Bundesministerium
Inneres

Bundeskriminalamt

Cybercrime Report 2023

Lagebericht über die Entwicklung von Cybercrime

Cybercrime Report 2023

Lagebericht über die Entwicklung von Cybercrime

Wien, im April 2024

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres, Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
+43 1 24836 985025 (SPOC)
bundeskriminalamt.at
Layout: BMI-I/C/10/a - Strategische Kommunikation und Kreation
Druck: Digitalprintcenter des Bundesministeriums für Inneres
Wien, 2024

Vorwort

Die Cyberkriminalität stellt seit Jahren den am stärksten wachsenden Bereich in der polizeilichen Anzeigenstatistik dar. Sie ist eine der größten Herausforderungen für die Sicherheit Österreichs und kann jede und jeden treffen – unabhängig von Alter, Bildung oder Vorwissen. Cybercrime wird zu einer immer größeren Gefahr für den funktionierenden Staat, für Betriebe, Bürgerinnen und Bürger. Als Gesellschaft stehen wir vor der Herausforderung, unsere Daten und Infrastrukturen zu schützen, um letztlich unsere Sicherheit in der digitalen Welt zu garantieren.

Im Rahmen der Kriminaldienstreform wird daher, ausgehend vom Bundesministerium für Inneres, in diesem Bereich technisch, organisatorisch sowie personell aufgerüstet. Initiativen wie die Etablierung von Cybercrime-Trainingscenters oder der Ausbau von Ausbildungskooperationen, beispielsweise mit der Cyber-HAK Tamsweg, sind wichtige Maßnahmen im Kampf gegen international agierende Cybercrime-Gruppierungen. Weitere Schwerpunkte liegen auf der Verstärkung der internationalen Zusammenarbeit mit anderen Strafverfolgungsbehörden und weiteren Investitionen in das Personal. Mittels Sondervertragslösungen werden IT-Spezialistinnen und IT-Spezialisten von außen angeworben, um das fachliche Know-how stetig weiterzuentwickeln und im Kampf gegen Cyberkriminelle wettbewerbsfähig zu bleiben.

Im Endausbau wird die größte Polizeireform der vergangenen beiden Jahrzehnte rund 700 neue Arbeitsplätze in den kommenden Jahren, 300 davon zur weiteren Stärkung der Bereiche Cybercrime und organisierte Kriminalität, umfassen. Im Hinblick auf den wachsenden personellen und technischen Bedarf im Bereich der Cybercrime-Bekämpfung ist ebenso eine organisatorische Änderung und Aufwertung des Cybercrime Competence Centers (C4) zu einer eigenen Abteilung im Bundeskriminalamt vorgesehen, um auch allen zukünftigen Herausforderungen und internationalen Standards weiterhin gerecht werden zu können.

Die Polizei wird im Jahr 2024 weiter ihren Fokus auf das Gebiet der Cyberkriminalität richten. Durch stete Weiterentwicklung und Fortbildung in diesem essenziellen Bereich ist es unser Bestreben, den Kriminellen noch effizienter entgegenzutreten. Der Bevölkerung werden wir weiter durch Information und Prävention die Möglichkeit bieten, sich vor der Kriminalität im digitalen Raum bestmöglich zu schützen.

Ihr
Bundesminister für Inneres,
Mag. Gerhard Karner

Ihr
Generaldirektor für die
öffentliche Sicherheit,
Mag. Dr. Franz Ruf, MA

Ihr
Direktor des Bundeskriminalamtes,
Mag. Andreas Holzer, MA

Inhalt

1 Einleitung

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

Die Ergebnisse aus den Analysen basieren auf Informationen, die in der fachlichen Zentralstelle des Bundeskriminalamts, dem Cybercrime Competence Center (C4), zusammenlaufen. Dabei handelt es sich um gesammelte Meldungen, Anzeigen, Statistiken aus internationalen Kooperationen, Informationsaustausch mit Mitgliedsstaaten, Ausbildungen, Positionspapiere sowie Studien von Dritten. Die Bestandsaufnahme der quantitativen Daten und qualitativen Inhaltsanalysen fand zu Beginn des Erscheinungsjahres statt, da auf die Verfügbarkeit der Daten von Jänner bis Dezember 2023 in der Polizeilichen Kriminalstatistik (PKS) Rücksicht genommen werden muss. Diese gibt, trotz eines zu verbessernden Anzeigeverhaltens mit vermuteten hohen Dunkelziffern, die strategischen Leitlinien der exekutiven Maßnahmen vor und dient der stetigen Weiterentwicklung beim Know-how-Aufbau und in der Kriminalitätsbekämpfung.

Trotz des erneuten Anstiegs von Cybercrime-Delikten und einer damit einhergehenden abnehmenden Aufklärungsquote konnten im Jahresvergleich bei absoluter Betrachtung mehr Straftaten aufgeklärt werden.

Internetkriminalität	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
Jahr 2014	8 966	3 660	40,8 %
Jahr 2015	10 010	4 157	41,5 %
Jahr 2016	13 103	5 072	38,7 %
Jahr 2017	16 804	6 470	38,5 %
Jahr 2018	19 627	7 332	37,4 %
Jahr 2019	28 434	10 187	35,8 %
Jahr 2020	35 915	12 012	33,4 %
Jahr 2021	46 179	17 020	36,9 %
Jahr 2022	60 195	20 378	33,9 %
Jahr 2023	65 864	20 818	31,6 %

Tabelle 1:
Zehn-Jahresvergleich Internetkriminalität/ Österreich 2014 - 2023 (Jänner - Dezember)

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

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

2 Entwicklungen, Trends und Beispiele

In der Meldestelle des Cybercrime Competence Centers wurden im Laufe des vergangenen Jahres vermehrt Angriffe auf Computersysteme oder Netzwerke mit Hilfe von Schadsoftware registriert. Ebenso kam es zu zahlreichen Erpressungsversuchen, sowohl bei Unternehmen als auch bei Privatpersonen. Genaue Auswertungen und Analysen zur PKS 2023 finden sich in Kapitel 3 wieder.

