Bundesministerium
Inneres

Bundeskriminalamt

Cybercrimereport 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, 2026

Cybercrimereport 2025

Wien, 2026

Vorwort

Die Bekämpfung von Cyberkriminalität stellt eine der größten Herausforderungen für die Sicherheit Österreichs dar. Die fortschreitende Digitalisierung und die zunehmende Vernetzung von Gesellschaft, Wirtschaft und öffentlicher Verwaltung schaffen zwar neue Chancen, erweitern jedoch zugleich die Angriffsflächen für kriminelle Handlungen im digitalen Raum. Um diesen Entwicklungen wirksam zu begegnen, verfolgt das Bundesministerium für Inneres eine umfassende Strategie, die technische, organisatorische und personelle Maßnahmen miteinander verbindet und die Widerstandsfähigkeit Österreichs gegenüber Cyberbedrohungen nachhaltig stärkt.

Ein wichtiger Aspekt dieser Strategie ist die Etablierung von Cybercrime-Trainingscentern, die es ermöglichen, Polizeibeamte und andere Sicherheitsfachleute auf die Herausforderungen der Cyberkriminalität vorzubereiten. Durch den Ausbau von Ausbildungskooperationen, wie mit den Cyber-HAKs, soll die Zusammenarbeit zwischen Bildungseinrichtungen, Forschung und Praxis gestärkt werden, um die notwendigen Kompetenzen und Fähigkeiten für die Bekämpfung von Cyberkriminalität zu entwickeln.

Eine weitere wichtige Maßnahme ist die Stärkung der internationalen Zusammenarbeit mit anderen Strafverfolgungsbehörden. Durch die Teilnahme an internationalen Foren und die Entwicklung von gemeinsamen Strategien und Standards soll die Effektivität der Bekämpfung von Cyberkriminalität erhöht werden. Die Investition in externe IT-Spezialistinnen und -Spezialisten soll die Fachkompetenz der Polizei und anderer Sicherheitsbehörden stärken und die Fähigkeit zur Bekämpfung von Cyberkriminalität verbessern.

Die organisatorische Änderung und Aufwertung des Cybercrime Competence Centers zu einer eigenen Abteilung im Bundeskriminalamt soll die Koordination und Steuerung der Bekämpfung von Cyberkriminalität verbessern. Durch den Ausbau dieser zentralen Anlaufstelle wird die Zusammenarbeit zwischen den verschiedenen Behörden und Einheiten gestärkt, um eine effektive und effiziente Bekämpfung von Cyberkriminalität zu ermöglichen.

Die kriminalpolizeiliche Arbeit soll durch die Stärkung der Bereiche IT-Ermittlungen und der IT-Forensik unterstützt werden. Durch die Beschaffung moderner Softwarelösungen und Datenbanken für das digitale Zeitalter wird die Fähigkeit zur Analyse und Verfolgung von Cyberkriminalität verbessert werden. Die Attraktivierung des Polizeiberufs für IT-Fachkräfte soll die Fachkompetenz der Polizei stärken und die Fähigkeit zur Bekämpfung von Cyberkriminalität verbessern.

Die Entwicklung eines grundrechtskonformen Einsatzes neuer Technologien, wie Künstlicher Intelligenz (KI), soll die Effektivität der Bekämpfung von Cyberkriminalität erhöhen, ohne die Grundrechte der Bürgerinnen und Bürger zu gefährden. Durch die Kooperation

mit Wissenschaft, Forschung und privatem Sektor wird die Entwicklung von neuen Technologien und Methoden unterstützt werden, um die Bekämpfung von Cyberkriminalität zu verbessern.

Mit dieser ganzheitlichen Ausrichtung schafft das Bundesministerium für Inneres die Grundlage für eine zukunftsorientierte und leistungsfähige Bekämpfung der Cyberkriminalität. Ziel ist es, die Resilienz Österreichs im digitalen Raum nachhaltig zu stärken und den bestmöglichen Schutz der Bevölkerung, der Wirtschaft und der staatlichen Infrastruktur sicherzustellen.

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 bietet eine umfassende Analyse der Komplexität des Phänomens Cybercrime und der kriminalpolizeilichen Maßnahmen in Österreich. Die Ergebnisse basieren auf einer umfassenden Datensammlung, die im Bundeskriminalamt durchgeführt wurde, einschließlich gesammelter Meldungen, Anzeigen, Statistiken aus internationalen Kooperationen, Informationsaustausch mit Mitgliedsstaaten, Ausbildungen, Positionspapieren sowie Studien von Dritten.

Eine zentrale Erkenntnis des Berichts ist die Feststellung eines Anstiegs bei den Cybercrime-Fällen, was auf eine zunehmende Bedrohung durch Cyberkriminalität hinweist. Gleichzeitig zeigt sich eine leichte Abnahme der Aufklärungsquote, was darauf hindeutet, dass es schwieriger wird, Cybercrime-Fälle aufzuklären. Diese Ergebnisse unterstreichen die Notwendigkeit einer kontinuierlichen Anpassung und Verbesserung der kriminalpolizeilichen Maßnahmen, um der sich verändernden Bedrohungslage gerecht zu werden.

Ein weiterer wichtiger Aspekt des Berichts ist die Personalrekrutierung von IT-Fachleuten für die Bekämpfung von Cybercrime. Die Ergebnisse zeigen, dass die Rekrutierung von qualifizierten IT-Fachleuten aufgrund der bestehenden Ressourcen herausfordernd ist. Als Konsequenz daraus wurde die Fokussierung auf den internen Wissensaufbau durch Präsenz- und Online-Schulungen verstärkt, um die notwendigen Kompetenzen und Fähigkeiten aufzubauen.

Die Aufbauorganisation und die Abläufe des C4 sind aufgrund der technischen Komplexität und der einhergehenden Spezialisierung sehr flexibel gestaltet. Das C4 verfolgt das Ziel, durch die ausgeübte zentrale Fachaufsicht einen Einblick in Vorgehensweisen zu geben und das Anzeigeverhalten in der Bevölkerung zu verbessern. Es wird weiterhin auf verstärkte Eigenverantwortung der Bürgerinnen und Bürger und auf präventive Maßnahmen als Schwerpunkt gesetzt, um die Risiken und Gefahren von Cybercrime zu minimieren.

Der Bericht enthält eine detaillierte Analyse der wichtigsten Phänomene, einschließlich:

- Phishing-Angriffe: Eine Form von Cybercrime, bei der Opfer durch gefälschte E-Mails oder Nachrichten dazu gebracht werden, sensible Informationen preiszugeben.
- Ransomware-Angriffe: Eine Form von Cybercrime, bei der Opfer durch Schadsoftware dazu gebracht werden, Lösegeld zu zahlen, um ihre Daten wiederherzustellen.
- Online-Betrug: Eine Form von Cybercrime, bei der Opfer durch gefälschte

Internetkriminalität	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
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 %
Jahr 2025	63.459	19.570	30,8 %
Veränderung zum Vorjahr (VJ)	1,8 %	-1,1 %	-0,9 %-Punkte

Tabelle 1: Zehnjahresvergleich Internetkriminalität / Österreich 2016 bis 2025 (Jänner bis Dezember)

Der Bericht bietet auch Handlungsempfehlungen, um die Risiken und Gefahren von Cybercrime zu minimieren, einschließlich:

- Die Verwendung von starken Passwörtern und Zwei-Faktor-Authentifizierung, um die Sicherheit von Online-Konten zu erhöhen.
- Die regelmäßige Aktualisierung von Betriebssystemen und Anwendungen, um Sicherheitslücken zu schließen.
- Die Verwendung von Antiviren-Software und Firewalls, um Schadsoftware und unerwünschte Netzwerkaktivitäten zu verhindern.
- Die Überprüfung von Online-Angeboten und -Transaktionen auf ihre Seriosität, um Betrug und Phishing-Angriffe zu vermeiden.

Insgesamt bietet der Bericht eine umfassende Analyse des Bereiches Cybercrime und der kriminalpolizeilichen Maßnahmen in Österreich. Durch die Kombination von präventiven Maßnahmen und einer verbesserten Anzeigebereitschaft kann die Aufklärungsquote von Cybercrime-Fällen erhöht und die Bevölkerung besser geschützt werden.

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 Erpressungsversuchen auf Unternehmen, aber auch auf Private. Genaue Auswertungen und Analysen zur Polizeilichen Kriminalstatistik (PKS) 2025 finden sich in Kapitel 2 wieder.

Auch im Jahr 2025 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 wird eine erfolgreiche Strafverfolgung erschwert.

2.1 Internetbetrug

Die überwiegende Mehrheit der Betrugsfälle wird digital initiiert, wobei die Täterinnen und Täter 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 2025 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 und auf Gebrauchtwarenplattformen. Neben einzelnen Täterinnen und Tätern 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 Trend zum Einsatz von künstlicher Intelligenz zur Erstellung betrügerischer Deep-Fakes sowie zur Automatisierung komplexer Betrugsmodelle setzte sich auch im Jahr 2025 fort. 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 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, das Onlineshops in Echtzeit überprüft und Fake Shops identifiziert.

Die polizeiliche Kriminalstatistik (PKS) des Jahres 2025 verzeichnet eine Abnahme der gemeldeten Fälle von Internetbetrug auf 31.001, was einem leichten Rückgang von 2,4 Prozent gegenüber dem Vorjahr entspricht.

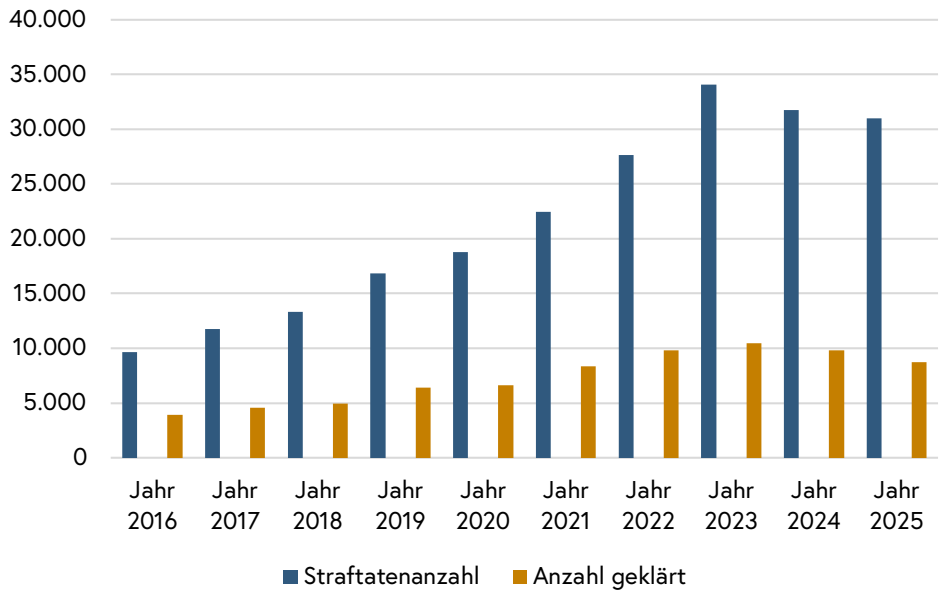

Abbildung 1: Zehnjahresvergleich Internetbetrug

Hervorzuheben sind die hohen Schadenszahlen im Bereich des Cyber-Trading-Frauds. Die Schadenssumme im Jahr 2025 belief sich hierbei ähnlich wie im Vorjahr auf zirka 120 Millionen Euro. Aus diesem Grund wurde im Bundeskriminalamt eigens eine Ermittlungsgruppe installiert, um diesem Deliktsfeld bundesweit koordiniert, international und zielgerichtet entgegentreten zu können.

Auch Phishing-Angriffe per E-Mail oder SMS waren 2025 hoch im Kurs. Anzumerken ist, dass neben klassischen Phishing-Versuchen, die auf Bankkundinnen und -kunden sowie Kreditkarteninhaberinnen und -inhaber abzielten, auch vermehrt Phishing-Angriffe auf Kundinnen und Kunden alternativer Online-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, Schadsoftware, 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.

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 oder einem Nutzer und dem Internet. Er versteckt die ursprüngliche IP-Adresse und leitet den Datenverkehr über eine andere Quelle weiter. 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-Geräte (Internet of Things). 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 Sicherheitslücken offen, durch die Angreiferinnen und 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 -entwickler 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 Investorinnen und Investoren werden dabei wertlos. Diese Betrugsform ist besonders häufig bei Decentralized-Finance-(DeFi)-Projekten und neuen Token auf dezentralen Börsen zu finden, da dort keine Regulierung existiert und die Entwicklerinnen und Entwickler meist anonym bleiben. DeFi-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 Täterinnen und Täter 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 Renditen 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 USDT zum Einsatz, die eine regelmäßige Auszahlung der angeblich erwirtschafteten Rendite an die eigene Wallet vortäuschen sollen.

Stablecoins sind digitale Währungen, die den Wert eines anderen Assets abbilden. Dabei handelt es sich meistens um Fiatwährungen, wie Euro oder US-Dollar. 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 (USD) 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 die 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 ihres 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 einen zumeist vierstelligen Betrag an eine gewisse Empfängerin oder einen gewissen Empfänger überweisen. Das Geld würde so bald wie möglich zurückgezahlt. Die Empfängerinnen und Empfänger sind sehr häufig 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 Täterinnen und Täter autorisiert werden.

2.8 Transportdienst-Trick

Ebenfalls auf Kleinanzeigenplattformen kursiert ein weiterer Trick. Die Täterinnen und Täter nehmen Kontakt auf und geben an, an der vom Opfer angebotenen Ware interessiert zu sein. Aufgrund des derzeitigen Aufenthaltsortes der vermeintlichen Käuferin bzw. 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 dieser Transportdienst in bar dabei, um diesen bei Abholung zu übergeben. Im Verlauf dieses angeblichen Kaufes 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 oder dem Käufer übernommen und somit bezahlt werden. Bei dieser Betrugsform tätigen gutgläubige Opfer tatsächlich Zahlungen an die Täterinnen und Täter, ohne dass die Ware je abgeholt wird.

2.9 Phishing

Phishing (abgeleitet vom englischen Wort „fishing“ = angeln) ist eine betrügerische Methode, bei der Cyberkriminelle versuchen, persönliche Informationen wie Passwörter und Kreditkartendaten bspw. 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/-Websites traten im Laufe des Jahres 2025 gehäuft in Erscheinung. Alle größeren Bankinstitute in Österreich waren von Phishing von Zugangsdaten für eBanking betroffen, wobei mit schädlichen Android-Applikationen mobile TANs für das Online-Banking abgegriffen wurden.

Anubis ist eine der hartnäckigsten und gefährlichsten Banking-Trojaner-Familien für Android-Geräte. Die Schadsoftware tarnt sich meist als harmlose App (zum Beispiel im Google Play Store oder auf gefälschten Webseiten) und stiehlt sensible Bankdaten sowie persönliche Informationen. Der Trojaner hat sich über die Jahre von einer Spionagesoftware zu einem multifunktionalen Bedrohungswerkzeug entwickelt.

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 Angreiferinnen und Angreifer fordern anschließend Lösegeld, um die Daten wieder freizugeben. Ransomware kann auf verschiedene Arten in ein System eindringen, zum Beispiel durch 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.

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 der Direktion für Staatsschutz und Nachrichtendienst [DSN]). Zusammengehörige Fälle (dieselbe Täterschaft, zusammenhängende Indikatoren der Kompromittierung etc.) werden zentral unter Einbeziehung der involvierten Polizeidienststellen koordiniert bzw. erfolgt eine Unterstützung der jeweiligen Sachbearbeiterin oder des jeweiligen Sachbearbeiters. In bestimmten Fällen erfolgt auch eine Übernahme von international durchzuführenden Anfragen, Datenabgleichen, der Koordination und der Fallkooperation mit anderen Ländern.

Im Jahr 2025 wurden insgesamt **111 Fälle** im Bundesgebiet zur Anzeige gebracht.

