adaptations to improve the fight against cybercrime and at establishing multiple cybercrime training centres both at provincial and local level. The project is currently being implemented (2025). The primary objective is to step up the fight against crime and to modernise criminal policing. Particular focus is on cybercrime.

As in previous years, one strategic focus will lie on the strengthening of national and international cooperation between governmental authorities, key organisations and relevant companies. Use cases for artificial intelligence in law enforcement will be further explored. In this context, the legal requirements set by the EU (e.g. AI Act) pose a major challenge, especially in view of the fact that many forensic tools rely on the use of AI and therefore have to take these requirements into account.

Since artificial intelligence plays an increasingly significant role in the fight against cybercrime (AI-generated phishing attempts, AI-assisted coding, etc.), it is intended to further develop existing resources in this regard. In particular, it is planned to collaborate on the drafting of legal frameworks and to continuously develop the professional skills of all employees working at the Criminal Intelligence Service Austria's Cybercrime Competence Centre (C4). The growing interconnectivity (Internet of things) calls for the development of new investigation methods and approaches. Hence, more expertise in this field is to be built.

The amendment of the Austrian Code of Criminal Procedure with regard to the seizure of data carriers and data presents new challenges to the Cybercrime Competence Centre and requires changes in digital evidence preservation. The new provisions clearly differentiate between the phases of seizure, technical preparation and analysis of the data's content. C4 has to adapt its processes accordingly and ensure that these phases are documented in a transparent and accountable manner. In particular, a clear separation between the investigative units and the supporting Sub-Department 5.2 is required and stipulated by law. The documentation necessary in the phase of data preparation has already been adapted in consultation with the judicial authorities and the required preparation forms of digital evidence preservation have been amended.

In 2024, staffing levels at C4 for both IT investigations and preservation of digital evidence (IT forensics) were raised as far as possible. The restructuring of Sub-Department 5.2 into Department 5 „Cybercrime Competence Centre“ has been completed.

The development of modern technical infrastructure for CIDs throughout Austria has been ongoing for some time. In 2021, a project named “SeILE” (creation of an ICT solution for special CID investigations) was launched in cooperation with the Federal Ministry of Justice and adapted according to the recommendations made by the Court of Audit. Within the framework of this project, it is intended to create an ICT solution for all those CID investigative and forensic activities that cannot be undertaken within the current digital environment of the Federal Ministry of the Interior due to valid security considerations.

12 Glossar

Anonymisierungsdienst

Bei Anonymisierungsdiensten handelt es sich um Services und Techniken im Internet, die dazu dienen, bestimmte Informationen, die auf die Identität von Internetnutzerinnen und Internetnutzern hindeuten könnten, zu verschleiern.

Antivirenprogramm

Ein Antivirenprogramm (synonym mit Virenscanner oder Virenschutz) ist eine Software, die bekannte Schadsoftware wie beispielsweise Computerviren (siehe Viren) in einem Computersystem aufspüren kann, blockiert und gegebenenfalls beseitigt. Auch wenn damit ein grundlegender Schutz gegeben ist, erfolgt dieser nicht zu hundert Prozent, da es laufend neue Schadsoftware gibt, die noch nicht erkannt wird.

Applikation / App

Eine Applikation, kurz App oder Anwendungssoftware, ist ein Computerprogramm. Häufig wird der Begriff „App" im Zusammenhang mit Anwendungen für mobile Endgeräte wie Tablets oder Smartphones verwendet.