Auch im Jahr 2023 wurden die Betrugshandlungen im Internet fortgesetzt. Insgesamt wird über die vergangenen Jahre ein sehr starker Anstieg bei Anzeigen im Bereich von Internetbetrug über das Tatmedium Internet verzeichnet. Aufgrund zunehmender Arbeitsteilung und Vernetzung der Tätergruppen, vor allem im Ransomware-Bereich, wird eine erfolgreiche Strafverfolgung erschwert.

2.1 Internetbetrug

Die überwiegende Mehrheit der Betrugsfälle wird digital initiiert, wobei die 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 Deliktformen des Internetbetrugs haben sich auch im Jahr 2023 weiter diversifiziert und stellen eine anhaltende Herausforderung für die österreichische Exekutive dar. Dieses breit gefächerte Spektrum umfasst unter anderem betrügerische Anrufe, falsche Gewinnversprechen, betrügerische Investitionsangebote sowie Love Scams, Phishing-Attacken und betrügerische Aktivitäten im Onlinehandel. Neben einzelnen 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.

In der PKS 2023 wurde eine deutliche Zunahme der gemeldeten Fälle von Internetbetrug auf 34.069 Delikte verzeichnet, was einem Anstieg von 23,3 Prozent gegenüber dem Vorjahr entspricht. Auffällig ist jedoch der Rückgang der Aufklärungsquote um 4,8 Prozentpunkte, was die fortlaufende Herausforderung in der Bekämpfung solcher Verbrechen unterstreicht. Diese Entwicklung ist vor allem auf die zunehmend raffinierten Verschleierungsmethoden im Internet und die Professionalisierung der Tätergruppen zurückzuführen.

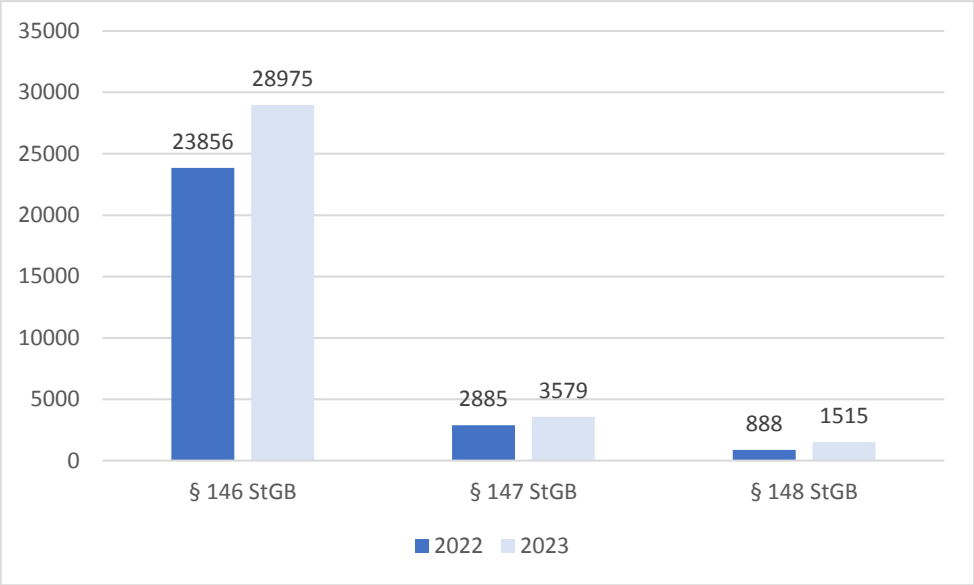

Abbildung 1: Jahresvergleich Internetbetrug nach Paragraphen des StGB (Anzahl der Anzeigen)

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. Ein wichtiger Meilenstein war die Einrichtung eines datenbankgestützten Lagebildes Betrug im Bundeskriminalamt, das aktuelle Trends und neue Betrugsmethoden schnell erfasst und definiert. Die daraus resultierenden Erkenntnisse trugen bereits zu ersten Erfolgen bei der Bekämpfung des Internetbetrugs bei.

Ein häufiges Phänomen ist der sogenannte „Falsche Polizist-Betrug“, der im Jahr 2023 einen Schaden von knapp 20 Millionen Euro verursachte. Diese Betrugsform richtet sich insbesondere gegen ältere Menschen und setzt auf psychischen Druck und fiktive Szenarien, um finanzielle Vorleistungen zu erzwingen. Zur Bekämpfung dieses Phänomens wurde ein Präventionsmodell entwickelt, das in Zusammenarbeit mit der Wirtschaftskammer Österreich, mit Banken und dem Seniorenrat Österreichs im Rahmen einer „GEMEINSAM.SICHER“-Aktion erfolgreich implementiert wurde.

Das Bundeskriminalamt verfolgt weiterhin innovative Ansätze, um auf dynamische Veränderungen und auf die damit verbundenen Herausforderungen reagieren zu können. In diesem Zusammenhang konnte 2023 durch intensive nationale und internationale Zusammenarbeit ein gezielter Schlag gegen die organisierte Kriminalität und vor allem gegen den Trickbetrug „Falscher Polizist“ gesetzt werden und ein internationaler Ermittlungserfolg generiert werden.