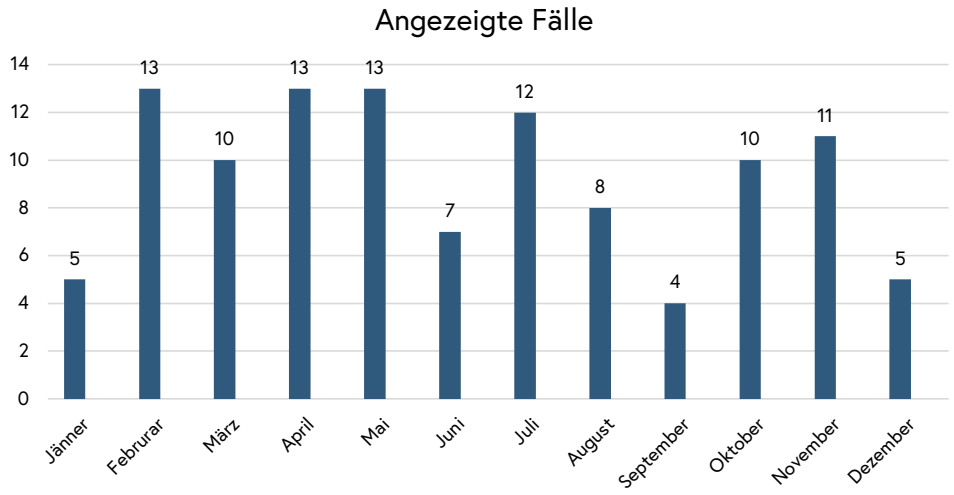

Abbildung 2: Monatliche Verteilung der Ransomware-Fälle 2025

Es ist erkennbar, dass ein beträchtlicher Teil der Angriffe, wie bereits im Vorjahr, durch viele kleinere Akteurinnen und Akteure durchgeführt wurde. Etablierte Gruppierungen wie INC (zwölf Fakten), Akira (elf Fakten) und RansomHub (fünf Fakten) verübten eine größere Zahl an Angriffen. Bei etwa 40 Prozent der Anzeigen konnte keine eindeutige Zuordnung zu einer bestimmten Akteurin oder einem bestimmten Akteur erfolgen. Derartige Zuordnungen gestalten sich zunehmend komplexer. Systeme von Opfern werden noch vor Anzeigenerstattung repariert oder neu installiert, um Betriebsunterbrechungen so kurz wie möglich zu halten. Ransomware-Akteurinnen und -Akteure versuchen, ihre Identität zu verbergen, hinterlassen bewusst irreführende Spuren, setzen

falsche Indikatoren, kooperieren untereinander oder teilen sich Ressourcen, Werkzeuge und Angriffstechniken. Neue Gruppierungen entstehen, bestehende durchlaufen einen Wandel, andere wiederum lösen sich auf. Ein weiterer Grund ist auch die schnelle Evolution von Malware. Die Methoden zur Durchführung von Ransomware-Angriffen entwickeln sich rapide.

Der überwiegende Teil der Angriffe richtete sich gegen Unternehmen. Es konnte keine Konzentration auf bestimmte Branchen festgestellt werden. 29 unterschiedliche Akteurinnen und Akteure konnten als Angreiferinnen und Angreifer identifiziert werden. Die folgende Grafik zeigt den Anteil an den Fällen der jeweiligen Akteurin oder des jeweiligen Akteurs.

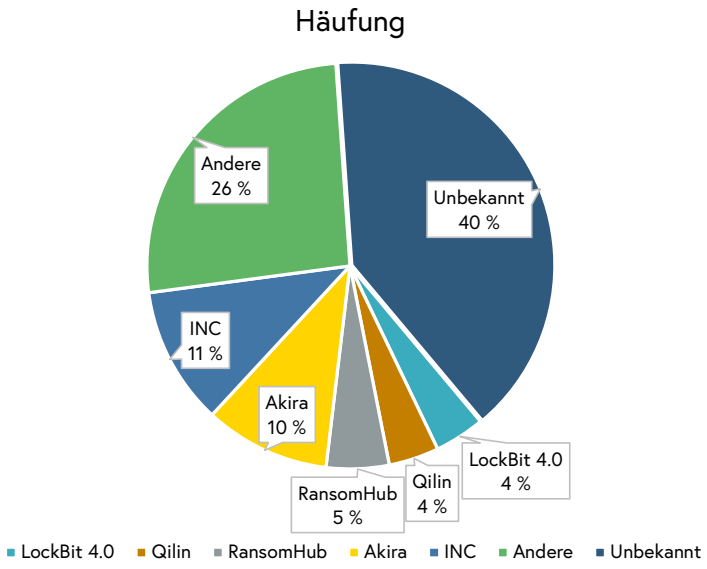

Abbildung 3: Ransomware-Arten und prozentuelle Verteilung 2025

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.

Auch im Jahr 2025 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 Täterinnen und Täter verwendeten verschiedene Methoden, wobei sogenannte DNS-Reflection- und Layer-7-Angriffe die häufigsten Techniken darstellten.

DNS-Reflection ist eine Methode, bei der Angreiferinnen und 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 Täterinnen und Täter 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 Täterinnen und Täter 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, CND-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 stellen Ransom-DDoS-Angriffe (RDDoS-Angriffe) dar. Diese liegen vor, wenn Täterinnen und Täter (-gruppierungen) versuchen, eine Person oder Organisation zu erpressen, dazu mit einem DDoS-Angriff drohen und Lösegeld verlangen. Beobachtungen zufolge führen manche Angreiferinnen und 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 und 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, wobei Unternehmen aus unterschiedlichen Wirtschaftsbereichen betroffen waren.

2.13 Online-Suchtmittelhandel

Der Online-Handel mit Suchtmitteln hat sich innerhalb des vergangenen Jahrzehnts zu einer bedeutenden Begehungsform der Suchtmittelkriminalität in Österreich entwickelt. Diese Form des Handels wird sowohl von Einzeltäterinnen und -tätern als auch von kriminellen Organisationen genutzt, um illegale Gewinne zu erzielen. Die hohe Anonymität, das Fehlen direkten Kontakts und die durchgehende Verfügbarkeit werden sowohl von den Händlerinnen und Händlern als auch von den Konsumentinnen und Konsumenten geschätzt. Darüber hinaus bietet der Online-Handel eine Verfügbarkeit von Suchtmitteln aller Art, auch an abgelegenen Orten.

Es wird angenommen, dass die Maßnahmen zur Bekämpfung der Corona-Pandemie zu einem Wachstum des Online-Handels mit Suchtmitteln geführt haben, da traditionelle Bezugsquellen teilweise weggefallen sind. Die Ermittlungen haben jedoch gezeigt, dass der Online-Drogenhandel den Straßenhandel nicht verdrängt oder ersetzt, sondern diesen vielmehr ergänzt. Der Online-Handel bietet vielmehr Suchtmittel höherer Qualität an, die auch im Straßenhandel gewinnbringend weiterverkauft werden können.

Der Online-Handel mit Suchtmitteln hat sich in den vergangenen Jahren von den Darknet-Netzwerken hin zum Clearnet, Instant-Messenger-Apps mit End-to-End-Verschlüsselung und Social-Media-Kanälen verschoben. Im Jahr 2025 wurden 1.303 Postsendungen mit Suchtmitteln sichergestellt und weitere 523 Sendungen mit Suchtmitteln internationaler Partner mit dem Ziel oder der Herkunft Österreich.

Die Statistik zeigt, dass Deutschland, die Niederlande und innerösterreichische Sendungen die Liste der Herkunftsländer anführen.

Eine neuere Begehungsform des Suchtmittelhandels ist der sogenannte „Dead Drop“, bei dem die Suchtmittel nicht per Post versendet, sondern an bestimmten Orten versteckt und die GPS-Koordinaten der Empfängerin oder dem Empfänger übermittelt werden.

Um dieser neuartigen Begehungsform entgegenzutreten, wurde im Jahr 2018 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 und -händler und koordinieren die polizeilichen Maßnahmen zur strafrechtlichen Verfolgung der Käuferinnen und Käufer. Darüber hinaus werden auch neue Strategien entwickelt und analysiert, um den Online-Suchtmittelhandel erfolgreich zu bekämpfen. Die internationale Zusammenarbeit und Koordination mit EUROPOL und anderen Drittstaaten ist eine zentrale Aufgabe dieses Fachreferats.

Die effektivste Maßnahme zur Bekämpfung des Online-Suchtmittelhandels bleibt jedoch die Zerschlagung der Vertriebswege. Deshalb werden bereits seit 2020 in enger Kooperation mit der österreichischen Zollverwaltung Schwerpunktkontrollen der Postwege durchgeführt. Diese Maßnahmen werden auch im Jahr 2026 fortgesetzt.

2.14 Bildliches sexualbezogenes Kindesmissbrauchsmaterial/Darstellungen minderjähriger Personen

Soziale Medien spielen eine entscheidende Rolle in der Verbreitung von sexualbezogenem Kindesmissbrauchsmaterial sowie sexualbezogenen Darstellungen Minderjähriger.

Entsprechende Hinweise auf Online-Kindesmissbrauch bekommt das Bundeskriminalamt nicht nur über die im Bundeskriminalamt eingerichtete Meldestelle. Amerikanische und kanadische Internetanbieter und Service-Provider, wie Google/Alphabet Inc., Meta Platforms, X Corp., Snap Inc., Reddit, Discord etc., scannen ihre Dienste permanent auf sexualbezogenes Kindesmissbrauchsmaterial. Die dabei festgestellten Dateien werden gelöscht und die verfügbaren Informationen an das US-amerikanische National Center for Missing and Exploited Children (kurz: NCMEC) übermittelt. NCMEC fungiert dabei als Schnittstelle zu den nationalen Strafverfolgungsbehörden und leitet die Verdachtsanzeigen auf Basis der IP-Adresse (Adresse, von der aus der Upload des strafrechtlich relevanten Materials stattgefunden hat) an die jeweils zuständige polizeiliche Zentralstelle des Landes weiter.

2025 – Neues Rekordhoch an Verdachtsmeldungen zu Online-Kindesmissbrauch

Mehr als 21.800 Meldungen zu Verdachtsfällen von Online-Kindesmissbrauch wurden auf diesem Weg im vergangenen Jahr dem Bundeskriminalamt übermittelt; ein besorgniserregendes Rekordhoch vor dem Hintergrund, dass sich die Anzahl der Meldungen binnen fünf Jahren mehr als verdreifacht hat.

Das Referat II/BK/3.2.7 im Bundeskriminalamt ist als Zentralstelle für die Auswertung von Meldungen zu Online-Kindesmissbrauch und Kindersextourismus sowie die Weiterleitung der Erkenntnisse an die zuständigen Strafverfolgungsbehörden der Bundesländer zuständig. In ihrer täglichen Arbeit sehen sich die insgesamt fünf Ermittlerinnen und Ermittler des auf Online-Kindesmissbrauch spezialisierten Fachreferats mit rund 1.800 Kindesmissbrauchsmeldungen im Monat konfrontiert. Die große Anzahl an Meldungen der US-NGO **NCMEC (National Center for Missing and Exploited Children)** lässt sich ohne entsprechende IT-Unterstützung nicht mehr zielführend bearbeiten. Das Referat II/BK/3.2.7 nutzt daher seit dem Jahr 2024 eine von der Europäischen Union aus Mitteln des ISF 2021-2027 finanzierte Softwarelösung, die Verdachtsmeldungen entgegen-

nimmt, vorsortiert und grafisch aufbereitet, um diese Hinweise im Rahmen der örtlichen Zuständigkeit weiterleiten zu können.

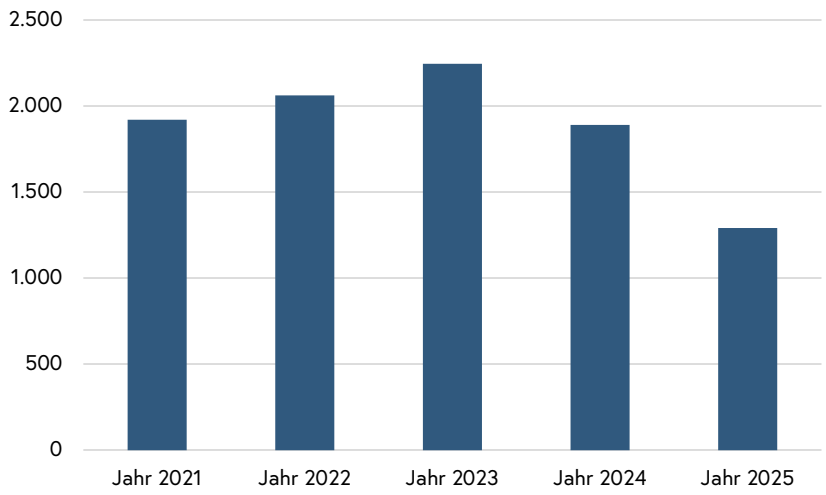

Abbildung 4: Fünfjahresvergleich der Anzeigen nach § 207a StGB

Neben der engen Zusammenarbeit mit **NCMEC** ist auch die laufende Kooperation mit Europol, Interpol und den Strafverfolgungsbehörden im In- und Ausland zu erwähnen. Ebenso erwähnenswert ist die enge Kooperation mit Nichtregierungsorganisationen wie Stopline, der Arbeitsgemeinschaft zum Schutz der Rechte der Kinder vor sexueller Ausbeutung – kurz: ECPAT (https://www.ecpat.at) und mit den nationalen Internet Service Providern (ISP).

Dank dieser multilateralen Kooperation konnten im Jahr 2025 österreichweit 294 Verdächtige ausgeforscht werden.

§ 207a StGB (Pornographische Darstellungen Minderjähriger)	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
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 %
Jahr 2025	1.291	1.151	89,2 %
Veränderung zum Vorjahr (VJ)	-31,7 %	-34,3 %	-3,6 %-Punkte

Tabelle 2: Zehnjahresvergleich der polizeilichen Anzeigen nach § 207a StGB

Die Ermittlungen gestalten sich zunehmend komplexer, sodass es trotz Zunahme der NCMEC-Meldungen zu einem Rückgang der Anzeigen im Vergleich zum Vorjahr kam. Gerade die Meldungen, bei denen ein Ermittlungsansatz vorliegt, sind zeitaufwendiger und erfordern mehr Einsatztechnik.

Weiterhin im Trend: Live Distance Child Abuse (LDCA)

Wie schon im vorangegangenen Jahr stellte der sogenannte „Live Distance Child Abuse“ (LDCA) auch im Jahr 2025 die Ermittlerinnen und Ermittler des Referats II/BK/3.2.7 im Bundeskriminalamt vor massive Herausforderungen. Das zunehmend relevante Kriminalitätsphänomen zeichnet sich dadurch aus, dass österreichische Täterinnen und Täter einen sexuellen Missbrauch von Kindern auf den Philippinen beauftragen, um diesen dann anschließend online und in Echtzeit zu konsumieren. Dank des außerordentlichen Engagements des spezialisierten Ermittlerinnen- und Ermittler-Teams im Bundeskriminalamt konnte im Jahr 2025 ein weiterer österreichischer Täter identifiziert werden, der im Chat philippinische Frauen zur Vornahme von Missbrauchshandlungen an Kindern vor laufender Kamera anleitete und sich somit zum Beitragstäter eines sexuellen Missbrauchs von Unmündigen machte.

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 2025 wurde im Bereich der Internetkriminalität erneut ein Anstieg der angezeigten Straftaten beobachtet, nachdem im Jahr 2024 die Zahl der Anzeigen erstmals zurückgegangen war.

Cybercrime im Fünf-Jahres-Vergleich			
Jahr	**Anzahl der angezeigten Straftaten**	**Anzahl der geklärten Straftaten**	**Aufklärungsquote (gerundet)**
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 %
Jahr 2025	63.459	19.570	30,8 %

Veränderung der Aufklärungsquote im Vergleich zum Vorjahr			
	Jahr 2024: 31,7 %	**Jahr 2025: 30,8 %**	**-0,9 %-Punkte**

Tabelle 3: Entwicklung der Anzeigen, der geklärten Fälle und der Aufklärungsquote von Cybercrime 2021 bis 2025 (Fünfjahresvergleich)

Die Entwicklung der Internetkriminalität zeigt, dass mit 63.459 Anzeigen im Jahr 2025 eine Zunahme gegenüber dem Vorjahr erreicht wurde. In der Gesamtbetrachtung bleiben die Zahlen auf hohem Niveau und haben sich in den vergangenen zehn Jahren mehr als versechsfacht. Die Aufklärungsquote sank um 0,9 Prozentpunkte.