BEC (Business E-Mail Compromise)

Angreiferinnen und Angreifer kompromittieren bei einem BEC den E-Mail-Schriftverkehr eines Unternehmens mit dem Ziel, Mitarbeiterinnen und Mitarbeiter der Firma zu einer Geldtransaktion auf das Bankkonto der Kriminellen zu veranlassen. Es handelt sich hier um gezielte Angriffe gegen bestimmte Unternehmen, da die Kriminellen im Vorfeld teilweise umfangreiche Recherchen anstellen und sich häufig mittels Social Engineering zusätzliche Informationen verschaffen. Um derartige Fälle zu vermeiden, ist eine Sensibilisierung der Unternehmensmitarbeiterinnen und -mitarbeiter durchzuführen und es ist ratsam, im Schriftverkehr mit Geschäftspartnerinnen und Geschäftspartnern vorsichtig zu sein. Bei unklaren oder eigenartigen Sachlagen über eine andere Technologie (Telefon) sind die Sachverhalte zu überprüfen.

Behördenwallets

Das C4 ist seit 2018 rechtlich und technisch in der Lage, Sicherstellungen von Kryptowährungen durchzuführen. Hierfür werden unter höchsten Sicherheitsvorkehrungen sogenannte Behördenwallets erstellt und zur Aufbewahrung von virtuellen Währungseinheiten verwendet. Das Bundeskriminalamt verfügt jederzeit über etwa 1.000 Behördenwallets von verschiedenen Kryptowährungen, die rund um die Uhr für Sicherstellungen durch Strafverfolgungsbehörden zur Verfügung stehen.

Bitcoin

Bitcoin (englisch für „digitale Münze“) ist ein weltweit verwendbares dezentrales Register und der Name eines immateriellen Vermögenswertes. Überweisungen werden von einem Zusammenschluss von Rechnern über das Internet mittels Blockchain (durchgehende Kette von Transaktionsblöcken) abgewickelt, sodass, anders als im herkömmlichen Bankverkehr, keine zentrale Abwicklungsstelle benötigt wird. Eigentumsnachweise können in einer persönlichen digitalen Brieftasche, einem sogenannten Wallet, gespeichert werden.

Caller-ID-Spoofing

Um ihre wahre Identität zu verschleiern, manipulieren die Kriminellen bei den Betrugsanrufen ihre Telefonnummer. Bei Anrufen eine falsche Nummer anzuzeigen, ist relativ leicht und mit wenig technischem Auf¬wand verbunden. Dazu können existierende – auch aus dem Ausland stammende – Telefonnummern ver¬wendet werden, obwohl die Inhaberinnen und Inhaber der Nummer für den Anruf gar nicht verantwortlich sind. Auch Fantasienummern, also Telefon-nummern, die nicht vergeben sind, können eingesetzt werden.

CaaS (Crime as a Service)

Die für die Begehung einer Straftat benötigten Dienste werden individuell zusammengestellt und gleich online erworben. Dabei handelt es sich vorwiegend um Hacking Tools, Schadsoftware wie beispielsweise Verschlüsselungstrojaner, aber auch um spezielle Dienstleistungen zur Geldwäsche, für Übersetzungen oder für den vermeintlichen Opfer-Support. Die Kriminellen benötigen damit kein tiefgreifendes technisches Wissen zur Straftatbegehung, sondern kaufen sich das fehlende Wissen schlichtweg zu.

Collège Européen de Police (CEPOL)

Die European Union Agency for Law Enforcement Training beziehungsweise Europäische Polizeiakademie ist eine durch Beschluss des Rates der europäischen Justiz- und Innenministerinnen und -minister im Jahr 2000 gegründete europäische Einrichtung zur Ausbildung der europäischen Polizei.

Cybermobbing

Der Begriff „Cybermobbing“ bezeichnet das absichtliche und über einen längeren Zeitraum anhaltende Beleidigen, Bedrohen, Bloßstellen, Belästigen oder Ausgrenzen von Personen über digitale Medien wie beispielsweise über soziale Netzwerke, Messenger-Apps oder in Videoportalen.