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 wie Verschlüsselungstrojaner, aber auch um spezielle Dienstleistungen zur Geldwäsche, für Übersetzungen oder für den vermeintlichen „Opfer-Support“. Auch die Nutzung von Bot-Netzwerken, die DDoS-Angriffen oder zum Versand von Spam-E-Mails dienen, kann vermehrt wahrgenommen werden. Ebenso wurde ein Anstieg beim Inverkehrbringen von Falschgeld, Kinderpornographie, Kreditkartendaten und gefälschten Urkunden registriert.

Durch die im Darknet angebotenen Dienste steigen vor allem Massenerpressungsmails und gezielte Erpressungen durch Ransomware mit Bitcoin-Forderungen an. 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 kaufen zu können. Mit einem Ransomware as a Service Modell (RaaS) lassen sich nach wie vor beträchtliche Gewinne erzielen.

2.3 Blockchain und Kryptowährungen

Kryptowährungen, insbesondere der Bitcoin, existieren mittlerweile seit über zehn Jahren. Anfangs noch von der breiten Masse der Bevölkerung als Spielerei abgetan, bestimmen sie heute zu einem bedeutenden Teil den polizeilichen Alltag. Egal ob Raub, Erpressung oder Betrug, in vielen Deliktsbereichen ist es bereits üblich geworden, dass Kryptowährungen von der Täterschaft genutzt werden. Eine Vielzahl von Polizistinnen und Polizisten in den Polizeiinspektionen, den Landeskriminalämtern und den Fachbereichen im Bundeskriminalamt sind täglich damit konfrontiert. Die Ermittlungen gestalten sich aufgrund der enormen Anzahl von Blockchains sowie ständigen Weiterentwicklungen als laufende Herausforderung, bei der es wichtig ist, den aktuellen Stand der Entwicklungen mitzuverfolgen. Da Kryptowährungen international genutzt werden, ist ein Austausch von Informationen und Erkenntnissen mit internationalen Polizeieinheiten und Organisationen wie Europol und Interpol essenziell.

Kryptowährungen beziehungsweise Blockchains sind ein sich stetig verändernder und wachsender Bereich. Fast täglich werden neue Währungen geschaffen, mit einer Vielzahl an Eigenschaften. Von hoher Anonymität bis zu niedrigen Transaktionsgebühren steht den Entwicklerinnen und Entwicklern und Nutzerinnen und Nutzern alles offen. Ein stetes Weiterbilden in diesem Bereich ist daher für die ermittelnden Polizistinnen und Polizisten von großer Bedeutung.

Im Laufe des Jahres 2023 sind viele neue Kryptowährungen hinzugekommen, sodass bereits über zwei Millionen verschiedene Kryptowährungen weltweit gelistet sind und

somit auch erworben werden können. Der Hype um die sogenannten „Non-Fungible Token“ (NFT), hierbei handelt es sich um digitale, einzigartige und geschützte Objekte, die nicht ersetzt werden können, hat sich im Laufe des Jahres gelegt. Der Börsengang des Bitcoins als ETF (engl. für „Exchange Traded Fund”, börsengehandelter Indexfond) und das bereits stattgefundene „Halving“ im Jahr 2024 wird voraussichtlich die Bekanntheit und den Preis von Kryptowährungen weiter nach oben treiben. Damit verbunden kann auch mit einem Anstieg der illegalen Nutzung gerechnet werden. Mit dem Bitcoin-Halving und dem genau festgelegten Gesamtangebot sollen die Anzahl neuer Coins, die im Bitcoin-Netzwerk generiert werden, verringert werden. Der Gesamtbestand an Bitcoin ist auf 21 Millionen Bitcoins festgelegt.

Im gesamten Jahr 2023 wurde auch bereits ein Anstieg der Fälle mit Kryptowährungs-Bezug bei polizeilichen Anzeigen festgestellt. Dies dürfte auch damit im Zusammenhang stehen, dass der Bevölkerung bewusst geworden ist, dass Ermittlungen in diesem Bereich möglich sind und auch gute Erfolge erzielt werden können.

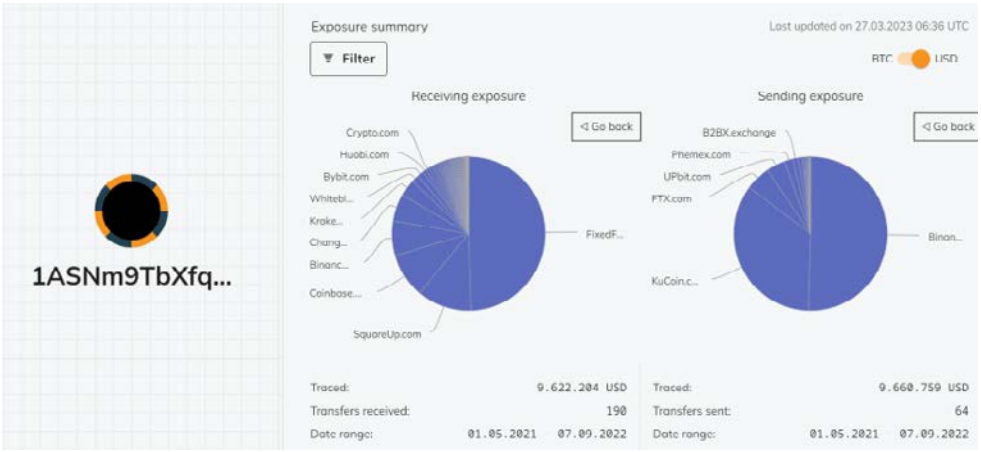

Abbildung 2: Analysesoftware – Details eines Kryptowährungs-Clusters

2.4 Pig Butchering: Liebes- und Investmentbetrug

Ein aktuell besonders häufig zu beobachtender Modus Operandi ist das sogenannte „Pig Butchering” in Kombination mit dem klassischen Love Scam. Der Begriff 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 Kriminellen 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 Betrüger beiläufig eine Krypto-investitions-Website, auf der sie angeblich bereits hohe Renditen erwirtschaftet hätten. Nach und nach überreden sie die potenziellen Opfer, 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 der Tether USD (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 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 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 Bildmaterial.