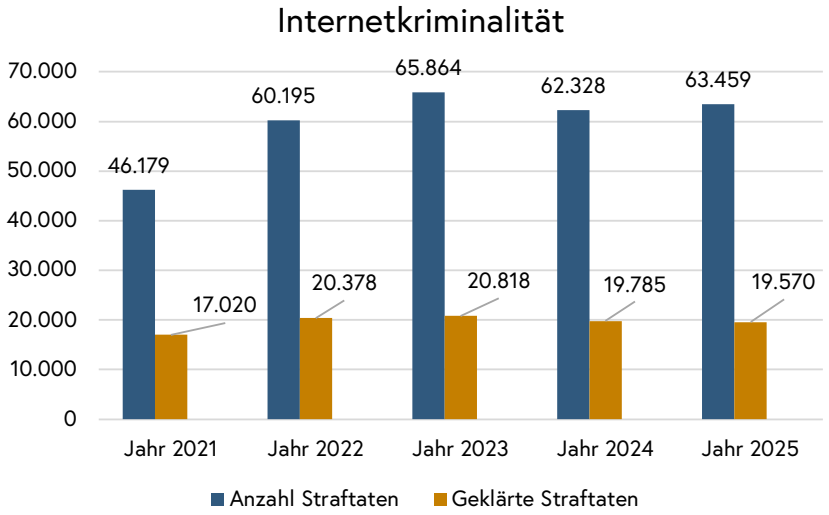

Abbildung 5: Entwicklung der Anzeigen und aufgeklärten Fälle von Cybercrime 2021 bis 2025

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 bei der Datenbeschädigung, dem Hacking oder sogenannten „Distributed Denial of Service“-(DDoS)-Angriffen.

Im Jahr 2025 konnte bei den Tatbeständen zu Cybercrime im engeren Sinn eine Zunahme der Anzeigen um 8,6 Prozent gegenüber dem Vorjahr verzeichnet werden. Dies lässt sich vor allem auf vermehrte Anzeigen im Bereich des § 148a StGB (Betrügerischer Datenverarbeitungsmissbrauch) und § 225a StGB (Datenfälschung) zurückführen.

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 immer intensiver, was auch zu einem Anstieg der strafbaren Handlungen in diesem Bereich führt.

Bei den Anzeigen nach § 126 a, § 126b und § 126c StGB handelt es sich oftmals um strafbare Handlungen, die Wirtschaftsbetriebe treffen. Die Zahl der Anzeigen bei § 126c

StGB (Missbrauch von Computerprogrammen oder Zugangsdaten) sank um 48 Prozent im Vergleich zum Vorjahr. Die Präventionskampagnen zeigten offenbar Wirkung.

Weiterhin eine Herausforderung stellt das sogenannte Cybermobbing (Fortdauernde Belästigung im Wege der Telekommunikation oder eines Computersystems § 107c StGB) dar, das auf 521 angezeigte Delikte anstieg.

§ 148a StGB regelt den betrügerischen Datenverarbeitungsmissbrauch, bei dem das Ergebnis einer automatisierten Datenverarbeitung unrechtmäßig beeinflusst wird, um sich oder Dritten einen Vermögensvorteil zu verschaffen, und bildet den größten Teil der Straftaten im Bereich „Cybercrime im engeren Sinn“ ab. Der Straftatbestand gewinnt zunehmend an Bedeutung, insbesondere in einer digitalisierten Welt mit automatisierten Systemen und KI-Anwendungen. Der Anstieg im Jahr 2025 lässt sich auf folgende **Ursachen zurückführen: Anrufkriminalität Tech Support, Abbuchung vom Konto (zumeist nach Phishing)**, Online-Bestellungen auf fremden Namen, Bestellbetrug (Ware nicht bezahlt).

Grundsätzlich steht § 225a StGB überwiegend in Kombination mit weiteren Straftaten wie insbesondere Betrug, Erpressung, Cybermobbing etc. So werden gefälschte Dokumente (zum Beispiel Lohnzettel, Meldezettel) für die Eröffnung eines Online-Kontos, den Abschluss von Online-Verträgen (zum Beispiel Handytarif) oder die Beantragung von Online-Krediten verwendet. Weitere relevante Sachverhalte in diesem Zusammenhang sind zum Beispiel: Bestellung von Waren auf fremden Namen, Veränderung von Fotos oder Accounts, Erstellung von Accounts im Namen der Opfer, gefälschte E-Mails für die Durchführung von Straftaten wie Betrug oder Erpressung.

Delikt	Angezeigte Fälle 2024	Angezeigte Fälle 2025	Geklärte Straftaten 2024	Geklärte Straftaten 2025
§ 107c StGB	462	521	355	413
§ 118a StGB	1.991	2.060	250	324
§ 119 StGB	12	20	10	16
§ 119a StGB	63	62	12	11
§ 126a StGB	241	270	58	67
§ 126b StGB	76	111	7	8
§ 126c StGB	496	258	67	52
§ 148a StGB	16.192	17.799	2.297	2.890
§ 225a StGB	713	887	237	245
Gesamt	20.246	21.988	3.293	4.026

§ 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 Paragraphen des Strafgesetzbuches – Vergleich 2024/2025.

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 Betrugsdelikte, Drogenhandel im Darknet, Cybergrooming oder Cybermobbing. In der Polizeilichen Kriminalstatistik umfasst Cybercrime im weiteren Sinne bspw. die Paragraphen 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. Nahezu die Hälfte der Internetdelikte entfällt auf Betrugsdelikte: 2025 wurden 31.001 Fälle von Internetbetrug angezeigt, ein Rückgang von 2,4 Prozent im Vergleich zum Vorjahr. Diese positive Entwicklung lässt sich durchaus auf die wirksame Präventionsarbeit zurückführen. Mit der fortschreitenden Digitalisierung verlagern sich Betrugsdelikte immer mehr ins Internet. Für die Täterinnen und Täter 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“) als Modus Operandi und international agierende Call-Center konnten nach wie vor festgestellt werden, ebenso der digitale Investmentbetrug.

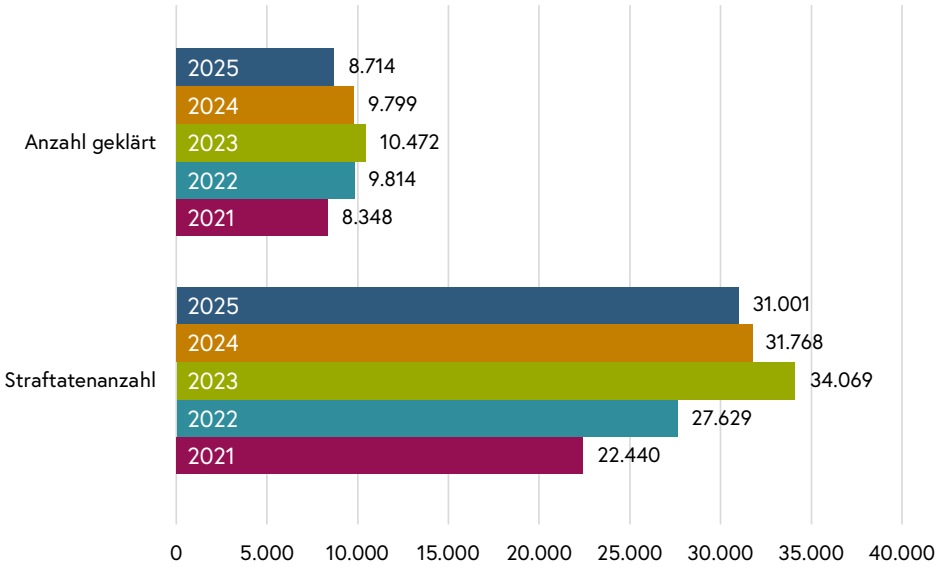

Abbildung 6: Fünfjahresvergleich Internetbetrug §§ 146 bis 148 StGB (Örtlichkeit „Internet“)

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, 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 2025 ein deutlicher Anstieg 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 § 105 StGB (Nötigung, 481 Anzeigen), § 107 StGB (Gefährliche Drohung, 1.714 Anzeigen) und § 27 SMG (Unerlaubter Umgang mit Suchtgiften, 1.116 Anzeigen) verzeichnet. § 3g Verbotsgesetz (Nationalsozialistische Wiederbetätigung, 1.206 Anzeigen) war auf einem anhaltend hohen Niveau.

SMS-Nachrichten zum Daten-Phishing sind weiterhin stark präsent: Es kursierten mehrere Spam-Kampagnen, die einen Hinweis auf eine angebliche „Zustellbenachrichtigung“ und weiterführende Links enthielten. Verstärkt wurden hier Links von nicht existierenden Zahlungsdienstleistern verwendet. Gegen Jahresende – in der Vorweihnachtszeit – stieg erneut die saisonal beobachtbare Anzahl an kriminellen Webshops (Fake- und Phishing-Shops) deutlich an. Auch zahlreiche Spamwellen mit Erpressungs-Mails (Sextortion) und

E-Mails zum Phishing von Bankdaten waren 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 2025 auf. Opfer möchten private Gegenstände auf Kleinanzeigenplattformen verkaufen. Täterinnen und Täter stellen den Kontakt zu den Opfern her und bekunden scheinbares Kaufinteresse. Die Täterinnen und Täter wirken seriös und ernsthaft interessiert. Schließlich wird von den Betrügerinnen und Betrügern vorgeschlagen, die Zahlung und die Übergabe der Ware über einen 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 scheinbar überwiesen werden kann. Mit dem Bestätigen der Freigabe wird schließlich kein Geld überwiesen. Stattdessen 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 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 als Zahlungsempfängerin oder Zahlungsempfänger ausländische Kontodaten 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 Hackerinnen und 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.

Erpressungen im Internet (§§ 144, 145 StGB)

Erfreulich ist der Rückgang der Anzeigen wegen Erpressung im Internet um 18,8 Prozent im Vergleich zum Vorjahr auf 2.380 angezeigte Fälle. Gleichzeitig konnte die Aufklärungsquote um 1,8 Prozentpunkte auf 9,6 Prozent gesteigert werden.

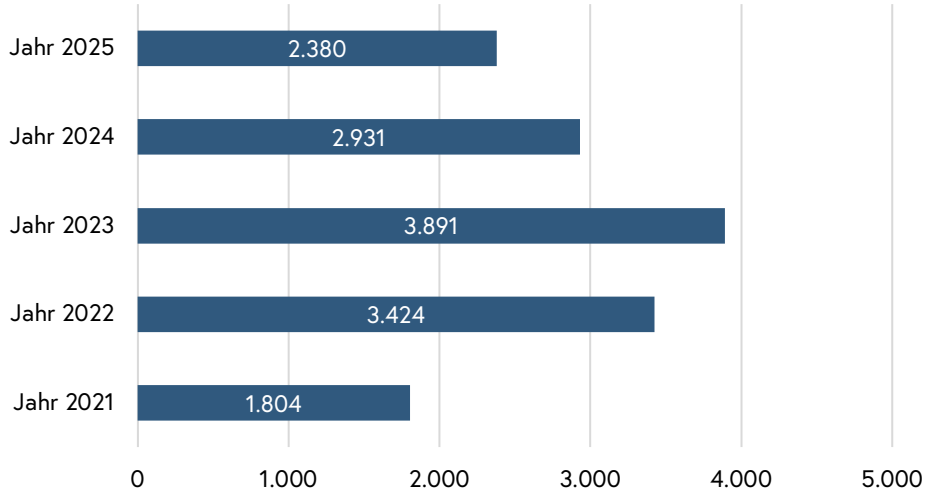

Abbildung 7: Erpressung im Internet – § 144 StGB (Erpressung), 145 StGB (Schwere Erpressung)

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 u. dgl.) vorgetäuscht und mit einem Strafverfahren gedroht, beispielsweise wegen Kinderpornografie, 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 2024	Angezeigte Fälle 2025	Geklärte Straftaten 2024	Geklärte Straftaten 2025
		Internetbetrug		
§ 146 StGB	26.578	25.571	8.101	6.892
§ 147 StGB	4.404	4.628	1.332	1.422
§ 148 StGB	786	802	366	400
Gesamt	31.768	31.001	9.799	8.714

Delikt	Angezeigte Fälle 2024	Angezeigte Fälle 2025	Geklärte Straftaten 2024	Geklärte Straftaten 2025
Sonstige Kriminalität im Internet				
§ 105 StGB	341	481	235	281
§ 106 StGB	187	218	142	175
§ 107 StGB	1.472	1.714	1.303	1.495
§ 107a StGB	419	462	386	421
§ 111 StGB	15	89	13	70
§ 115 StGB	60	59	46	51
§ 218 StGB		73		46
§ 223 StGB	125	142	95	108
§ 224 StGB	64	94	33	77
§ 228 StGB	2	2	2	2
§ 229 StGB	2	2	1	2
§ 231 StGB	44	59	12	18
§ 232 StGB	38	18	37	14
§ 241a StGB	3	3	1	0
§ 282 StGB		70		70
§ 283 StGB	309	279	302	265
§ 297 StGB	10	159	10	139
§ 27 SMG	762	1.116	570	627
§ 28 SMG	8	36	7	25
§ 28a SMG	54	95	44	67
§ 30 SMG	45	52	40	37
§ 32 SMG		1		1
§ 3a VerbotsG	1	1	1	1
§ 3d VerbotsG	7	4	6	4
§ 3e VerbotsG	1	1	0	1
§ 3g VerbotsG	1.222	1.206	1.186	1.179
§ 3h VerbotsG	50	60	48	59
§ 4 NPSG	129	186	102	116
Sonstige Kriminalität im Internet Summe	**5.370**	**6.682**	**4.622**	**5.351**

Tabelle 5: Jahresvergleich 2024/2025 angezeigte Fälle von Cybercrime im weiteren Sinn nach Paragraphen

3.4 Dunkelziffer und Anzeigeverhalten

Die Dunkelziffer im Bereich der Internetkriminalität ist ein komplexes Phänomen, das durch eine Vielzahl von Faktoren beeinflusst wird. Internationale Erfahrungswerte zeigen, dass die Dunkelziffer im Bereich der Internetkriminalität besonders hoch ist, da viele Betroffene aus Scham, Angst oder wegen geringer Schäden keine Anzeige erstatten.

Es gibt mehrere Gründe, warum die Anzeige von Internetkriminalität wichtig ist:

- Verbesserung der Beweismittellage: Jede Anzeige kann dazu beitragen, die Beweismittellage gegen verdächtige Tätergruppen zu stärken. Durch die Analyse von Anzeigen und Beweismitteln können die Strafverfolgungsbehörden ein umfassenderes Bild von den Täterinnen und Tätern und ihren Methoden erhalten.
- Frühe Erkennung von neuen Massenphänomenen: Die Anzahl der Anzeigen kann dazu beitragen, neue Massenphänomene früher zu erkennen. Durch die Analyse von Anzeigen und Trends können die Strafverfolgungsbehörden neue Bedrohungen identifizieren und präventive Maßnahmen ergreifen.
- Präventionsmaßnahmen: Durch die Anzahl der Anzeigen können Präventionsmaßnahmen zeitnäher gesetzt werden. Die Strafverfolgungsbehörden können aufgrund der Anzeigen gezielte Präventionsmaßnahmen entwickeln und umsetzen, um die Anzahl der Geschädigten zu reduzieren.
- Reduzierung der Anzahl der Geschädigten: Mit zielgerichteten Warnhinweisen kann die Anzahl der Geschädigten reduziert werden. Durch die Verbreitung von Warnhinweisen und Informationen über die Methoden der Täterinnen und Täter können die Bürgerinnen und Bürger besser vorbereitet werden, um sich vor Internetkriminalität zu schützen.

Es ist jedoch wichtig zu beachten, dass die Wiedererlangung abhandengekommener Vermögenswerte nicht immer gelingt. Dies liegt daran, dass die Täterinnen und Täter oft ihre Spuren gut verwischen und die Strafverfolgungsbehörden Schwierigkeiten haben, die Täterinnen und Täter zu identifizieren und zu verfolgen.