Cyber Trading Fraud

Beim Cyber Trading Fraud gehen Betrügerinnen und Betrüger sehr raffiniert vor: Sie locken potenzielle Anlegerinnen und Anleger für vermeintlich lukrative Investitionsgeschäfte im Internet an und verleiten sie zu Geldzahlungen. Die Kontaktaufnahme geschieht vornehmlich über Internet-Werbeanzeigen, soziale Netzwerke, Anrufe aus eigens geschaffenen Callcentern oder Massenmails. Durch die professionelle Vorgehensweise ist es besonders wichtig, zu wissen, wie man sich am besten vor den Kriminellen schützen kann, denn das eingezahlte Geld wird nicht wie versprochen angelegt, sondern verschwindet im kriminellen Netzwerk.

Darknet

Große Teile des Internets sind für übliche Suchmaschinen nicht zugänglich. Diese zeigen oft nur Inhalte des offenen Internets, des Clearwebs, an. Dort liegen alle Daten unverschlüsselt vor und können durchsucht werden und meist auch über eine Adresse, die sogenannte URL, aufgerufen werden. Um in das Darknet, beispielsweise das Tor-Netzwerk zu gelangen, benötigt man einen speziellen Browser, wie den Tor-Browser. Daten werden im Darknet anonym und verschlüsselt über verschiedene Server geschickt. Das Darknet war ursprünglich für Personen und Organisationen gedacht, die von Zensur bedroht waren. Heutzutage reicht das Spektrum an illegalen Aktivitäten im Darknet vom Drogen- und Waffenhandel über Dokumentenfälschung, Geldfälschung, Datenhandel bis hin zur Kinderpornografie und weit darüber hinaus.

DDoS-Angriffe

DDoS-Angriffe beziehungsweise „Distributed Denial of Service"-Angriffe sind Attacken auf die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems oder von Netzwerken, meistens mit dem Ziel, diese zu blockieren und somit regulären Benutzerinnen und Benutzern keinen Zugriff mehr zu ermöglichen. Die Angriffe erfolgen häufig von vielen verschiedenen Ressourcen aus dem Internet. Neben politisch oder persönlich motivierten Angriffen versuchen Kriminelle auch häufig, Geld mit DDoS-Angriffen zu erpressen.

Domain Name System (DNS)

Das DNS ist einer der wichtigsten Dienste im Internet. Seine Hauptaufgabe ist die Auflösung des Domainnamens, wie zum Beispiel www.bmi.gv.at, in eine IP-Adresse (siehe IP-Adresse), um eine Kommunikation zwischen den Computersystemen zu ermöglichen.

European Cybercrime Center (EC3)

Das EC3 ist ein Teil von Europol und wurde eingerichtet, um in folgenden drei Bereichen signifikante Unterstützung für die Mitgliedsstaaten zu schaffen:

- Bekämpfung von Cybercrime, begangen durch organisierte Gruppierungen, die beispielsweise durch Online-Betrug große Geldmengen erbeuten.
- Bekämpfung von Formen von Cybercrime, die die Opfer massiv schädigen, wie beispielsweise sexueller Missbrauch von Kindern.
- Bekämpfung von Cybercrime (inklusive Cyberattacken), der gegen kritische Infrastruktur und Informationssysteme der EU-Mitgliedsstaaten gerichtet ist.

Fiatwährungen

Als Fiatgeld oder Fiatwährungen werden Währungen bezeichnet, die von Regierungen reguliert und kontrolliert werden. Beispiele sind der Euro, der US-Dollar oder der Schweizer Franken. Fiatwährungen sind Währungen, die nicht an den Preis eines Rohstoffes wie Gold oder Silber gebunden sind.

Firewall

Eine Firewall ist ein System aus hardware- und/oder softwaretechnischen Komponenten, um Netzwerke sicher miteinander zu verbinden. Die Firewall analysiert den Netzwerkverkehr und hat beispielsweise die Aufgabe, unerwünschte Zugriffe von außen – wie die vom Internet – zu blockieren.