2.5 Tochter-Sohn Trick über WhatsApp-Nachrichten

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

2.6 Bezahldiensttrick

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

2.7 Transportdienst-Trick

Ebenfalls auf Kleinanzeigenplattformen kursiert ein weiterer Trick: Die Täter nehmen Kontakt auf und täuschen Interesse an der vom Opfer angebotenen Ware vor. Aufgrund des derzeitigen Aufenthaltsortes der vermeintlichen Käuferin beziehungsweise des vermeintlichen Käufers, die zumeist angeblich im Ausland weilen, kann die Ware jedoch 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 vom Käufer übernommen und somit bezahlt werden. Bei dieser Betrugsform bestätigen gutgläubige Opfer tatsächlich Zahlungen an den Täter, ohne dass diese je die Ware abholen lässt.

2.8 Phishing

Phishing E-Mails/Websites traten auch 2023 gehäuft in Erscheinung. Alle größeren Bankinstitute in Österreich waren mittels Phishing von Zugangsdaten für E-Banking betroffen, wobei mit schädlichen Android-Applikationen mobile TANs für das Online-Banking abgegriffen wurden. Besonders im Rahmen der Anubis Android-Malware waren mehrere Phishing- und Malware-Verbreitungskampagnen im Umlauf. Der Link zur Phishing-Seite lässt sich nur per Android-Browser (Android-User-Agent) öffnen. Nach Eingabe der Daten erfolgt die Aufforderung zum Download einer sogenannten „Sicherheits-App“.

2.9 Ransomware

Ransomware ist eine Schadsoftware, die von Kriminellen verwendet wird, um den Zugriff auf Daten oder das gesamte Computersystem eines Opfers zu verhindern. Dabei werden die Daten auf dem Computer des Opfers verschlüsselt oder der Zugriff darauf

wird blockiert. Die Angreifer fordern anschließend Lösegeld, um die Daten wieder freizugeben. Ransomware kann auf verschiedene Arten in ein System eindringen, zum Beispiel durch Öffnen von E-Mail Anhängen, Social Engineering oder durch das 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 Angreifer können von finanziellen Forderungen bis hin zu ideologischen Gründen reichen. In diesem Zusammenhang wird auf den „Ransomware Report 2023“ des C4 im Bundeskriminalamt verwiesen.

Im Bundeskriminalamt C4 werden die 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 (selbe 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 durch das Büro 5.2. International durchzuführende Anfragen, Datenabgleich, Koordination, Fallkooperation mit anderen Ländern etc. erfolgt durch das C4.

Insgesamt wurden im Jahr 2023 148 Fälle im gesamten Bundesgebiet zur Anzeige gebracht.

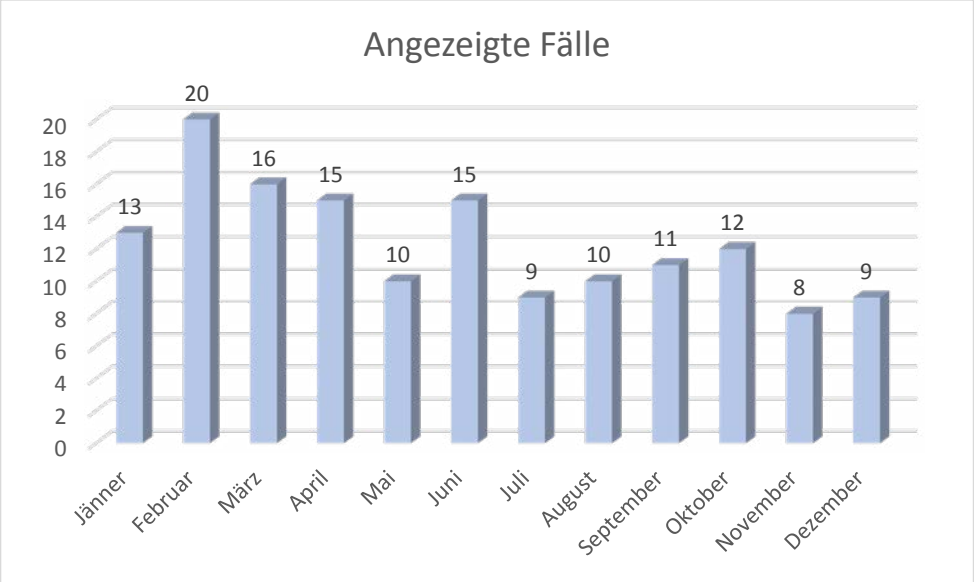

Abbildung 3:
Monatliche Verteilung der Ransomware-Fälle 2023

Die Mehrheit der Angriffe erfolgte in der ersten Jahreshälfte und danach wurde ein leichter Rückgang verzeichnet. Es ist erkennbar, dass ein großer Teil der Angriffe durch viele kleinere Akteure durchgeführt wurde. Lediglich einige wenige Gruppierungen (zum Beispiel LockBit) zeichnen sich für fortgesetzte Tathandlungen und mehrere Angriffe verantwortlich.

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

Über ein Drittel der Angriffe fanden auf Unternehmen statt. Dabei kann keine Konzentration auf bestimmte Zielbranchen festgestellt werden. Es konnten 35 unterschiedliche Akteure als Angreifer identifiziert werden.