Deshalb ist es wichtig, dass die Verhinderung von Straftaten durch verstärkte Bewusstseinsbildung und Aufklärung priorisiert wird. Die Täterinnen und Täter nutzen oft menschliche Schwächen wie Gier und Sehnsüchte nach Anerkennung oder Beziehungen aus, um sich zu bereichern. Social Engineering bleibt ein maßgeblicher Angriffsvektor, da die Täterinnen und Täter oft psychologische Manipulationen anwenden, um die Opfer zu täuschen.

Die Bekämpfung der Internetkriminalität erfordert eine enge Zusammenarbeit zwischen Strafverfolgungsbehörden und der Zivilgesellschaft. Um wirksam zu sein, müssen Bürgerinnen und Bürger über die Methoden und Taktiken der Internetkriminellen informiert

werden, damit sie sich selbst vor möglichen Angriffen schützen können. Gleichzeitig müssen Strafverfolgungsbehörden ihre Kapazitäten und Ressourcen ausbauen, um effektiv gegen die Täterinnen und Täter vorgehen zu können. Internetkriminalität ist ein vielschichtiges Problem, das eine umfassende und koordinierte Anstrengung erfordert. Durch die Kooperation zwischen Strafverfolgungsbehörden, Bürgerinnen und Bürgern sowie anderen relevanten Akteurinnen und Akteuren kann dieses Kriminalitätsfeld gezielt bekämpft und die Sicherheit im Internet verbessert werden.

4 Ermittlungserfolge (Beispiele)

4.1 Operation „Bunker“ (Gemeinsamer Erfolg DSN/ Bundeskriminalamt)

Verfassungsschutz forscht gemeinsam mit Bundeskriminalamt „Swatting-Netzwerk“ aus

Falsche Bombendrohungen lösten österreichweit Großeinsätze aus – koordinierter Zugriff im Ausland stoppt Tätergruppe.
Der Direktion Staatsschutz und Nachrichtendienst (DSN) ist in enger Zusammenarbeit mit den Landesämtern Staatsschutz und Extremismusbekämpfung (LSE), dem österreichischen Bundeskriminalamt (BK), den Landeskriminalämtern (LKA) und internationalen Partnern ein entscheidender Schlag gegen ein kriminelles Netzwerk gelungen, das für eine Serie von sogenannten „Swatting“-Vorfällen verantwortlich war. Unter Swatting versteht man gezielte Falschmeldungen, die polizeiliche und rettungsdienstliche Großeinsätze auslösen und erhebliche öffentliche Verunsicherung durch breite öffentliche Berichterstattung hervorrufen. Das Netzwerk steht im Verdacht, seit September 2024 per E-Mail mehrfach Bombendrohungen an öffentliche Einrichtungen und Bildungseinrichtungen in mehreren Bundesländern verschickt zu haben.

Intensive Ermittlungen des Verfassungsschutzes und Bundeskriminalamts
Seit 2024 ermittelte die DSN intensiv zu einer Serie von Bombendrohungen, die durch E-Mails verschickt wurden. Insgesamt langten bis dato in Österreich über 300 Drohungen ein, die der Tätergruppe zugeordnet werden können.
Durch umfangreiche Ermittlungen konnte die DSN in Kooperation mit Ermittlerinnen und Ermittlern des Cybercrime Competence Centers (C4) des österreichischen Bundeskriminalamts sowie dem LKA Salzburg die mutmaßlichen Hauptakteure identifizieren. Bei den Tätern handelt es sich um vier deutsche Staatsangehörige im Alter von 16 bis 23 Jahren, die sich über verschlüsselte Kommunikationsplattformen und anonyme Internetdienste organisiert haben. Die Täter versuchten, durch eine Reihe von Anonymisierungstechniken ihre Spuren und Identitäten zu verschleiern. Aufgrund der technischen Analysen der Täterinfrastruktur und der Verfolgung der Spur der Kryptowährungen durch das C4 war es möglich, einzelne Täter zu identifizieren.
Am 25. November 2025 haben die deutschen und österreichischen Behörden gemeinsam Hausdurchsuchungen und Sicherstellungen bei den Verdächtigen durchgeführt. Zuvor fanden bereits bei drei weiteren Tatverdächtigen weitere Maßnahmen durch die deutschen

Sicherheitsbehörden statt. Die Ermittlungen wurden an das deutsche Bundeskriminalamt übergeben und fortgesetzt.

Hintergrund zum Phänomen „Swatting“

„Swatting“ bezeichnet das absichtliche Auslösen gefälschter Notfälle unter falschem Namen, um ein Eingreifen von Spezialeinheiten („SWAT“) oder andere Großeinsätze auszulösen. Neben der strafrechtlichen Relevanz stellt diese Form der Bedrohung eine erhebliche Gefahr für Einsatzkräfte und unbeteiligte Personen dar. Ursprünglich richtete sich diese Mobbingart überwiegend gegen Einzelpersonen. Eine Gefahrensituation wurde vorgetäuscht, um beim Opfer das Einschreiten von Einsatzkräften zu provozieren. In jüngster Vergangenheit wurde allerdings eine abgewandelte Form des Swattings beobachtet: Nicht nur Einzelpersonen, sondern insbesondere öffentlich zugängliche Einrichtungen wie Schulen, Behörden, Bahnhöfe und Einkaufszentren standen im Fokus der Kriminellen. In den österreichischen „Swatting-Fällen“ wurden schwerpunktmäßig vorgetäuschte Bombendrohungen abgesetzt. Die Ermittlungen zeigen, dass die intrinsische Tatseite der Kriminellen auf eine größtmögliche mediale Berichterstattung abzielt. Eine großräumige Evakuierung einer Schule oder eines Bahnhofs mit entsprechendem Medienecho wird auf Täterseite als Erfolg verbucht und online damit geprahlt.

Vorgehensweise der Tätergruppe

Den Erkenntnissen des Verfassungsschutzes zufolge vernetzten sich die Täterinnen und Täter über verschiedene Online-Plattformen und tauschten sich ausschließlich in der virtuellen Welt aus. Es ist davon auszugehen, dass sich die überwiegend jugendlichen und teils noch minderjährigen Personen in der Regel nicht persönlich kennen und anonym bleiben wollen. In diesem losen Zusammenschluss sind sie vermutlich auf der Suche nach Anerkennung und Abenteuer. Eine hierarchische Rangordnung unter den Kriminellen ist derzeit nicht ableitbar. Je nach Erfolg des ausgelösten Einsatzes steigt der eigene Status innerhalb der Szene.

Fallweise löst eine Person mit einer E-Mail über 100 Drohungen aus. Anders als in der ursprünglichen Form des Swattings, wo das Opfer gemobbt werden soll, steht hier tatsächlich das Medienecho im Zentrum. Die Täterinnen und Täter fühlen sich durch öffentliche Aufmerksamkeit in ihrem Handeln bestätigt und können dies in Foren, Chats usw. als Erfolg präsentieren, beispielsweise durch Veröffentlichung von Screenshots von Medienberichten auf ihren Online-Profilen.

Rechtliche Konsequenzen

Das vorsätzliche Absetzen falscher Bombendrohungen oder anderer schwerwiegender Notrufe ist in Österreich eine Straftat und kann mit Freiheits- und Geldstrafen geahndet werden. Darüber hinaus können die verursachten Kosten für Polizeieinsätze, Evakuierungen und andere Maßnahmen, die sich oft im hohen vier- bzw. fünf- oder sogar sechsstelligen Bereich bewegen, den Täterinnen bzw. den Tätern vollständig in Rechnung

gestellt werden. Dies kann zu Schadensersatzforderungen führen und auch zivilrechtliche Ansprüche von Betroffenen bleiben unberührt.

Weitere Informationen: https://www.bundeskriminalamt.at/newsba08.html?id=70586855465650595556673d

Mediale Berichterstattung

Bei Swatting-Einsätzen und hacktivistisch motivierten Cyberangriffen, insbesondere Distributed-Denial-of-Service-(DDoS-)Angriffen, stellt die Erzielung öffentlicher Aufmerksamkeit häufig ein wesentliches Tatmotiv dar. Die mediale Berichterstattung über entsprechende Vorfälle wird von den Akteurinnen und Akteuren regelmäßig zur Selbstinszenierung genutzt und innerhalb einschlägiger Szenen als Erfolgsnachweis („Trophäe") verbreitet. Die dadurch erzielte Sichtbarkeit kann Nachahmungshandlungen begünstigen und zur Steigerung des Ansehens der Täterinnen und Täter innerhalb ihrer jeweiligen Bezugsgruppen beitragen.

Vor diesem Hintergrund wird um eine entsprechende Berücksichtigung dieses Umstands in der medialen Berichterstattung ersucht. So können etwa plakative Schlagzeilen wie „Evakuierung nach Bombendrohung" oder eine besondere Hervorhebung der Tätergruppe oder der Auswirkungen eines Vorfalls von den Täterinnen und Tätern als Beleg für die Wirksamkeit ihrer Handlungen instrumentalisiert werden. Eine sachliche und verhältnismäßige Berichterstattung kann dazu beitragen, die angestrebten Aufmerksamkeitseffekte und strategischen Kommunikationsziele nicht zusätzlich zu fördern sowie eine unbegründete Verunsicherung in der Bevölkerung zu vermeiden.

4.2 Anlagebetrug mittels Kryptowährungen – Komplexes Ermittlungsverfahren in Kärnten

In Kärnten wurde einer der bedeutendsten österreichischen Fälle von Kryptowährungsbetrug gerichtlich abgeschlossen. Als führende Ermittlungsstellen waren die Wirtschafts- und Korruptionsstaatsanwaltschaft (WKStA), der Ermittlungsbereich EB 05 Betrug und der Assistenzbereich 06 IT-Beweissicherung des Landeskriminalamtes Kärnten sowie das Bundeskriminalamt tätig.

Die Täter betrieben über mehrere Jahre ein international ausgerichtetes Firmen- und Plattformnetzwerk, über das Anlegerinnen und Anlegern hohe Renditen durch Investitionen in Kryptowährungen sowie angebliche Immobilien- und Technologieprojekte versprochen wurden. Zur Gewinnung neuer Investorinnen und Investoren kamen professionelle Online-Auftritte, Social-Media-Marketing und Empfehlungsprogramme zum Einsatz.

Die Ermittlungen ergaben, dass die beworbenen Geschäftsmodelle und Ertragsquellen weitgehend nicht vorhanden beziehungsweise wirtschaftlich nicht nachvollziehbar

waren. Anlegerinnen und Anlegern wurden über digitale Plattformen und Wallet-Systeme teilweise fiktive Vermögenswerte und Gewinne angezeigt. Die Finanzierung von Auszahlungen erfolgte zumindest teilweise durch Einzahlungen neuer Investorinnen und Investoren.

Von dem Betrugssystem waren rund 40.000 Personen im In- und Ausland betroffen. Der nachgewiesene Schaden belief sich auf etwa 20 Millionen Euro. Die Täter verschleierten Geldflüsse durch internationale Firmenstrukturen, Kryptowallets und zahlreiche Transaktionen über verschiedene Blockchain-Netzwerke.

Das Ermittlungsverfahren stellte aufgrund seines Umfangs und seiner internationalen Verflechtungen eine besondere Herausforderung dar. Neben einer Vielzahl von Beschuldigten und weiteren Verfahrensbeteiligten mussten zahlreiche Geschädigte identifiziert, vernommen und deren Vermögensschäden dokumentiert werden. Zusätzlich erschwerte ein komplexes Geflecht aus nationalen und internationalen Gesellschaften die Nachvollziehbarkeit von Verantwortlichkeiten und Finanzströmen.

Einen wesentlichen Ermittlungsaufwand verursachte zudem die Auswertung einer großen Anzahl sichergestellter digitaler Datenträger. Besonders ressourcenintensiv war die Analyse von mehreren tausend Kryptowährungstransaktionen über unterschiedliche Wallets, Börsen und Blockchain-Netzwerke hinweg. Zur Bewältigung dieser zahlreichen komplexen Aufgaben leistete auch das Bundeskriminalamt entsprechende Unterstützung.

Der Fall verdeutlicht die zunehmende Professionalisierung von Anlagebetrügerinnen und -betrügern im Bereich digitaler Vermögenswerte sowie die Bedeutung spezialisierter Ermittlungs- und Analysemethoden bei der Bekämpfung komplexer Cybercrime-Delikte.

4.3 Operation „SIMCARTEL"

Cybercrime as a Service: Internationales Ermittlerinnen- und Ermittlerteam zerschlägt kriminelles Netzwerk
Joint Action Day in Riga – sieben Festnahmen, über 1.200 SIM-Boxen und 40.000 SIM-Karten sichergestellt
Im Rahmen einer international koordinierten Operation ist es dem Bundeskriminalamt (BK) in enger Zusammenarbeit mit dem Landeskriminalamt Salzburg unter der Leitung der Staatsanwaltschaft Wien gelungen, ein hochorganisiertes, weltweit agierendes Cybercrime-Netzwerk zu zerschlagen.
Die Maßnahmen erfolgten in Kooperation mit Lettland, Estland, Europol und Eurojust. Im Zuge eines koordinierten „Joint Action Day" am 10. Oktober 2025 in Riga/Lettland kam es zu sieben Festnahmen, zahlreichen Hausdurchsuchungen sowie umfangreichen Sicherstellungen.

„Der aktuelle Erfolg des Bundeskriminalamtes und des Landeskriminalamtes Salzburg zeigt einmal mehr: Die enge internationale Kooperation ist entscheidend im Vorgehen gegen die internationale Kriminalität. Unsere Spezialistinnen und Spezialisten genießen weltweit einen ausgezeichneten Ruf“, sagte Innenminister Gerhard Karner.

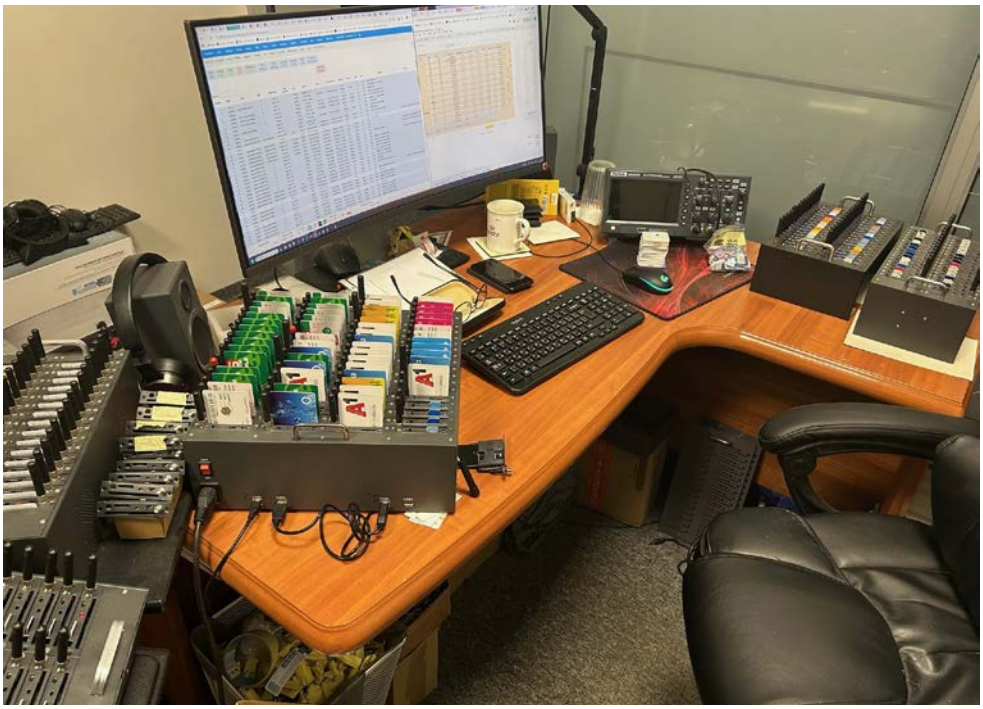

Foto: © State Police of Latvia/Arturs Andrejs Blomkalns

International koordinierte Ermittlungen

Die Ermittlungen richteten sich gegen ein kriminelles Netzwerk, das im sogenannten „Cybercrime as a Service“-Bereich tätig war und technische Infrastruktur für betrügerische und erpresserische Aktivitäten bereitstellte.