IKT

Der Begriff „Informations- und Kommunikationstechnologie“ (Abkürzung: IKT, alternativ auch IuK) bezeichnet Technik, die zum Erheben, Speichern, Übertragen und Weiterverarbeiten von Daten und Informationen genutzt wird. Zu dieser Technik gehören beispielsweise Computer, Handys/Smartphones und Tablets, aber auch Netzwerke.

IP-Adresse

Eine IP-Adresse dient zur eindeutigen Adressierung von Computern und anderen Geräten in einem Netzwerk, das auf dem Internetprotokoll (IP) basiert. Sie wird jedem Gerät in einem Netzwerk zugewiesen und macht somit jedes Gerät adressierbar und damit erreichbar. Die IP-Adresse entspricht funktional der Rufnummer in einem Telefonnetz.

Technisch wird unterschieden zwischen IP-Version 4 (IPv4) und IP-Version 6 (IPv6). Letzteres wurde unter anderem eingeführt, da die Anzahl der möglichen öffentlichen Adressen bei IPv4 stark beschränkt ist und mittlerweile als aufgebraucht gilt.

Kryptowährungen und Blockchain

Kryptowährungen sind digitale Zahlungsmittel, die auf verschlüsselten Datensätzen basieren. Mit dieser Form der Zahlungsmittel ist ein digitaler Zahlungsverkehr ohne ein dazwischengeschaltetes Geldinstitut möglich. Der Besitz des Code-Schlüssels stellt dabei das Eigentum dar. Zahlungstransaktionen mit Kryptowährungen werden in sogenannten Blöcken gespeichert. Das Buchungssystem nennt man Blockchain. Die bekannteste Kryptowährung ist der Bitcoin. Das Bitcoin-Zahlungssystem wurde 2008 unter dem Pseudonym Satoshi Nakamoto erstmals veröffentlicht. Obwohl Kryptowährungen in den vergangenen Jahren auch Kursverluste hinnehmen mussten, ist ein steigender Trend bei legalen wie auch illegalen Bezahlvorgängen zu beobachten. Insbesondere im Bereich Cybercrime haben sich „Cryptos“, vor allem bei Massenerpressungs-E-Mails und im Suchtgifthandel, durchgesetzt. Auch wenn Bitcoin immer noch an erster Stelle rangiert, wird mittlerweile ebenso mit anderen, als „Altcoins“ bezeichneten, Kryptowährungen bezahlt.

Love Scam / Romance Scam

Bei Love Scam handelt es sich um eine Art von Partnerinnen- und Partnervermittlungsbetrug. Die Kriminellen stellen meist den ersten Kontakt per E-Mail oder über soziale Medienplattformen her und versuchen, eine Vertrauensbasis durch zum Beispiel die Zusagen von persönlichen Treffen zu schaffen. In Folge der elektronischen Kommunikation versucht der oder die Kriminelle das Opfer zum Übersenden von Geld und Wertgegenständen zu überreden, indem eine Notsituation vorgetäuscht wird. Tatsächlich existiert die dargestellte, geliebte Person aber nicht, sondern dient nur als Tarnung. Die Kriminellen schrecken dabei auch nicht davor zurück, die Identität und den Internetauftritt von realen Personen dafür zu missbrauchen.

Malspam

Bei Malspam beziehungsweise „Malicious Spam" handelt es sich um Spam-E-Mails, die zur Verbreitung von Schadsoftware dienen. Diese E-Mails können bereits Schadsoftware oder schädliche Elemente beinhalten (wie beispielsweise Dropper, Downloader etc. jeweils versteckt als JavaScript, eingebettet in komprimierten Dateien oder anderen Datenformaten). Oder diese E-Mails beinhalten „nur" einen Link, der aktiv vom Empfänger angeklickt werden muss, damit die schädlichen Komponenten auf dem Gerät des Opfers installiert werden.