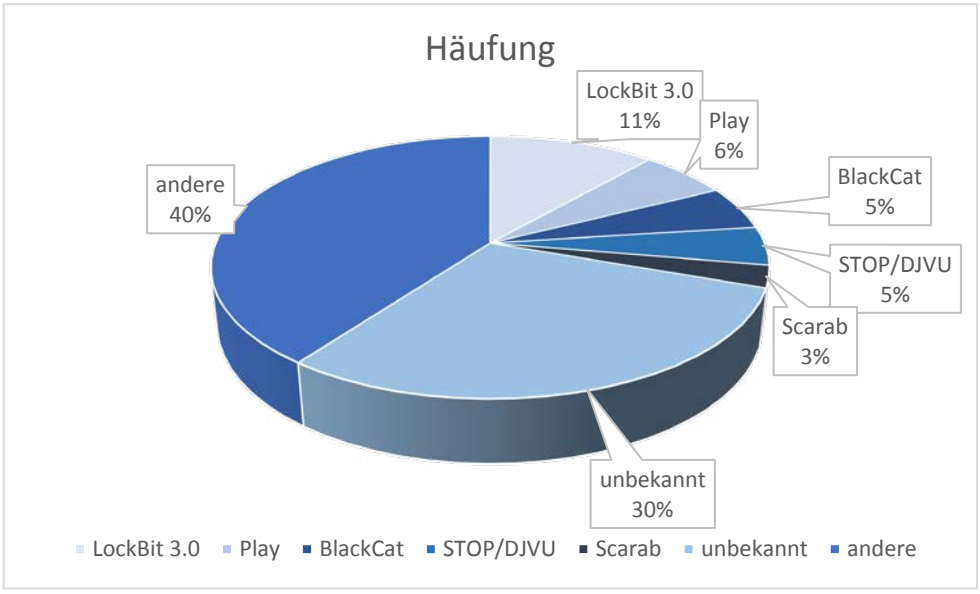

Abbildung 4:
Ransomware-Arten und prozentuelle Verteilung 2023

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

2.10 RDDoS-Angriffe

Eine Sonderform von DDoS-Attacken stellten auch im vergangenen Jahr Ransom-DDoS-Angriffe (RDDoS-Angriffe) dar. Diese liegen vor, wenn Täter (-gruppierungen) versuchen, eine Person oder Organisation zu erpressen, dazu mit einem DDOS-Angriff drohen und Lösegeld verlangen. Beobachtungen zufolge führen manche 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 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.

2.11 Suchtgifthandel im Darknet

Der Onlinehandel mit illegalen Suchtmitteln ist seit nunmehr einigen Jahren eine gängige Form der Suchtmittelkriminalität und hat sich auch in Österreich damit als neue Begehungsform etabliert. Kriminelle Organisationen, als auch Einzeltäter, verwenden vor allem das Darknet sowie vermehrt auch andere Online-Plattformen zur Abwicklung ihres organisierten Suchtmittelhandels und erwirtschaften damit ihre illegalen Gewinne. Dabei werden die gesamten Geschäftsgebarungen, angefangen von der Anbahnung, über die Verkaufsverhandlungen bis hin zur Bezahlung über diese verschlüsselten Netzwerke, abgewickelt. Von den Verkäuferinnen und Verkäufern als auch Käuferinnen und Käufern wird dabei der hohe Grad an Anonymität und das Fehlen des persönlichen Kontakts, als auch die ständige Verfügbarkeit, geschätzt.

Die Ermittlungen in diesem Deliktsfeld haben gezeigt, dass der Online-Drogenhandel den Straßenhandel nicht verdrängt, sondern diesen vielmehr ergänzt und erweitert. Im Unterschied zum Straßenhandel werden im Bereich des Online-Handels über zahlreiche Plattformen vor allem Suchtmittel höherer Qualität erworben, die auch im Straßenhandel gewinnbringend weiterverkauft werden. Ferner bietet der Onlinehandel ein diverseres, leicht zugängliches Angebot vor allem nicht üblicher synthetischer Suchtmittel.

Inwieweit Österreich vom Online-Suchtmittelhandel betroffen ist, zeigt sich durch nachstehende Zahlen. Seit September 2016 werden vom deutschen Zoll regelmäßig

Schwerpunktkontrollen bei Export-Briefsendungen durchgeführt. Dabei wurden im internationalen Briefzentrum Frankfurt am Main Postsendungen sichergestellt, die illegales Suchtmittel beinhalteten. Adressiert waren die Briefsendungen an Empfänger aus über 90 verschiedenen Nationen. Dabei belegte Österreich seit Beginn der Kontrollen, gemessen an der Anzahl der Empfängerinnen und Empfänger, den zweiten Platz hinter den USA und liegt vor Ländern wie Großbritannien, Frankreich oder Australien. Vom zweiten Halbjahr 2019 bis Ende 2021 führte Österreich diese Reihung sogar an. Auch innerhalb Österreichs werden regelmäßig Postsendungen mit illegalen Suchtmitteln sichergestellt. Im Jahr 2023 konnten durch das Zollamt Österreich 3.302 Sendungen mit Suchtmitteln sichergestellt werden. Von internationalen Partnern wurden weitere 285 Sendungen mit illegalen Suchtmitteln, mit Ziel oder Herkunft Österreich, sichergestellt. Im Anschluss durchgeführte Ermittlungen zu diesen Sicherstellungen ergaben, dass das Suchtgift der aufgegriffenen Briefsendungen meist über Darknet-Marktplätze bestellt wurde, wobei in der jüngeren Vergangenheit eine Verlagerung vom Darknet auf Instant-Messenger-Apps mit End-to-End Verschlüsselung und Social-Media-Kanälen zu beobachten ist.