Über eigens entwickelte Online-Plattformen boten die Täter anonymisierte Telefonnummern an, die auf fremde Identitäten in über 80 Ländern registriert waren. Diese Dienste ermöglichten es anderen kriminellen Gruppen, verschiedenste Delikte zu begehen – von Online-Betrug, Erpressung und Schlepperei bis hin zur Verbreitung kinderpornografischen Materials.

In enger Abstimmung mit Europol und Eurojust konnten Ermittlerinnen und Ermittler aus Österreich, Lettland und Estland dem Netzwerk mehr als 3.200 Betrugsfälle zuordnen. Mehr als 1.700 Fälle wurden in Österreich verzeichnet, rund 1.500 in Lettland. Der dabei entstandene Schaden beläuft sich auf mehr als 4,5 Millionen Euro.

„Dieser Einsatz zeigt einmal mehr, dass Cyberkriminalität nur durch enge internationale Kooperation wirksam bekämpft werden kann. Die erfolgreiche Zerschlagung dieser Infrastruktur ist das Ergebnis monatelanger, präzise koordinierter Ermittlungsarbeit und verdeutlicht, dass Kriminelle auch im digitalen Raum keine Grenzen ausnutzen können,

ohne auf entschlossene Strafverfolgung zu stoßen“, sagte der Direktor des Bundeskriminalamtes Andreas Holzer.

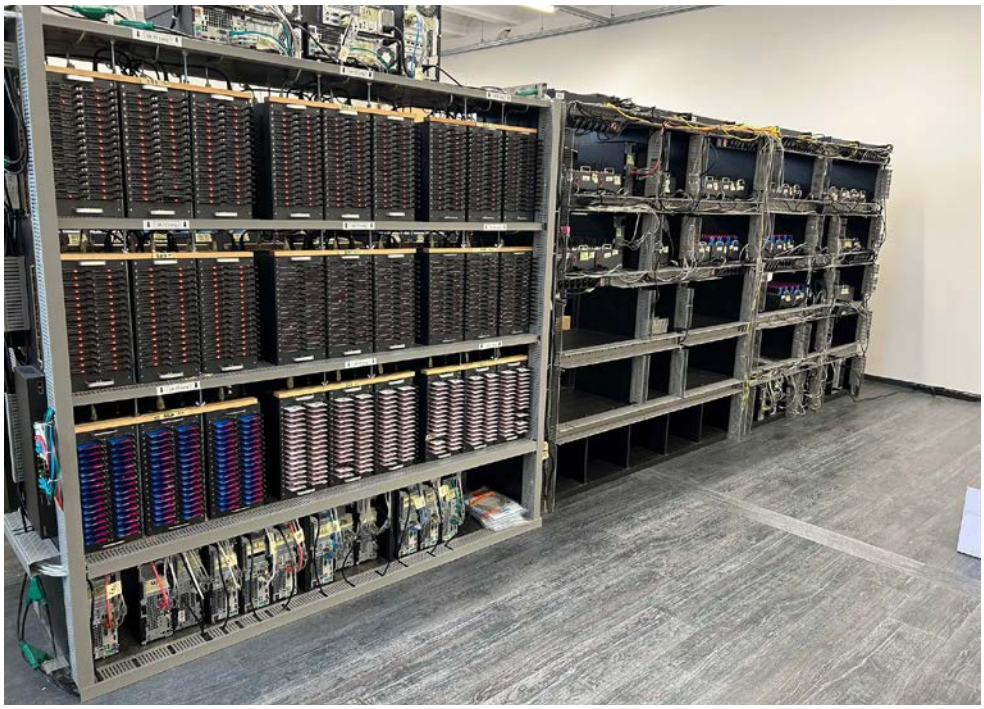

Foto: © State Police of Latvia/Arturs Andrejs Blomkalns

Weiterführende Informationen: https://www.bundeskriminalamt.at/newsa403.html?id=41665731317875324739513d

4.4 Weitere internationale Amtshandlungen mit Beteiligung des österreichischen Bundeskriminalamts

Operation „Stream“

Kidflix, eine der weltweit größten Plattformen für pädophile Inhalte, wurde im Rahmen einer internationalen Operation gegen sexuellen Kindesmissbrauch abgeschaltet. Die Ermittlungen wurden von Europol unterstützt und vom Bayerischen Landeskriminalamt sowie der Zentralstelle Cybercrime Bayern (ZCB) geleitet. Über 35 Länder weltweit beteiligten sich an der Operation, auch das Bundeskriminalamt Österreich.

https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users

Operation „Cumberland“

Bei einer europaweiten Polizeiaktion gegen eine kriminelle Gruppe, die an der Verbreitung von Missbrauchsbildern von Minderjährigen beteiligt war, konnten mehr als 273 Tatverdächtige identifiziert und im Februar vergangenen Jahres 25 Festnahmen durchgeführt werden. Ausgangspunkt der Operation war die Verhaftung eines dänischen Staatsangehörigen im November 2024, der über eine von ihm betriebene Online-Plattform mittels KI erstelltes Missbrauchsmaterial verbreitet hatte. An der unter der Leitung der dänischen Strafverfolgung durchgeführten Operation „Cumberland“ waren neben 18 weiteren Staaten auch das österreichische Bundeskriminalamt in Kooperation mit den Landeskriminalämtern Wien und Burgenland beteiligt.

https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

Operation „RapTor“

270 Festnahmen bei weltweiter Razzia im Darknet gegen Online-Drogen- und kriminelle Netzwerke. Eine von Europol koordinierte globale Strafverfolgungsaktion hat dem organisierten Verbrechen einen schweren Schlag versetzt: 270 Händlerinnen und Händler sowie Käuferinnen und Käufer wurden in zehn Ländern festgenommen. Die internationale Razzia mit dem Namen Operation „RapTor“ zerschlug Netzwerke, die mit Drogen, Waffen und gefälschten Waren handelten, und sendete damit ein klares Signal an Kriminelle, die sich hinter der Illusion der Anonymität verstecken.

https://www.europol.europa.eu/media-press/newsroom/news/270-arrested-in-global-dark-web-crackdown-targeting-online-drug-and-criminal-networks

5 C4 – Schwerpunkte und Abläufe

5.1 Nationale und internationale Koordinierungs-, Ermittlungs- und Meldestelle

Das Cybercrime Competence Center (C4) ist eine spezialisierte Einheit innerhalb des Bundeskriminalamts, die 2011 gegründet wurde, um die Bekämpfung von Computerkriminalität voranzutreiben. Die Hauptaufgabe des C4 besteht darin, die Koordination und Unterstützung von Ermittlungen im Zusammenhang mit Cybercrime zu gewährleisten, wie Hacking, Phishing, Online-Betrug und andere Formen von Computerkriminalität.

Das C4 ist auch für die elektronische Beweismittelsicherung und deren Auswertung zuständig, um Beweise für Strafverfahren zu sichern und auszuwerten. Durch die nationale und internationale Koordination und Zusammenarbeit bei der Bekämpfung von Cybercrime kann das C4 eine effektive und grenzüberschreitende Bekämpfung von Computerkriminalität ermöglichen.

Das C4 dient als wichtige Drehscheibe und Koordinationspunkt für alle Polizeidienststellen in Österreich, um landesweite und internationale Ermittlungen zu unterstützen und zu koordinieren. Durch die enge Zusammenarbeit mit anderen Behörden und Organisationen, wie der Direktion Staatsschutz und Nachrichtendienst (DSN), kann das C4 eine umfassende und effektive Bekämpfung von Cybercrime gewährleisten.

Das C4 ist auch Teil des Inneren Kreises der operativen Koordinierungsstrukturen (IKDOK), der von der Strategie des Bundeskanzleramts getragen wird. Durch diese enge Verbindung kann das C4 seine Arbeit laufend anpassen und eine effektive Unterstützung bei der Bekämpfung von Cybercrime leisten.

Für weitere Informationen zur Cybersicherheit kann die Website des Bundeskanzleramts unter https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment.html besucht werden. Dort finden sich umfassende Informationen zu den Themen Cybersicherheit, E-Government und Datenschutz sowie zu den Maßnahmen und Initiativen, die von der österreichischen Regierung ergriffen werden, um die Cybersicherheit in Österreich zu stärken.

Die Präventionsarbeit gewinnt im Cybercrime-Bereich immer mehr an Bedeutung, da viele Betrugsdelikte durch entsprechende Bewusstseinsbildung und Vorsicht verhindert werden

können. Deshalb wurden im Jahr 2025 zahlreiche Veranstaltungen von Ministerien, der Wirtschaftskammer und weiteren relevanten Organisationen mit Expertise unterstützt, um die Öffentlichkeit über die Risiken und Gefahren im Cybercrime-Bereich aufzuklären.

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 2025** erreichten **16.968 Anfragen** die Meldestelle, wobei **10.220** davon einen Bezug zu Cybercrime hatten. Spammails traten über das ganze Jahr verteilt auf (insgesamt 5.331). Damit kann eine deutliche Zunahme der eintreffenden Meldungen im Vergleich zum Vorjahr festgestellt werden. Auf die verstärkten Präventionstätigkeiten seitens der Kriminalpolizei und nichtstaatlichen Organisationen sowie auf ein vermehrtes Bewusstsein in der Bevölkerung kann in diesem Zusammenhang verwiesen werden. Eine Diversifizierung der Meldemöglichkeiten für Unternehmen und Bevölkerung kann festgestellt werden.

Beispielhaft werden folgende Seiten erwähnt:
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 stellt sie das Koordinierungs- und Informationszentrum für diesen Themenkreis dar. Zusätzlich umfasst diese Tätigkeit proaktive und präventive Maßnahmen, wobei auftretende Phänomene, insbesondere im Bereich von Phishing-Attacken, auch ministeriumsübergreifend koordiniert und die notwendigen Maßnahmen eingeleitet werden. Die deutlich erkennbare Sensibilisierung und Bewusstseinsbildung zum Thema Cybercrime erfolgt unter anderem durch die fortlaufende Kooperation mit unterschiedlichen Institutionen aus dem Bereich der Wirtschaft und mit Vereinen, wie 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 zudem als Drehscheibe zu anderen internationalen Dienststellen und Polizeieinheiten wie dem Interpol Digital Cyber Center (IDCC), dem European Cybercrime Centre (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 diesbezüglichen 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

Berichtsmonat	Anzahl der relevanten E-Mail-Meldungen	Anzahl der relevanten Telefonmeldungen	Relevante Web-Frontend Meldungen	Summe aller Meldungen
Jänner 2025	734	41	21	1.245
Februar 2025	623	53	10	1.058
März 2025	678	28	15	1.285
April 2025	563	44	14	1.067
Mai 2025	609	39	30	1.341
Juni 2025	804	26	16	1.317
Juli 2025	842	37	17	1.598
August 2025	971	34	1	1.755
September 2025	1.132	33	3	1.911
Oktober 2025	1.134	40	0	1.835
November 2025	787	42	0	1.324
Dezember 2025	762	37	0	1.232

Tabelle 6: Monatliche Übersicht aller Meldungen an die C4 Meldestelle

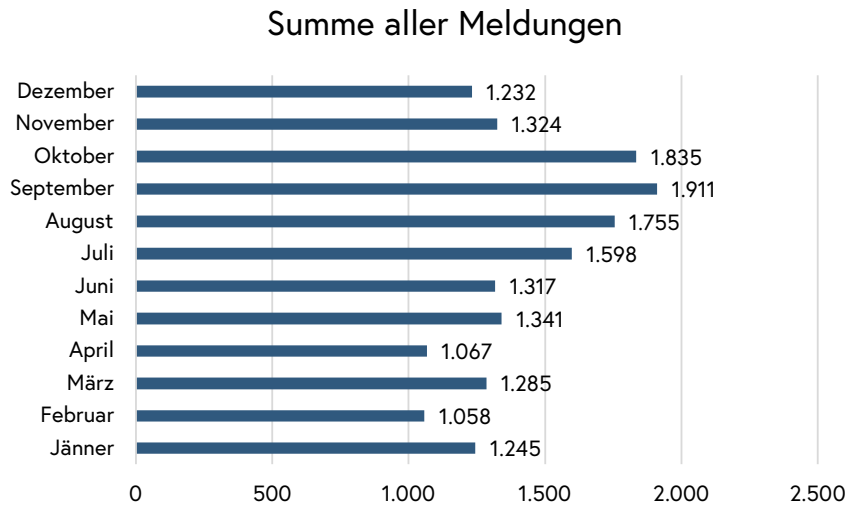

Abbildung 8: Gesamtanzahl der Meldungen an die C4 Meldestelle nach Monaten (Jahresverlauf)

5.2 Digitales Beweismittelmanagement (DBM)

Der Bereich „Digitales Beweismittelmanagement“ (DBM) im C4 fasst die Kompetenzen zusammen, 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 und bei Bedarf der Landeskriminalämter sowie das Fallmanagement als Schnittstelle zwischen Forensik, Ermittlungen, Technik und der Justiz.

Die Auswahl, Inbetriebnahme und laufende Betreuung moderner Auswertesoftware gehören dabei 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
- Auswahl und Einsatz moderner Software und performanter Hardware, um große digitale Beweismittelmengen überhaupt erst durchsuchbar und bearbeitbar zu machen

Foto: Serverlandschaft des C4 (© C4)

Mithilfe spezieller Programme zur Sichtung großer Datenmengen wurden 2025 insgesamt 42 neue Fälle mit einem Analyseausgangsdatenvolumen von über 31 Terabyte erstellt. Zusätzlich wurden 187 separate virtuelle Maschinen zur Beweismittelsichtung und fallbezogenen Recherche in Betrieb genommen, womit insgesamt über 1.000 Personen unterschiedlicher Aufgabenbereiche wie Ermittlungen, Analyse, Dolmetschdienst, Staatsanwaltschaften und Sachverständige Zugriff auf eine moderne Arbeitsumgebung zur Strafverfolgung erhalten haben. Im größten Einzelfall kooperierten mehr als 400 Personen.

Eine der wesentlichen Herausforderungen stellte 2025, wie auch in den Vorjahren, die Modernisierung der vorhandenen Speicher- und Rechenkapazität sowie die Verbesserung der Vernetzung mit weiteren Dienststellen dar. Es wurden Verbesserungen im Bereich der IT-Security zur Reduzierung von Risiken im Umgang mit Schmutzdaten umgesetzt. Die enge Zusammenarbeit mit dem Team des Projekts SeILE (Schaffung einer IKT-Lösung für kriminalpolizeiliche Ermittlungen) wurde fortgeführt sowie mit technischen Proof of Concepts unterstützt. Des Weiteren wurde die technische Mitarbeit bei operativen Fallbearbeitungen im Cybercrime Competence Center und darüber hinaus intensiviert.

5.3 C4 Forensik

Sowohl IT-Forensik als auch mobile Forensik spielen eine wichtige Rolle bei der Aufklärung von Straftaten und der Bekämpfung von Cyberkriminalität. Im Jahr 2025 mussten die Forensikerinnen und Forensiker des C4 eine erhebliche Datenmenge bewältigen, insgesamt 1.743,5 Terabyte (TB). Die Auswertung von digitalen Daten ist ein zentraler Aspekt kriminalpolizeilicher Ermittlungsarbeit. Die C4 Forensik hat sich als ein unverzichtbarer Partner bei der Bekämpfung von Cyberkriminalität und anderen schweren Straftaten erwiesen.

Die rasante technische Entwicklung und die zunehmende Verwendung von Schutzmechanismen wie Verschlüsselungsverfahren machen die Auswertung von digitalen Medien immer schwieriger. Die Forensikerinnen und Forensiker müssen daher ständig ihre Fähigkeiten und Kenntnisse aktualisieren, um mit den neuesten Technologien und Methoden Schritt halten zu können.