Money Mules

Wie die deutsche Übersetzung der Bezeichnung „Money Mule", nämlich „Geldesel", vermuten lässt, wird von einer Person illegal erworbenes Geld im Rahmen von Kurierdiensten transferiert, um die Strafverfolgung zu erschweren. Meist erhält die Person ein Entgelt für den Geldtransfer, ist sich aber dabei nicht bewusst, dass sie aktiv an Geldwäsche beteiligt ist. Die Anwerbung erfolgt oft über E-Mail.

Network Address Translation (NAT)

Bei Carrier Grade NAT teilt der Provider eine IPv4-Adresse aus dem privaten Adressbereich „10.0.0.0/8" den Endkundenanschlüssen zu – keine „öffentliche IP-Adresse" (§ 92 Abs 3 Z 16 TKG). Auf diese Weise spart er mittlerweile sehr rare öffentliche IPv4-Adressen. Zwischen dem privaten Provider-Netz und dem öffentlichen IPv4-Netz vermittelt dann die NAT oder Port Address Translation (PAT). Der dafür zuständige vermittelnde Server kümmert sich um die Adressübersetzung zwischen den privaten und öffentlichen IPv4-Adressen und reicht die Pakete zwischen den Netzwerken weiter. NAT wurde ursprünglich für lokale Netzwerke – wie den WLAN-Router zu Hause entwickelt – die nur eine öffentliche IPv4-Adresse zugeteilt bekommen haben. Diese wird aber von mehreren Clients als Zugang zum öffentlichen Netz genutzt. NAT findet hier in einem kleinen Rahmen mit wenigen Clients statt. Bei Carrier Grade NAT sind davon meist mehrere tausend Clients betroffen und gleichzeitig wird doppelt geNATet, weil Kundinnen und Kunden immer noch nur eine IPv4-Adresse für mehrere Clients bekommen.

Bei jedem NAT- oder PAT-Vorgang wird nicht nur die private IP-Adresse in eine öffentliche übersetzt, sondern auch die zu der Netzwerkadressierung (IP-Adresse und Port, Schreibweise zum Beispiel 194.203.112.23:80) gehörenden Ports ändern sich. Das bedeutet, dass bei jedem NAT-Vorgang von dem NAT-Verbindungsserver einer bestimmten IP-Adresse aus dem internen Netz eine bestimmte Portnummer der öffentlichen IP im externen Netz (dem Internet) eindeutig zugewiesen wird, damit der Kommunikationsvorgang nachvollziehbar bleibt. Sonst wüsste der Verbindungsserver nicht, wer welche Kommunikation durchführt. Das Identifikationsmerkmal des Nutzeranschlusses ist daher nicht mehr nur die IP-Adresse, sondern auch der sogenannte Source-Port oder sozusagen als „Rückrechnung" für die Provider die Ziel-IP und der Ziel-Port.

Non-fungible-Token (NFT)

Ein Non-Fungible Token (NFT) ist ein kryptografisch eindeutiges, unteilbares, unersetzbares und überprüfbares Token, das einen bestimmten Gegenstand, sei er digital oder physisch, in einer Blockchain repräsentiert.

Open Source Intelligence (OSINT)

OSINT befasst sich mit der Gewinnung von Informationen, die über offene Quellen frei verfügbar im Internet zu finden sind. Diese Daten werden für weitere Ermittlungen und Analysen herangezogen, um gezielte Erkenntnisse daraus herzuleiten.

Phishing

Mit Phishing wird versucht, beispielsweise über gefälschte Webseiten, E-Mails oder andere Messenger-Nachrichten an persönliche Daten zu gelangen. Phishing steht häufig in Zusammenhang mit zumindest versuchten Betrugshandlungen und Identitätsmissbrauch.

Ransomware

Als Ransomware wird Schadsoftware bezeichnet, die den Zugriff auf Daten und elektronische Systeme durch Verschlüsselung von Daten oder Bereichen des Betriebssystems einschränkt oder verhindert. Diese Ressourcen werden erst wieder nach Bezahlung eines Lösegeldes („ransom"), meist in Form von Kryptowährung, freigegeben.