Es wird angenommen, dass ca. zwei Drittel der sichergestellten Sendungen ursprünglich aus den Niederlanden stammen, diese teils jedoch zuvor nach Deutschland verbracht und dort in den Postweg eingebracht werden. Ferner konnte eine Zunahme von sichergestellten Paketsendungen mit zumeist großen Mengen an synthetischen Substanzen via Österreich in Richtung Ozeanien und Amerika beobachtet werden. Diesbezüglich wurde die Kooperation mit den betroffenen Ländern ausgebaut.

Zur Bekämpfung dieser Begehungsform der Suchtmittelkriminalität wurde im Jahr 2018 ein spezialisiertes Referat im Büro zur Bekämpfung der Suchtmittelkriminalität im Bundeskriminalamt eingerichtet. Dieses konzentriert sich hauptsächlich auf Ermittlungen gegen in Österreich ansässige Online-Suchtmittelhändler und koordiniert die polizeilichen Maßnahmen zur strafrechtlichen Verfolgung der Käuferinnen und Käufer. Neben den operativen Ermittlungsmaßnahmen werden durch das Fachreferat, teils im Wege des internationalen polizeilichen Informationsaustausches, fortwährend neue Strategien entwickelt und aktuelle Entwicklungen analysiert. Dabei zeigt sich, dass die effektivste Maßnahme zur Bekämpfung dieser Kriminalitätsform die Zerschlagung der Vertriebswege ist. Zu Erreichung dieses Ziels werden seit Beginn 2020 die operativen Ermittlungen mit Schwerpunktkontrollen der Postwege kombiniert und ergänzt. Diese Schwerpunktkontrollen erfolgen in enger Abstimmung und Kooperation mit der österreichischen Zollverwaltung und können als sehr erfolgreich bezeichnet werden.

Auch im Jahr 2024 werden diese Maßnahmen weiter fortgeführt und intensiviert.

2.12 Bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellungen minderjähriger Personen

2023 – Neues Rekordhoch an übermittelten NCMEC-Verdachtsmeldungen

Im Jahr 2023 kam es zur Übermittlung von insgesamt 15.882 Verdachtsmeldungen durch US Internet Service Provider an das Bundeskriminalamt. Ein neuer Rekord an Meldungen, der den letztjährigen Spitzenwert in der langjährigen Kooperation zwischen den National Center for Missing & Exploited Children NCMEC und dem Bundeskriminalamt um mehr als 5.700 Meldungen übertraf.

Abbildung 5:
Fünf-Jahresvergleich der Anzeigen nach § 207a StGB

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

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

Basierend auf den übermittelten NCMEC Reports gelang es dem zuständigen Referat BK 3.2.7 im Jahr 2023, insgesamt 16 Opfer zu identifizieren (13 Minderjährige, drei Opfer in der Altersgruppe von 15 bis 18 Jahren und zwei Opfer in Deutschland).

Ebenfalls im Zunehmen ist das Phänomen des so genannten „Long Distance Child Abuse“. So sieht sich die Kriminalpolizei mit einer stetig steigenden Anzahl von Fällen konfrontiert, in denen österreichische Täter den sexuellen Missbrauch von Kindern auf den Philippinen beauftragen und diesen anschließend online in Echtzeit konsumieren.

Hier ist positiv zu vermerken, dass es der spezialisierten Ermittlungseinheit im Bundeskriminalamt im Jahr 2023 möglich war, in Zusammenarbeit mit den Landeskriminalämtern und der österreichischen Verbindungsbeamtin in Bangkok, **elf** minderjährige Opfer auf den Philippinen zu identifizieren und diese von weiteren Missbrauchshandlungen zu bewahren.

§ 207a StGB (Bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellungen minderjähriger Personen)	**Straftatenanzahl**	**Anzahl geklärt**	**Aufklärungsquote**
Jahr 2014	465	390	83,9 %
Jahr 2015	465	409	88,0 %
Jahr 2016	681	602	88,4 %
Jahr 2017	733	650	88,7 %
Jahr 2018	1 161	1 037	89,3 %
Jahr 2019	1 666	1 541	92,5 %
Jahr 2020	1 702	1 528	89,8 %
Jahr 2021	1 921	1 775	92,4 %
Jahr 2022	2 061	1 889	91,7 %
Jahr 2023	2 245	2 053	91,4 %

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

3
Jahresrückblick

3.1 Zahlen und Fakten im Überblick

Die nachfolgenden Zahlen und Daten stammen aus der öffentlich verfügbaren und offiziell verlautbarten Polizeilichen Kriminalstatistik (PKS). Eine Zunahme der begangenen Straftaten im Cybercrime-Bereich konnte auch im Jahr 2023 beobachtet werden. Dieser Trend wird seit geraumer Zeit durch die anhaltende Verlagerung vieler Lebensaspekte in die digitale Welt zusätzlich verstärkt.

Cybercrime im 5-Jahresvergleich

Jahr	Anzahl der angezeigten	Anzahl geklärt	Aufklärungsquote
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 %

Tabelle 3:
Entwicklung der Anzeigen, geklärten Fälle und der Aufklärungsquote von Cybercrime 2019 bis 2023 (Fünf-Jahres-Vergleich)

Die Entwicklung der Internetkriminalität zeigt, dass mit 65.864 Anzeigen im Jahr 2023 und somit einer Zunahme von 9,4 Prozent gegenüber dem Vorjahr ein neuer Spitzenwert erreicht wurde. Der Aufwärtstrend setzt sich erwartungsgemäß kontinuierlich fort: im Vergleich zum Jahr 2019 wurden mehr als doppelt so viele Straftaten angezeigt. Bedingt durch den deutlichen Zuwachs 2023 ging die prozentuelle Aufklärungsquote um 2,2 Prozentpunkte im Vergleich zum Vorjahr zurück. In absoluten Zahlen konnten jedoch 440 zusätzliche Straftaten seitens der Kriminalpolizei aufgeklärt werden.