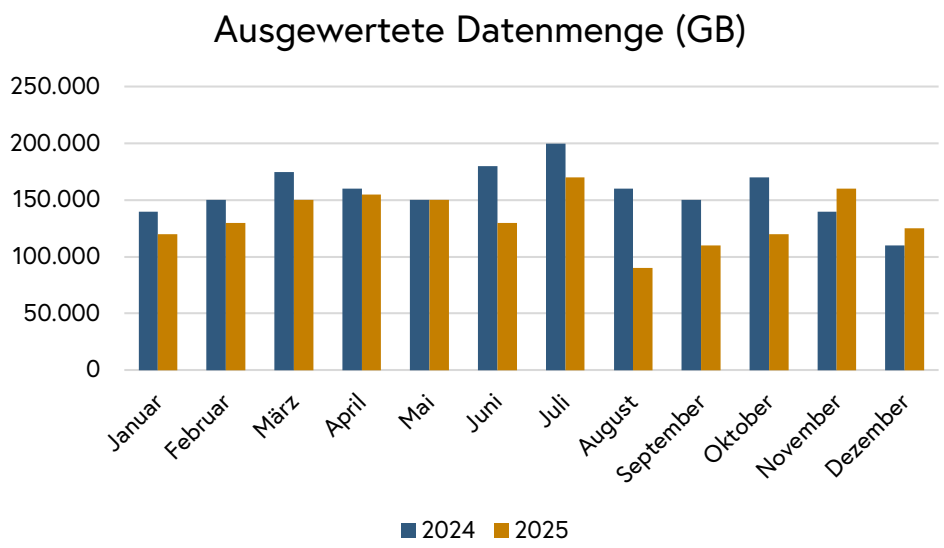

Abbildung 9: IT-Forensik – Ausgewertete Datenmengen in GB

Die C4 Forensik und die Landeskriminalämter müssen sich zunehmend mit umfassenden Auswertungen von Smartphones und Cloud-Speichern auseinandersetzen, die teilweise schwer bewältigt werden können. Die Menge der auszuwertenden Daten bleibt auf hohem Niveau, da Festplatten, Netzwerkdaten und Mobiltelefon-Daten immer größer und komplexer werden.

Insgesamt stellen die IT-Forensik und die mobile Forensik eine wichtige Komponente der Strafverfolgung dar, da sie es oftmals ermöglichen, digitale Beweismittel zu sichern und auszuwerten, um Straftaten aufzuklären und Täterinnen und Täter zu überführen.

Die Herausforderungen, die die IT-Forensik und die mobile Forensik mit sich bringen, erfordern jedoch eine ständige Anpassung und Weiterentwicklung der Methoden und Techniken, um die Effektivität und Effizienz der Ermittlungen zu gewährleisten.

Das Chip-Off-Verfahren, ein zeit- und ressourcenaufwendiger Prozess, bei dem Memory-Chips von ihrer Hardware physisch entfernt werden, kann nur zentral im Cybercrime Competence Center (C4) durchgeführt werden. Im Jahr 2025 wurden 113 solcher Verfahren abgeschlossen.

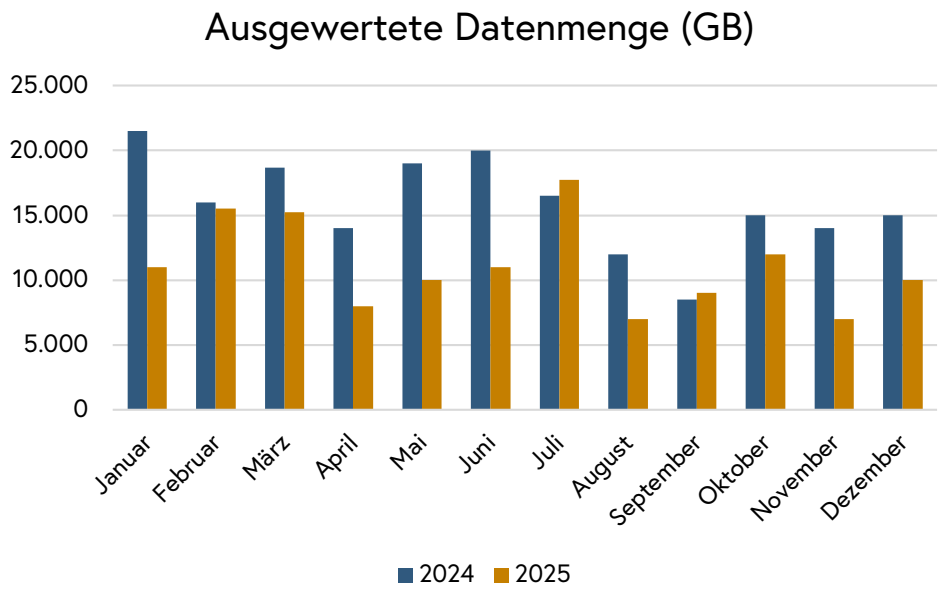

Abbildung 10: Mobile Forensik – Ausgewertete Datenmengen in GB

Die Kfz-Forensik spielt eine wichtige Rolle bei der Aufklärung von schweren Straftaten, insbesondere im Bereich der organisierten Kriminalität und der grenzüberschreitenden Schwerkriminalität. Hierbei wird ein Kraftfahrzeug oft als Transport- oder Tatmittel verwendet, wodurch es zu einem wichtigen Beweismittel wird. Die während des Betriebes automatisch generierten und gespeicherten Informationen können bei fachgerechter Auswertung und Aufbereitung für kriminalpolizeiliche Ermittlungen und das Strafverfahren von enormer Bedeutung sein.

Die Bediensteten des Fachbereichs Automotive IT des C4 führen bundesweit gerichtsverwertbare Beweisaufnahmen für alle Dienststellen des Bundesministeriums für Inneres und der Landespolizeidirektionen durch. Sie wirken auch aktiv an Schwerpunktaktionen und operativen Einsätzen mit, wenn die sofortige Sicherung von Beweismitteln notwendig erscheint und Anordnungen der Staatsanwaltschaften vollzogen werden müssen. In der Berichtsperiode Jänner bis Dezember 2025 wurden insgesamt 150 Fahrzeuge ausgewertet.

Aufgrund ihrer besonderen Expertise werden die Bediensteten der Automotive IT häufig zu internationalen Ermittlungen zur Auswertung von Fahrzeugdaten hinzugezogen. Ihre Arbeit ist von entscheidender Bedeutung für die Aufklärung von Straftaten und die Sicherung von Beweismitteln. Durch ihre enge Zusammenarbeit mit anderen Dienststellen und ihre Teilnahme an internationalen Ermittlungen tragen sie dazu bei, die Sicherheit und die Rechtsordnung in Österreich und im Ausland zu stärken.

5.4 Entwicklung und Innovation

Die zunehmende Komplexität von Straftaten und die Verwendung von fortschrittlichen Technologien durch Täterinnen und Täter erfordern eine integrierte Vorgehensweise, die sowohl die bewährten Fähigkeiten im Ermittlungsbereich als auch wissenschaftliche Unterstützung umfasst. Das Büro 5.4 – Entwicklung und Innovation – spielt eine entscheidende Rolle bei der Bereitstellung von wissenschaftlicher Expertise, um die kriminalpolizeiliche Arbeit zu unterstützen.

Die Analyse von komplexen Datenmengen und die Identifizierung von Mustern und Zusammenhängen erfordern eine Vielzahl von wissenschaftlichen Methoden und Techniken. Im Jahr 2025 hat das Büro 5.4 eine Reihe von Projekten durchgeführt, die die Anwendung von mathematischen und statistischen Methoden bei der Analyse von Geldflüssen in Kryptowährungen, der Untersuchung von forensischen Artefakten und der Entschlüsselung von Daten und Datenträgern umfassten.

Die Zusammenarbeit mit den Ermittlerinnen und Ermittlern ist von entscheidender Bedeutung, um die komplexen Zusammenhänge zu erkennen und nachzuweisen. Es ist jedoch nicht nur wichtig, Erkenntnisse zu gewinnen, sondern auch, sie in einer übersichtlichen und nachvollziehbaren Form darzustellen, um sie für die kriminalpolizeiliche Arbeit nutzbar zu machen.

Eine weitere wichtige Aufgabe des Büros 5.4 ist die Beobachtung und Analyse neuer Technologien auf ihre Bedeutung für die kriminalpolizeiliche Arbeit. Im Jahr 2025 lag ein Schwerpunkt auf künstlicher Intelligenz. Es wurde in nationalen und internationalen Projekten, Arbeitsgruppen und Gremien mitgearbeitet, um die Zusammenarbeit mit Polizeiorganisationen und Forschungseinrichtungen zu fördern.

Insgesamt zeigt sich, dass die Arbeit des Büros 5.4 – Entwicklung und Innovation – von entscheidender Bedeutung für die kriminalpolizeiliche Arbeit ist, um die Herausforderungen der modernen Kriminalität zu meistern und die Sicherheit der Öffentlichkeit zu gewährleisten. Durch die Kombination von wissenschaftlicher Unterstützung, Zusammenarbeit mit nationalen und internationalen Partnern und Präventionsarbeit

kann das Büro 5.4 einen wichtigen Beitrag zur Bekämpfung von Cyberkriminalität und anderen Straftaten leisten.

5.5 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 Exekutivbediensteten 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 Exekutivbediensteten 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 Täterinnen und Täter zu identifizieren und Beweise zu sammeln, die vor Gericht auch verwertbar sind.
Das Cybercrime Competence Center des Bundeskriminalamtes 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 Exekutivbediensteten in den Bundesländern liegen seit 2025 in der Zuständigkeit der Cybercrime Trainingscenter (CCTC) der Landeskriminalämter, wodurch eine noch größere Reichweite gewährleistet werden soll. Das Cybercrime Competence Center des Bundeskriminalamtes bietet unterschiedliche Spezialausbildungen und Expertinnen- und Expertenschulungen (Sachbearbeiterinnen- und Sachbearbeiter-Schulungen) an.
Einem größeren polizeilichen Bereich wird das Thema Cybercrime 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 und in der Folge auch für Richterinnen und Richter entwickelt und durchgeführt, die im Sinne einer zielgerichteten Strafverfolgung speziell auf technische Hintergründe und hiermit einhergehende Ermittlungsmöglichkeiten im Cyber-Bereich fokussierte. Ziel ist es, einem möglichst großen Personenkreis Cybercrime-Grundkompetenzen zu vermitteln. Die Ausbildungen finden jeweils in Form von Webinaren statt, wodurch es möglich ist,

einschlägiges kriminalpolizeiliches Fachwissen bundesweit an Staatsanwältinnen und Staatsanwälte, Bezirksanwältinnen und Bezirksanwälte sowie Richterinnen und Richter weiterzugeben. Die Kooperation mit dem BMJ ist mittlerweile zu einem fixen Bestandteil im Ausbildungsbereich geworden.

12. Internationales Symposium Neue Technologien in Bern, Schweiz
Rund 250 internationale Expertinnen und Experten von Sicherheitsbehörden sowie aus Wissenschaft und Wirtschaft kamen am 5. und 6. November 2025 in Bern zusammen, um über das Thema „Zukunft der Kriminalitätsbekämpfung – technische Innovationen und gesellschaftliche Herausforderungen" zu diskutieren. Bereits zum zwölften Mal veranstalteten das Cybercrime Competence Center (C4) des Bundeskriminalamtes Österreich, die Schweizer Bundespolizei fedpol, das Bayerische Landeskriminalamt und das Landeskriminalamt Baden-Württemberg dieses länderübergreifende Symposium.

Die Komplexität der Polizeiarbeit wächst stetig und spiegelt die vielfältigen Herausforderungen wider, denen die Gesellschaft gegenübersteht. Die Polizei agiert an der Schnittstelle von Technologie, Gesellschaft und Recht. So steigen neben technologischen Anforderungen an eine moderne Polizeiarbeit zugleich auch Anforderungen an Menschen und Organisationen. Ohne den Einsatz moderner technologischer Werkzeuge sind die Problemstellungen nicht mehr zu meistern. Ziel des Symposiums war, neben der Vorstellung laufender Projekte, marktreife Ergebnisse aus Forschung und Entwicklung, aber auch technische Herausforderungen und Bedarfe im polizeilichen Kontext zu präsentieren. Zudem soll eine Möglichkeit geboten werden, aktuelle gesellschaftspolitische Herausforderungen in 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 sie in Diskussionsrunden. Neben dem fachlichen Austausch bot das Symposium auch ein Forum für umfassende länderübergreifende Vernetzung und Kooperation.

5.6 ZASP – Zentrale Anfragestelle für Social Media und Online Service Provider

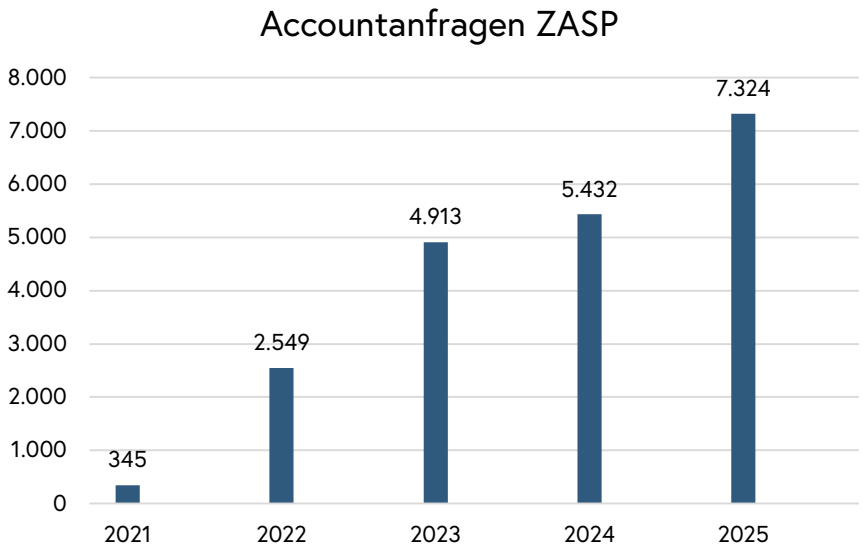

Abbildung 11: Accountanfragen im Jahresverlauf

Bei vielen Ermittlungen sind internationale Anfragen an Social-Media-Plattformen und ausländische Diensteanbieter im Internet erforderlich. Im Jahr 2025 wurden insgesamt 7.324 Accountanfragen gestellt. Zu den Tatbeständen Betrug, Erpressung, Freiheit/Nötigung/gefährliche Drohung, Cybercrime im engeren Sinn und sexuelle Integrität wurden die meisten Accountanfragen gestellt.

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.

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.