RAT (Remote-Access-Trojaner)

Hierbei handelt es sich um ein Schadprogramm, das eine Hintertür (backdoor) für administrative Kontrolle auf dem Zielsystem öffnet. RAT werden üblicherweise im Hintergrund durch ein Programm heruntergeladen, das Anwenderinnen und Anwender aufgerufen haben – beispielsweise ein Spiel oder einen E-Mail-Anhang. Sobald das Zielsystem kompromittiert ist, macht sich der Eindringling diesen Umstand zunutze, um RAT auf andere anfällige Computer zu verteilen.

Schadsoftware

Bei Schadsoftware (synonym mit den Begriffen Schadprogramme, Schadcode oder Malware) handelt es sich um Programme oder Skripte, die mit dem Ziel entwickelt wurden, eine unerwünschte und meistens schädliche Funktion auf Computersystemen auszuführen.

Smart Contracts

Dabei handelt es sich um Computerprotokolle, die Verträge abbilden, überprüfen oder die Verhandlung und Abwicklung eines (Kauf-)Vertrags technisch unterstützen.

Social Engineering

Bei Social Engineering werden vermeintliche menschliche Schwächen wie Neugier oder Angst ausgenutzt, um Zugriff auf sensible Daten oder Informationen zu erhalten. Bei Cyber-Angriffen verleiten Kriminelle ihre Opfer dazu, eigenständig wichtige Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadsoftware auf ihren Systemen zu installieren. Während vor vielen Jahren noch der Müll nach Dokumenten und Datenträgern durchsucht wurde, geschieht das Ausforschen von Informationen heutzutage oft durch das Ausspähen von Daten auf Social-Media-Plattformen und Anrufen mit falschen Identitäten.

Spam

Als Spam bezeichnet man elektronische, unerwünschte Nachrichten, die massenhaft und gezielt über verschiedene Kommunikationsdienste verbreitet werden. Teilweise beinhaltet Spam in harmlosen Varianten unerwünschte Werbung. Häufig jedoch enthält Spam auch Schadsoftware im Anhang, Links zu infizierten Webseiten oder wird für Phishing-Angriffe genutzt.

Stablecoins

Stablecoins sind digitale Währungen, die den Wert eines anderen Assets abbilden. Dabei handelt es sich meistens um Fiatwährungen, wie zum Beispiel Euro oder US-Dollar. Ein Stablecoin kann also den Wert einer anderen Währung spiegeln.

Stranded Traveller Scam

Die Opfer erhalten eine E-Mail von jemandem, den sie meist persönlich kennen und in der behauptet wird, dass das Gegenüber wegen eines Raubüberfalls in einem fremden Land gestrandet wäre und sie braucht, um ihm/ihr zu helfen, nach Hause zurückzukehren. Gefordert werden Geldbeträge in unterschiedlicher Höhe. Tatsächlich wurde das E-Mail-Konto gehackt und die Nachricht an alle Kontakte im Adressbuch gesendet. Die Hacker können E-Mails an das Konto des Opfers umleiten und so das weitere Geschehen steuern.

Trojaner (Trojanisches Pferd)

Als Trojanisches Pferd bezeichnet man ein Computerprogramm oder eine Applikation, das als nützliche oder harmlose Anwendung getarnt ist, im Hintergrund aber ohne das Wissen der Anwenderinnen und Anwender eine andere, meist schädliche, Funktion erfüllt.

Uniform Resource Locator (URL)

Eine URL identifiziert und lokalisiert Ressourcen im Internet, wie beispielsweise Webseiten. Das URL-Format macht eine eindeutige Bezeichnung von Dokumenten im Internet möglich und beschreibt die Internetadresse von Objekten, die von einem Browser gelesen werden können, zum Beispiel https://www.bmi.gv.at/.