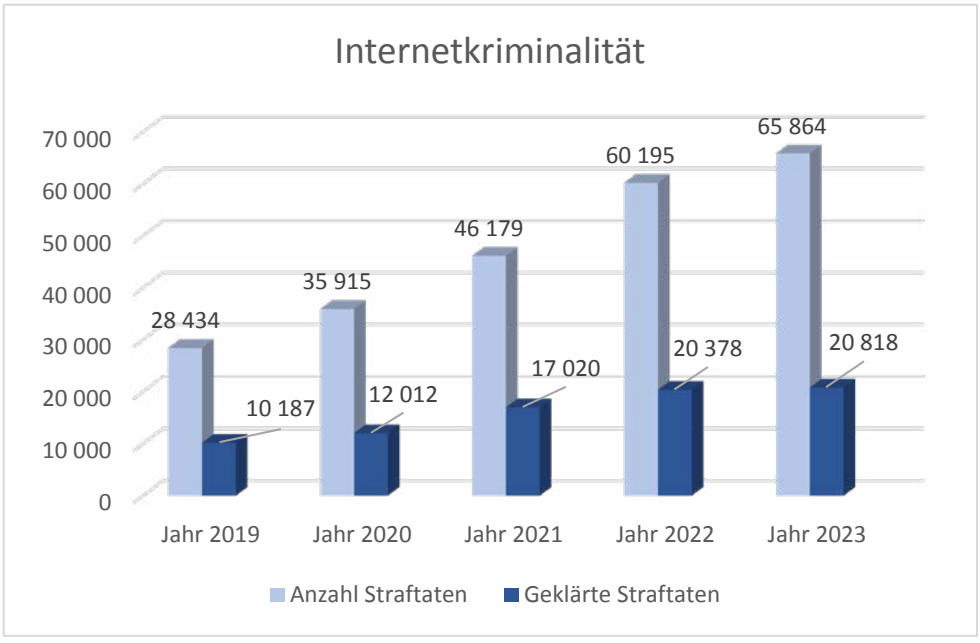

Abbildung 6:
Entwicklung der Anzeigen und aufgeklärten Fälle von Cybercrime 2019 bis 2023

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

Im Jahr 2023 konnte bei Tatbeständen zu Cybercrime im engeren Sinn ein leichter Rückgang der Anzeigen in Höhe von 6,4 Prozent gegenüber dem Vorjahr verzeichnet werden, was jedoch mit einer geänderten statistischen Erfassung im Hinblick auf § 148a StGB einhergeht.

Im Zuge der Analyse des Zahlenmaterials kann folgendes festgestellt werden:

Die Zunahme der Anzeigen nach §107c und §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.

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

Bei den Anzeigen nach §126 a, §126b und §126c StGB sind Rückgange zu verzeichnen, deren Ursachen darauf zurückführen sind, dass es sich hier oftmals um strafbare Handlungen, die Wirtschaftsbetriebe treffen, handelt. Durch die Aufklärung in diesem Bereich und auch die Zusammenarbeit mit der Wirtschaftskammer konnte erreicht werden, dass sich Firmen im digitalen Bereich besser schützen. Einerseits werden Mitarbeiterinnen und Mitarbeiter sensibilisiert, andererseits werden technische Vorkehrungen gegen Cyberangriffe getroffen. Darüber hinaus ist der finanzielle Schaden oftmals gering, wenn sie über Backups verfügen und daher kein Datenverlust eintritt. Dieser geringe Schaden führt auch dazu, dass die Anzeigebereitschaft sinkt und hier durchaus mit einer höheren Dunkelziffer zu rechnen ist.

Der Rückgang der Anzeigen nach §148a StGB in der Statistik verzerrt das Bild etwas. Grund ist ein OGH-Urteil aus dem Jahr 2023. Dieses hatte zur Folge, dass Behebungen mit einer fremden Bankomatkarte jetzt als Einbruch angezeigt und auch statistisch erfasst werden. Die Statistik im Bereich des §129 StGB bestätigt dies und zeigt, dass es hier zu einer Steigerung gekommen ist.

Die Zunahme der Anzeigen nach §225a StGB beruht auf der steigenden Digitalisierung im Alltag. Immer mehr Menschen verwenden digitale Medien zunehmend intensiver, was auch zu einem Anstieg der strafbaren Handlungen in diesem Bereich führt. Darüber hinaus finden vermehrt Kontrollen im Schwerverkehr statt und es werden Manipulationen an Fahrtenschreibern angezeigt, die ebenfalls den Tatbestand des §225a StGB erfüllen.

Delikt	Angezeigte Fälle 2022	Angezeigte Fälle 2023	Geklärte Straftaten 2022	Geklärte Straftaten 2023
§ 107c StGB	402	458	305	365
§ 118a StGB	1 796	1 858	183	256
§ 119 StGB	12	13	10	9
§ 119a StGB	64	67	16	11
§ 126a StGB	375	308	59	82
§ 126b StGB	109	59	4	3
§ 126c StGB	525	305	99	40
§ 148a StGB	18 441	17 154	3680	3369
§ 225a StGB	652	729	367	183
GESAMT	22 376	20 951	4723	4318

§ 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 2022/2023.

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,zum Beispiel Betrugsdelikte, Drogenhandel im Darknet, Kindesmissbrauch-Online, Cybergrooming oder Cybermobbing. In der Polizeilichen Kriminalstatistik umfasst Cybercrime im weiteren Sinne beispielsweise die Paragrafen des Internetbetrugs und der sonstigen Kriminalität im Internet.