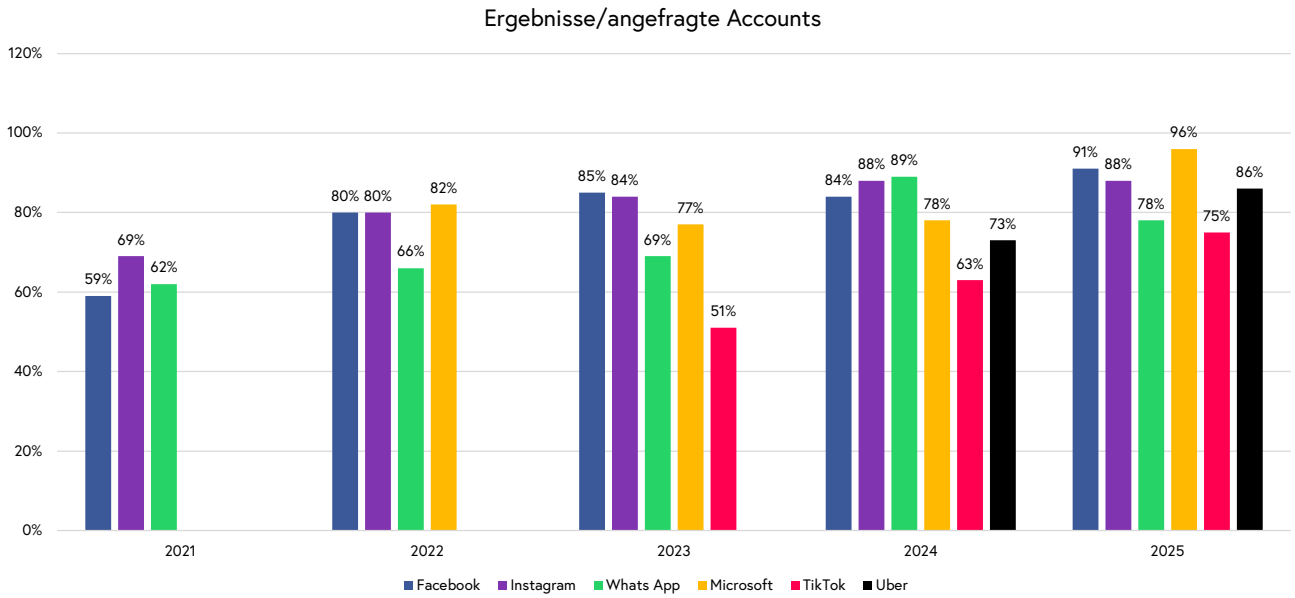

Abbildung 12: ZASP-Erfolgsquote im Jahresvergleich (eingelangte Rückmeldungen in Prozent)

6 Rechtliche Herausforderungen aus Sicht der Kriminalpolizei (Schwerpunkt Strafprozessrechtsänderungsgesetz 2024)

6.1 Rechtliche Neuausrichtung auf Basis des Erkenntnisses des Verfassungsgerichtshofs

Der Verfassungsgerichtshof (VfGH) hat in seinem Erkenntnis vom 14. Dezember 2023 (G 352/2021) festgestellt, dass die Sicherstellung von Mobiltelefonen in Strafverfahren ohne vorhergehende richterliche Bewilligung verfassungswidrig sei. Dies verstoße gegen das Datenschutzgesetz und das Recht auf Privatleben. Grundrechtseingriffe müssen verhältnismäßig sein. In konsequenter Umsetzung des Erkenntnisses trat mit Wirkung zum 1. Jänner 2025 das Strafprozessrechtsänderungsgesetz 2024 in Kraft (StPO-Reform 2024). Neben den inhaltlichen Grundlagen der Gesetzesänderung wird eine Grobbilanz auf Praxistauglichkeit für das erste Jahr der Umsetzung (2025) umrissen (Basis: parlamentarische Materialien):

Inhaltliche Grundlagen StPO-Reform 2024

- Neueinführung der Ermittlungsmaßnahme „Beschlagnahme von Datenträgern und Daten“, die eine vorherige gerichtliche Entscheidung zur Begründung einer Sicherstellung von Datenträgern und Daten zum (Ermittlungs-)Zweck der Auswertung verlangt
- Erhöhung der Begründungspflicht für die Anordnung der Staatsanwaltschaft und die gerichtliche Entscheidung durch Anlehnung an andere bereits bestehende Ermittlungsmaßnahmen
- Möglichkeit der Beschlagnahme auch von Daten, die in anderen (externen) Speicherorten als einem Datenträger gespeichert sind, soweit auf sie von diesem aus zugegriffen werden kann (zum Beispiel Cloud-Computing, Server)
- Einführung einer Nichtigkeitssanktion von Ergebnissen einer Auswertung, sofern die Ermittlungsmaßnahme nicht rechtmäßig angeordnet und bewilligt wurde
- Gliederung der Beschlagnahme von Datenträgern und Daten in mehrere Phasen zwecks erhöhter Transparenz, insbesondere der Beteiligungsmöglichkeiten von Beschuldigten und Opfern bei der Selektion von erheblichen Tatsachen, ebenso

Informationspflichten von Behörden an betroffene Personen (erhöhter Rechtsschutz)

- Transparenz durch strenge Dokumentation der Durchführung der Ermittlungsmaßnahme von der Phase der technischen Aufbereitung von Daten bis zur Phase der inhaltlichen Auswertung von Daten
  - Phase der technischen Aufbereitung von Daten unter Einhaltung forensischer Standards enthält die
    - Entsperrung von Speichermedien (zum Beispiel Datenträger, Cloudspeicher, Server),
    - Sicherung von Daten (allenfalls samt Wiederherstellung gelöschter oder zerstörter Daten) in Form einer Originalsicherung (Rohdaten) des gesamten Datenbestandes sowie die
    - Erstellung einer Arbeitskopie (eine Kopie der Originalsicherung, anhand derer die konkrete forensisch technische Aufbereitung durch die Kriminalpolizei bzw. die Staatsanwaltschaft erst erfolgen kann)
  - Phase der Auswertung soll nur mehr diesen begrenzten Datenbestand umfassen, der als „Ergebnis der Datenaufbereitung" gewonnen wurde. Sowohl Kriminalpolizei als auch Staatsanwaltschaft haben diesen begrenzten Datenbestand sodann im Rahmen der gerichtlichen Bewilligung auf erhebliche Tatsachen zu untersuchen, wobei sie auch Suchparameter zum Zweck der Auswertung festlegen können. Zusätzlich soll ausdrücklich auch Beschuldigten und Opfern das Recht eingeräumt werden, weitere Suchparameter zu beantragen, wodurch auch Opferschutzinteressen Rechnung getragen wird.

6.2 Praktische Erwägungen – „erste Grobbilanz" StPO-Reform 2024

Die StPO-Reform 2024 hat sich im Tätigkeitsbereich des C4 sehr gut etabliert und ist im Großen und Ganzen funktional, mit Ausnahme weniger Problemstellungen in der Praxis:

- Der Gesetzgeber sieht das Auftauchen neuer Tatsachen erst in der Phase der Auswertung (Ermittlung) und nicht schon in der Phase der forensischen Aufbereitung. Faktisch tauchen aber bereits beim forensischen Aufbereiten einer Festplatte Zufallsfunde auf (zum Beispiel bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellungen minderjähriger Personen/pornografische Darstellung Minderjähriger). Um diese Zufallsfunde gerichtstauglich verwerten zu können, müsste eine neue Anordnung bei Gericht erwirkt werden.
- Ebenso, wenn neue Tatsachen zum Fall selbst auftauchen (zum Beispiel: die Täterin bzw. der Täter verwendet eine weitere IP-Adresse), müsste eine neuerliche richterliche Entscheidung herbeigeführt werden und alles beginnt wieder in der Phase der forensischen Auswertung. Im Ergebnis bedeutet dies eine aufwändige Schleife zurück zur Staatsanwaltschaft und wieder nach vorne zu den

ermittelnden Personen (Kriminalpolizei). Damit läuft der Faktor Zeit gegen die Strafverfolgung, was in Wirtschaftsstrafverfahren äußerst nachteilig ist (Vermögen wurde bereits ins Ausland verbracht bzw. verwässert).

- Zu lange Reaktionszeit auf neue Kriminalitätsphänomene einerseits (was machen Tätergruppen generell, welche rechtlichen Schlupflöcher werden ausgenützt) und technische Entwicklungen andererseits. Gesetzgebungsprozesse dauern zu lange, um rasch auf derartige Entwicklungen reagieren zu können.
- Gesetzliche Vorgaben, die nach dem Stand der Technik nicht umsetzbar sind: Einfaches Beispiel ist die Einsichtnahme in komplexe Programme sowie die effektive Löschung von Daten. Ebenso das Thema „allgemein gebräuchliches Dateiformat“: Datenaufbereitungen sind in den wenigsten Fällen einfache PDF-Dateien (Berichte) oder Excel Sheets, die von den ermittelnden Personen an die Staatsanwaltschaft zu übermitteln sind.

6.3 „Carrier Grade NAT“-Problematik

Im Cybercrimereport 2024 wurde über die häufige Nutzung der „Carrier Grade NAT“-Technologie, bei der mehreren Internetnutzerinnen oder -nutzern zeitgleich idente IP-Adressen vom Netz-Provider zugewiesen werden, berichtet. Im Ergebnis bedeutet dies, dass viele Straftaten nicht geklärt und auch die Verfasserinnen und Verfasser von Hasspostings sowie Fake News nicht ausgeforscht werden können, da eine IP keiner einzelnen Person zugeordnet werden kann. Das Problem wurde bis jetzt nicht gelöst und es bestehen nach wie vor, selbst auf europäischer Ebene, sehr große Unterschiede, was die rechtlichen Rahmenbedingungen betrifft.

6.4 Vorratsdatenspeicherung

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 Dauer der Kommunikation sowie IP-Adressen betreffend Internetverbindungen. Solche Daten sind für polizeiliche Ermittlungen im Bereich Cybercrime für die Täterausforschung jedoch essenziell. Trotz des Urteils des Europäischen Gerichtshofs (EuGH) vom 30. April 2024 (Az.: C-470/21), das den Handlungsrahmen für die Mitgliedstaaten der EU zumindest erweitert, gibt es bis dato auf nationaler Ebene keine Gesetzesänderung. Die Europäische Kommission arbeitet jedoch konsequent an einem neuen Vorschlag, der mit den Vorgaben des EuGH vereinbar sein soll. Eine harmonisierte Lösung auf EU-Ebene wäre wünschenswert, um eine effektivere Kriminalitätsbekämpfung zu ermöglichen.

6.5 Pseudoanonyme Transaktionen von virtuellen Währungen

- Kryptowährungen wie Bitcoins, Ethereum, Tether etc. sind unter anderem auch ein beliebtes Mittel für Finanztransaktionen im Zusammenhang mit Geldwäsche und für Käufe illegaler Waren im Internet. Jede und 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 können.
- 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 MiCA-Verordnung (MiCA-VO) und der 3. Geldtransfer-VO (seit 30. Dezember 2024 in Kraft). Durch diese soll die Kryptobranche innerhalb der EU stärker reguliert werden. Die MiCA-VO enthält eine zentrale Legaldefinition des Begriffs „Kryptowerte“ sowie Anforderungen an das öffentliche Angebot und die Zulassung zum Handel mit Kryptowerten. Die 3. Geldtransfer-VO dehnt die bereits bestehenden Geldwäschepräventionspflichten für Zahlungsdienstleister auf Kryptodienstleister aus. Diese sind im Zusammenhang mit Kryptotransfers verpflichtet, konkrete Angaben zur Zahlerin oder zum Zahler und zur Zahlungsempfängerin oder zum Zahlungsempfänger einzuholen, wodurch die Rückverfolgbarkeit des Zahlungsflusses von Kryptowerten und somit auch die Strafverfolgung erleichtert wird.
- Abschließend kann festgehalten werden, dass die Rückverfolgung und das Sicherstellen bzw. die Beschlagnahme von Kryptowerten ressourcenintensiv sind und ein schnelles und orchestriertes Zusammenwirken von Behörden und Diensteanbietern im In- und Ausland erfordern.

6.6 Befugnis zur Serverüberwachung

Derzeit ist es nicht möglich, die Kommunikation eines Servers zu überwachen. Dies ist dahingehend nachteilig, weil ein Server ein leistungsfähiges Computersystem (im Dauerbetrieb) ist, das dazu dient, Dienste, Ressourcen oder Daten für andere Computer (Clients) in einem Netzwerk bereitzustellen. So zum Beispiel die Verwaltung von Datenbanken, die Bereitstellung von E-Mails, die Speicherung von Dateien oder die Ausführung von Anwendungen. Server kommunizieren einerseits mit anderen Servern und andererseits mit Endgeräten (für die sie übergeordnete Tätigkeiten ausführen). Derzeit ist es rechtlich für die Kriminalpolizei nicht möglich, diese (automatische, zwischen zwei Rechnern bestehende) Kommunikation zu überwachen. Laut der eingeschränkten gesetzlichen Begrifflichkeit muss für die Überwachung eine natürliche Person (Mensch) dazwischengeschaltet sein. Eine reine Kommunikation zwischen Maschinen ist rechtlich nicht für eine Überwachung gedeckt. Dieser Umstand ist in Österreich einzigartig und müsste rechtlich dringend bereinigt werden, zumal dies in anderen Rechtsordnungen so nicht besteht.

7 Kriminalprävention im digitalen Zeitalter

7.1 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.
Cyberprävention 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 Akteuren 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 -nutzer oftmals schwieriger zu erkennen sind. Bei Vorträgen und Beratungen durch Präventionsbedienstete wird die Bevölkerung sensibilisiert, wie sie sich vor diesen Gefahren schützen kann. Ein Schwerpunkt wurde auf maßgeschneiderte Vorträge für Seniorinnen und Senioren gelegt, um über die Risiken und Schutzmaßnahmen im Internet aufzuklären. Diese Zielgruppe ist besonders anfällig für Online-Betrügereien und verschiedene Telefonbetrugsformen wie „Falscher Polizist“, „Enkel- oder Neffentrick“, „Angehörige in Not“ oder „Technische-Service-Dienste“ und benötigt maßgeschneiderte Informationen und Präventionstipps.
Die Themen der Cyberprävention sind vielfältig und betreffen verschiedene Zielgruppen. Dementsprechend werden die Inhalte den aktuellen Kriminalitätsfeldern angepasst, aufgearbeitet und 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. Besonders eingegangen wird auf neue Entwicklungen, die durch technologische Innovationen und gesellschaftliche Veränderungen entstehen.
- **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 von Zwei-Faktor-Authentifizierung, ein achtsamer Umgang mit verdächtigen E-Mails sowie regelmäßige Software-Updates.

Diese Schulungen tragen dazu bei, das Bewusstsein für Cyberrisiken 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 über 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 Stärkung 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 Cyberrisiken zu erhöhen und globale Präventionsstrategien zu fördern.

Im Rahmen der 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, und
- **eine Webinar-Reihe 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 und den Austausch von Informationen zu ermöglichen. Ziel der CRI ist:

- **der Erfahrungsaustausch** und Austausch **bewährter Praktiken**,
- **Strategien** und Maßnahmen zu entwickeln, die sowohl die Prävention als auch die Reaktion auf Ransomware-Angriffe verbessern und
- **Informationsaustausch** zwischen Ransomware-Opfern, Strafverfolgungsbehörden und Cyber-Notfallteams (CERTs) fördern, 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 internationaler Zusammenarbeit.

Medienkampagnen
Im Rahmen ihrer umfassenden Maßnahmen zur Kriminalprävention setzt die Polizei regelmäßig gezielte Informations- und Sensibilisierungskampagnen zu aktuellen Betrugsphänomenen um.

Ein besonderer Schwerpunkt liegt dabei auf dem Thema Anlagenbetrug, der insbesondere durch digitale Kommunikationskanäle stark zugenommen hat und häufig vulnerable Personengruppen betrifft.

Die Kampagnen werden in Kooperation mit anerkannten Partnerinstitutionen wie der Finanzmarktaufsicht (FMA) und dem Verein für Konsumenteninformation (VKI) umgesetzt. Ziel ist, durch gebündelte Expertise eine möglichst breite und nachhaltige Aufklärung der Bevölkerung zu gewährleisten. Die Informationsmaßnahmen umfassen unter anderem zielgruppenspezifische Radiobeiträge – insbesondere für Seniorinnen und Senioren –, redaktionelle Beiträge in Printmedien, umfassende Online-Informationen sowie Social-Media-Kampagnen. Ergänzend dazu werden gemeinsame Pressekonferenzen mit FMA und VKI abgehalten, um Medienvertreterinnen und -vertreter aktuell zu informieren und die öffentliche Aufmerksamkeit auf bestehende Risiken sowie konkrete Präventionsmaßnahmen zu lenken.

Darüber hinaus wurde die Kampagne „#10TageGegenPhishing“ initiiert, die in Zusammenarbeit mit zahlreichen Partnerorganisationen – insbesondere der Payment Services Austria (PSA) und „Watchlist Internet“ – umgesetzt wird. Ziel dieser Initiative ist, die Bevölkerung über aktuelle Phishing-Methoden aufzuklären, konkrete Schutzmaßnahmen zu vermitteln und die Sensibilität im Umgang mit verdächtigen Nachrichten, E-Mails und Webseiten nachhaltig zu erhöhen.