Virus

Bei (Computer-)Viren handelt es sich um die älteste Art von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich trägt. Sie treten in Kombination mit einem Wirt auf, das heißt mit einem infizierten Dokument oder einer Applikation.

Verschlüsselung

Verschlüsselung transformiert Daten in Abhängigkeit von einer Zusatzinformation, dem „Schlüssel", in einen zugehörigen Geheimtext, der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation, das heißt die Zurückgewinnung des Klartextes aus dem Geheimtext, wird Entschlüsselung genannt.

Wallet

Ein Wallet, der englische Begriff für „Geldbeutel" oder „Portemonnaie", ist eine virtuelle Geldtasche, in der Benutzerinnen und Benutzer Bitcoins oder andere Kryptowährungen aufbewahren. Insofern kann ein Wallet mehrere unterschiedliche Kryptowährungen beinhalten. Darüber hinaus gibt es unterschiedliche Arten von Wallets.

WHOIS

WHOIS ist ein Service im Internet, der vor allem zur Abfrage von Daten zu Domainnamen genutzt wird. Vor der DSGVO war es uneingeschränkt möglich, Eigentümerinnen und Eigentümern, Ansprechpartnerinnen und Ansprechpartner der Domain (siehe Domain Name System) sowie IP-Adressen über diesen Dienst abzufragen, da alle Daten öffentlich zugänglich gewesen sind.

Deliktsbezeichnungen nach Paragrafen

NPSG – Neue-Psychoaktive-Substanzen-Gesetz

- § 4 NPSG Gerichtliche Strafbestimmungen

Strafgesetzbuch (StGB)

- § 107a StGB Beharrliche Verfolgung
- § 107c StGB Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems
- § 118a StGB Widerrechtlicher Zugriff auf ein Computersystem
- § 119 StGB Verletzung des Telekommunikationsgeheimnisses
- § 119a StGB Missbräuchliches Abfangen von Daten
- § 126a StGB Datenbeschädigung
- § 126b StGB Störung der Funktionsfähigkeit eines Computersystems
- § 126c StGB Missbrauch von Computerprogrammen oder Zugangsdaten
- § 144 StGB Erpressung
- § 145 StGB Schwere Erpressung
- § 146 StGB Betrug
- § 147 StGB Schwerer Betrug
- § 148 StGB Gewerbsmäßiger Betrug
- § 148a StGB Betrügerinnen und Betrügerischer Datenverarbeitungsmissbrauch
- § 207a StGB Bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellungen minderjähriger Personen
- § 207b StGB Sexueller Missbrauch von Jugendlichen
- § 208a StGB Anbahnung von Sexualkontakten zu Unmündigen
- § 218 StGB Sexuelle Belästigung und öffentliche geschlechtliche Handlungen
- § 223 StGB Urkundenfälschung
- § 224 StGB Fälschung besonders geschützter Urkunden
- § 225a StGB Datenfälschung
- § 228 StGB Mittelbare unrichtige Beurkundung oder Beglaubigung
- § 229 StGB Urkundenunterdrückung
- § 231 StGB Gebrauch fremder Ausweise
- § 232 StGB Geldfälschung
- § 241a StGB Fälschung unbarer Zahlungsmittel
- § 283 StGB Verhetzung
- § 297 StGB Verleumdung

Suchtmittelgesetz SMG

- § 27 SMG Unerlaubter Umgang mit Suchtgiften
- § 28 SMG Vorbereitung von Suchtgifthandel

- § 28a SMG Suchtgifthandel
- § 30 SMG Unerlaubter Umgang mit psychotropen Stoffen
- § 31 SMG Vorbereitung des Handels mit psychotropen Stoffen
- § 31a SMG Handel mit psychotropen Stoffen
- § 32 SMG Unerlaubter Umgang mit Drogenausgangsstoffen

Verbotsgesetz (VerbotsG)

- §§ 3a–3h VerbotsG Wiederbetätigung