Gamification
Im Rahmen eines modernen Präventionsansatzes setzt das Bundeskriminalamt verstärkt auf Gamification, um sicherheitsrelevante Inhalte zielgruppengerecht und nachhaltig zu vermitteln. Dabei werden aktuelle kriminalitätsrelevante Themen systematisch analysiert und aufbereitet. Auf Grundlage dieser Analysen entstehen neue interaktive Lern- und Spielformate, die regelmäßig weiterentwickelt und auf der Website des Bundeskriminalamtes veröffentlicht werden.
Ziel dieses Ansatzes ist, Bürgerinnen und Bürger praxisnah für Gefahren im Alltag zu sensibilisieren und ihre Handlungskompetenz zu stärken. Die interaktiven Kriminalpräventions-Quizze ermöglichen es, auf spielerische Weise relevantes Wissen zu erwerben und anhand realitätsnaher Fallbeispiele zu vertiefen. Nutzerinnen und Nutzer lernen, Risiken frühzeitig zu erkennen, angemessen zu reagieren und präventive Maßnahmen wirksam umzusetzen.
Im Rahmen dieses Gamification-Ansatzes wurden bereits interaktive Quizformate, unter anderem als Kahoot-Quiz, entwickelt und implementiert. Diese sind auf der Homepage

des Bundeskriminalamtes im Bereich „Prävention“ abrufbar. Durch die Kombination aus fachlich fundierten Inhalten, anschaulichen Praxisbeispielen und spielerischen Elementen wird ein niedrigschwelliger Zugang zu sicherheitsrelevanten Themen geschaffen.
Mit diesem innovativen Format trägt das Bundeskriminalamt dazu bei, Präventionsarbeit zeitgemäß, interaktiv und wirkungsvoll zu gestalten. Bürgerinnen und Bürger sind eingeladen, ihr Wissen zu testen, ihre Kompetenzen auszubauen und sich aktiv mit Fragen der persönlichen Sicherheit auseinanderzusetzen – für mehr Schutz und Sicherheit in allen Lebensbereichen.

Geplante Präventionskampagne „Account Sicherheit“

Für das Jahr 2026 plant Österreich die nationale Präventionskampagne „Account Sicherheit“. Diese Kampagne zielt darauf ab, die Bürgerinnen und Bürger über die Bedeutung von 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

Neben der Weiterentwicklung digitaler Präventionsangebote wurde auch die personelle Kompetenz gezielt ausgebaut: Insgesamt 50 neue Kolleginnen und Kollegen wurden zu Präventionsbediensteten ausgebildet. Damit stärkt das Bundeskriminalamt nachhaltig die Beratungs- und Informationskompetenz der Polizei sowohl im analogen als auch im digitalen Raum.
Zusätzlich nahmen sämtliche Präventionsbedienstete an Online-Schulungen in zentralen Zukunfts- und Gefahrenfeldern teil. Die Fortbildungsmaßnahmen umfassten insbesondere die Themen künstliche Intelligenz (KI), Anlagenbetrug, Account-Sicherheit sowie Radikalisierung im Netz. Diese kontinuierliche Qualifizierung stellt sicher, dass Präventionsfachkräfte aktuelle Entwicklungen frühzeitig erkennen und kompetent darauf reagieren können.
Ein besonderer Schwerpunkt liegt auf der Ausbildung im Bereich künstliche Intelligenz. KI stellt sowohl eine bedeutende Chance als auch ein potenzielles Risiko für die Cybersicherheit dar. Aus- und Weiterbildungen für Präventionsbedienstete und Polizistinnen und Polizisten sind daher unerlässlich, um einen sicheren und verantwortungsvollen Umgang mit KI-Technologien zu gewährleisten und mögliche Missbrauchsgefahren frühzeitig zu identifizieren.
Die kontinuierliche Weiterqualifizierung wird auch im Jahr 2026 fortgeführt. Durch die Kombination aus innovativen Präventionsformaten, fundierter Analyse aktueller Kriminalitätsphänomene und gezielter Personalentwicklung leistet das Bundeskriminal-

amt einen wesentlichen Beitrag zur nachhaltigen Stärkung der Sicherheitskompetenz in der Bevölkerung und innerhalb der Organisation.

Kriminalprävention mit der Zielgruppe Jugendliche – „UNDER18“
In Österreich bietet das Bundeskriminalamt, Büro 1.6 Kriminalprävention und Opferhilfe, mit dem Gewaltpräventionsprogramm „UNDER18“ österreichweit ein universelles, umfassendes, primärpräventives und entwicklungsorientiertes Jugend-Kriminalpräventionsprogramm an, das hauptsächlich in Schulen umgesetzt wird.

Ein wichtiger Teilbereich der Kriminalprävention mit Jugendlichen ist das Gewaltpräventionsprogramm „Click & Check“. Es befasst sich mit der Förderung eines verantwortungsvollen Umgangs mit digitalen Medien. Besonderes Augenmerk wird dabei auf die Erarbeitung von Handlungsstrategien sowie die Förderung der Rechtssicherheit beim täglichen Internetverkehr, insbesondere im Social-Media-Bereich, gelegt.

Im Jahr 2025 wurden im Rahmen von „UNDER18“ 8.499 Workshops an Schulen durchgeführt und dabei 198.000 Schülerinnen und Schüler sowie Lehrpersonal und Erziehungsberechtigte erreicht.

Ein wichtiger Bestandteil der Präventionsarbeit mit Jugendlichen ist die Zusammenarbeit mit saferinternet.at. Präventionsexpertinnen und -experten des Bundeskriminalamtes sind Mitglied im saferinternet.at-Beirat und nehmen regelmäßig an Vernetzungstreffen und Arbeitsgruppensitzungen mit Vertreterinnen und Vertretern anderer Ministerien und NGOs teil. Damit sind eine stetige Weiterentwicklung der Präventionsprogramme und die rasche Reaktion auf auftretende Phänomene gewährleistet.

Fazit
Durch die enge Zusammenarbeit der Kriminalprävention und „Watchlist Internet“, die Teilnahme an internationalen Kampagnen und durch nationale Präventionsprojekte 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/nicht alles gratis.
- Halten Sie Ihren Virenschutz/Firewall stets aktuell.
- Vorsicht, wenn jemand Sie unter Druck setzen will.
- Verschicken Sie niemals Ausweiskopien.

7.2 Cybercrime-Anzeigenerstattung

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

Um sich hierfür optimal vorzubereiten, helfen Ihnen folgende Tipps:

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

Stellen Sie bitte fallrelevante(s) Beweismittel/Datenmaterial wie E-Mails, Chat-Verläufe, Zahlungsbelege, Screenshots, digitale Fotos oder Videos u. v. m. 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-E-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 dazu am besten selbst, welche der für die Tathandlung relevanten Daten beim jeweiligen Account-Anbieter beziehungsweise Online Service Provider gespeichert werden und für Sie zugänglich sind oder deren Bekanntgabe über diesen angefordert werden kann.

Wenn es sich um komplexere Tathandlungen handelt, **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 Beamtinnen und Beamten nach Absprache mit diesen **in geeigneter Form** zur Verfügung (beispielsweise über https://cryptshare.bmi.gv.at). Die Bereitstellung der Daten 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

8 Strategie und Ausblick

Die Bekämpfung der Cyberkriminalität ist ein wichtiger Schwerpunkt für die Strafverfolgungsbehörden in Österreich. Um diesem Bereich gerecht zu werden, müssen die Ausbildung und das Know-how aller involvierten Kolleginnen und Kollegen kontinuierlich verbessert werden. Die Ausbildung im Cyber-Bereich muss weiter forciert werden, um sicherzustellen, dass alle Strafverfolgungsbehörden über das notwendige Know-how verfügen, um Cyberkriminalität effektiv zu bekämpfen. Dies umfasst nicht nur die Schulung von Fachpersonal, sondern auch die kontinuierliche Weiterbildung und Aktualisierung von Kenntnissen und Fähigkeiten, um den sich ständig ändernden Bedrohungen und Herausforderungen im Cyber-Bereich gerecht zu werden.

Im Rahmen der Kriminaldienstreform wurden organisatorische Anpassungen auf Landes- und regionaler Ebene vorgenommen, um die Bekämpfung der Cyberkriminalität zu verbessern. Mehrere Cybercrime-Trainingscenter wurden eingerichtet, um die Ausbildung und das Know-how der Strafverfolgungsbehörden zu verbessern. Diese Trainingscenter sollen als zentrale Anlaufstellen für die Aus- und Weiterbildung von Fachpersonal dienen und sicherstellen, dass alle Strafverfolgungsbehörden über die notwendigen Ressourcen und Kenntnisse verfügen.

Die Stärkung der nationalen und internationalen Zusammenarbeit zwischen staatlichen Behörden, Organisationen und Unternehmen ist ein wichtiger Schwerpunkt. Durch die enge Zusammenarbeit mit internationalen Partnern und die Teilnahme an globalen Initiativen kann Österreich von den Erfahrungen und Kenntnissen anderer Länder profitieren und gleichzeitig seine eigenen Erfahrungen und Kenntnisse teilen. Dies ermöglicht es, die Bekämpfung der Cyberkriminalität auf internationaler Ebene zu koordinieren und effektiver zu gestalten.

Die Einsatzmöglichkeiten künstlicher Intelligenz in der Strafverfolgung müssen weiter ausgelotet werden, unter Berücksichtigung der rechtlichen Vorgaben der EU. Die künstliche Intelligenz bietet enorme Möglichkeiten, um die Effizienz und Effektivität der Strafverfolgung zu verbessern, jedoch müssen auch die rechtlichen und ethischen Implikationen berücksichtigt werden. Die Mitarbeit bei der Erarbeitung von rechtlichen Rahmenbedingungen für den Einsatz von künstlicher Intelligenz in der Strafverfolgung ist geplant, um sicherzustellen, dass die Einsatzmöglichkeiten auf eine rechtlich und ethisch vertretbare Weise genutzt werden.

Die kontinuierliche Weiterentwicklung von Fachexpertise ist vorgesehen, um sicherzustellen, dass die Strafverfolgungsbehörden über die notwendigen Kenntnisse und Fähigkeiten verfügen, um die Herausforderungen der Cyberkriminalität zu meistern.

Die fortschreitende Vernetzung erfordert die Entwicklung neuer Ermittlungsmethoden und Ermittlungsansätze, um die Sicherheit und Integrität von Daten und Systemen zu gewährleisten.

Die Novellierung der Strafprozessordnung in Österreich bezüglich der Beschlagnahme von Datenträgern und Daten stellt die Polizei 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. Die notwendige Dokumentation in der Phase der Aufbereitung von Daten wurde bereits in Absprache mit der Justiz adaptiert.

Das Ziel ist, die Kriminalitätsbekämpfung weiterzuentwickeln und den Dienst zu modernisieren, um die Herausforderungen der Cyberkriminalität effektiv zu meistern. Durch die kontinuierliche Weiterentwicklung von Fachexpertise, die Stärkung der nationalen und internationalen Zusammenarbeit sowie die Einsatzmöglichkeiten künstlicher Intelligenz kann Österreich seine Position als Vorreiter in der Bekämpfung der Cyberkriminalität weiter stärken und die Sicherheit und Integrität von Daten und Systemen gewährleisten.

9 Strategy and Outlook (English)

Austrian law enforcement agencies consider the fight against cybercrime a high priority. In order to meet the challenges in this area, it is necessary to continuously improve the training and know-how of all involved personnel. Further promoting training in the field of cybercrime is central to ensuring that all law enforcement agencies have the required knowledge to effectively combat cybercrime. This not only concerns training for specialised personnel but also requires the continuous expansion and updating of knowledge and skills to effectively counter the constantly evolving threats and challenges in the cyberspace.

Organisational structures on provincial and regional levels were streamlined in the course of the criminal policing reform to improve the fight against cybercrime. Several cybercrime training centres were established to refine the training and know-how at law enforcement agencies. These training centres serve as the central contact points regarding the training of specialised personnel. They ensure that all law enforcement agencies have the necessary resources and knowledge at their disposal to effectively fight cybercrime.

Another important factor is strengthening national and international cooperation between state authorities, organisations and enterprises. In the framework of close cooperation with international partners and participation in global initiatives, Austria not only benefits from the experiences and expertise provided by other countries, but also shares its own. This makes it possible to coordinate the fight against cybercrime on an international level and render it more effective.

The potential use of AI in law enforcement requires further exploration, especially in terms of compliance with EU legislation. AI offers numerous opportunities to enhance the effectiveness and efficiency of law enforcement; however, legal and ethical implications must be taken into consideration. There are plans to actively participate in drawing up the legal framework for the use of AI in law enforcement. This shall guarantee that AI is used in a legal and ethical manner.

The continuous expansion of expertise is planned to make sure that law enforcement agencies have the necessary skills and knowledge to meet the challenges in the field of cybercrime. Ever-growing interconnectedness requires new developments in investigative methods and approaches to provide for the security and integrity of data and systems.

The amendment of the Austrian Code of Criminal Procedure with regard to the seizure of data carriers and data presents new challenges to the police and necessitates changes in digital evidence preservation. The new provisions clearly differentiate between the phases of seizure, technical preparation and analysis of data. The documentation necessary in the phase of data preparation has already been adapted in consultation with judicial authorities.

The goal is to continue developing the fight against crime and to modernise police work to effectively meet the challenges posed by cybercrime. Austria can further strengthen its position as a leading force in the fight against cybercrime and guarantee the security and integrity of data and systems by continuously developing expert knowledge, strengthening national and international cooperation and exploring the possible use of AI.

10 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 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 Täterinnen und Täter zu veranlassen. Es handelt sich hier um gezielte Angriffe gegen bestimmte Unternehmen, da die Täterinnen und Täter 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 Täterinnen und Täter bei den Betrugsanrufen ihre Telefonnummer. Bei Anrufen eine falsche Nummer anzuzeigen, ist relativ leicht und mit wenig technischem Aufwand verbunden. Dazu können existierende – auch aus dem Ausland stammende – Telefonnummern verwendet werden, obwohl die Inhaberinnen und Inhaber der Nummer für den Anruf gar nicht verantwortlich sind. Auch Fantasienummern, also Telefonnummern, 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 Verschlüsselungstrojaner, aber auch um spezielle Dienstleistungen zur Geldwäsche, für Übersetzungen oder für den vermeintlichen Opfer-Support. Die Täterinnen und Täter benötigen damit kein tiefgreifendes technisches Wissen zur Straftatbegehung, sondern kaufen sich das fehlende Wissen 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, 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 im Internet potenzielle Anlegerinnen und Anleger für vermeintlich lukrative Investitionsgeschäfte an und verleiten sie zu Geldzahlungen. Die Kontaktaufnahme geschieht vornehmlich über Internet-Werbeanzeigen, soziale Netzwerke, Anrufe aus

eigens geschaffenen Call-Centern oder Massenmails. Durch die professionelle Vorgehensweise ist es besonders wichtig, zu wissen, wie man sich am besten vor den Täterinnen und Tätern 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, dem Clearweb, an. Dort liegen alle Daten unverschlüsselt vor und können durchsucht sowie meist 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 Täterinnen und Täter 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 Centre (EC3)

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

1. Bekämpfung von Cybercrime, begangen durch organisierte Gruppierungen, die beispielsweise durch Online-Betrug große Geldmengen erbeuten.
2. Bekämpfung von Formen von Cybercrime, die die Opfer massiv schädigen, wie sexueller Missbrauch von Kindern.
3. Bekämpfung von Cybercrime (inklusive Cyberattacken), die 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 aus dem 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 als 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 Täterin bzw. der Täter stellt meist den ersten Kontakt per E-Mail oder über soziale Medienplattformen her und versucht, eine Vertrauensbasis durch zum Beispiel die Zusagen von persönlichen Treffen zu schaffen. In Folge der elektronischen Kommunikation versucht die Täterin oder der Täter, 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 Täterinnen und Täter schrecken dabei auch nicht davor zurück, die Identität und den Internetauftritt von realen Personen dafür zu missbrauchen.

Malspam

Bei Malspam bzw. „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 Dropper, Downloader etc., jeweils versteckt als JavaScript, eingebettet in komprimierten Dateien oder anderen Datenformaten). In einer anderen Variante beinhalten diese E-Mails „nur" einen Link, der aktiv von der Empfängerin oder dem 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 Endkundinnen- und 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 kleinem 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. RATs werden üblicherweise im Hintergrund durch ein Programm heruntergeladen, das Anwenderinnen und Anwender aufgerufen haben, bspw. ein Spiel oder ein E-Mail-Anhang. Sobald das Zielsystem kompromittiert ist, macht sich der Eindringling diesen Umstand zunutze, um RATs 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-)Vertrages 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 Täterinnen und Täter 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 Anrufe 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 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 gerade sie brauche, um ihr/ihm 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 Hackerinnen und 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 Wissen von Anwenderinnen und Anwendern eine andere, meist schädliche Funktion erfüllt.

Uniform Resource Locator (URL)

Eine URL identifiziert und lokalisiert Ressourcen im Internet wie 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 verbreiten und unterschiedliches Schadpotenzial in sich tragen. 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 Klartexts 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 Eigentümer, 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 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