Der Internetbetrug stellt zahlenmäßig den größten Bereich der Cyberkriminalität dar und ist auch maßgeblich für den letztjährigen Gesamtanstieg der Delikte verantwortlich. Mehr als die Hälfte der Internetdelikte fallen auf Betrugsdelikte: 2023 wurden 34.069 Fälle von Internetbetrug angezeigt, ein Plus von 23,3 Prozent. Mit der fortschreitenden Digitalisierung verlagern sich Betrugsdelikte immer mehr ins Internet. Für die Kriminellen ist es ein Leichtes, aufgrund technischer Anonymisierung sowie Verschleierung der Finanzflüsse Betrugshandlungen unerkannt und damit „sicher" durchzuführen. Zusätzlich können durch den weltweiten Zugang zum Internet immer mehr Menschen als potenzielle Opfer angesprochen werden. Der Bestellbetrug, sowohl kauf- als auch verkaufseitig, gehört hierbei zu den größten Bereichen, gefolgt von unbefugten Abbuchungen von Bankkonten der Opfer. Auch der Anrufbetrug (Stichwort „falscher Polizist") und international agierende Call Center trieben die Statistik in die Höhe, ebenso der digitale Investmentbetrug.

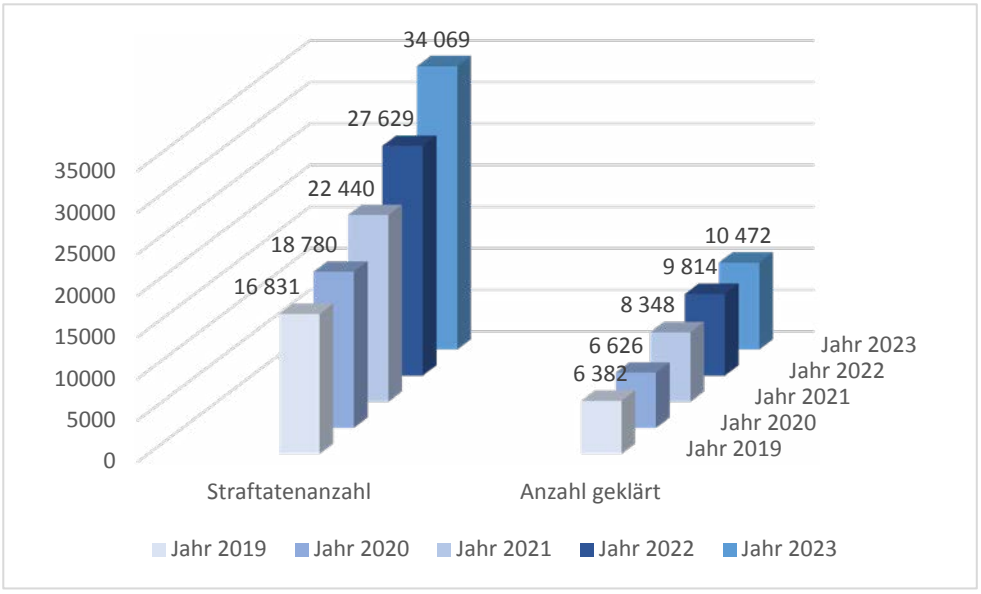

Abbildung 7: Fünf-Jahresvergleich Internetbetrug §§ 146-148 StGB (Örtlichkeit „Internet")

Unter sonstiger Kriminalität im Internet versteht man Straftaten, die ihren Tatort im Internet haben. Ausgenommen sind Cybercrime im engeren Sinn, der Internetbetrug, bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellungen minderjähriger Personen.

(§ 207a StGB) und die Anbahnung von Sexualkontakten zu Unmündigen (§ 208a StGB). Im Bereich der sonstigen Kriminalität im Internet wurde im Jahr 2023 ein leichter Anstieg der Delikte verzeichnet. Eine zunehmende Verlagerung klassischer Strafrechtsdelikte ins Internet lässt sich seit Jahren beobachten. Gleichzeitig werden sogenannte „Crime-as-a-Service"-Leistungen im Darknet angeboten. Dabei handelt es sich vorwiegend um Hacking-Tools oder Erpressungstrojaner. Ebenso wird ein vermehrter Vertrieb von Falschgeld, Kinderpornografie und Kreditkartendaten wahrgenommen. Durch die im Darknet angebotenen Dienste stiegen 2023 vor allem Erpressungen mit Ransomware und Massenerpressungsmails stark an, meist begleitet von Geldforderungen in Kryptowährungen.

Zunahmen wurden beispielsweise bei § 106 StGB (Schwere Nötigung, 307 Anzeigen) sowie § 107 StGB (Gefährliche Drohung, 1.209 Anzeigen) und § 107a StGB (Beharrliche Verfolgung, 470 Anzeigen) verzeichnet. Anzeigen nach § 223 StGB (Urkundenfälschung) und dem Verbotsgesetz (Wiederbetätigung) sanken, bleiben jedoch nach wie vor auf hohem Niveau (bspw. 729 Anzeigen nach § 3g VerbotsG).

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

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

Die Vorgehensweise der Täter hat sich im Laufe der Zeit dahingehend verändert, als dass das Senden dieser SMS vielmehr als Vorbereitungshandlung dient. Anschließend erfolgt eine telefonische Kontaktaufnahme mit gespoofter Telefonnummer. Beim sogenannten „Caller-ID-Spoofing" wird die Nummer auf dem Display des Angerufenen („gespoofte Telefonnummer") mit technischen Mitteln verfälscht und ist somit nicht mehr rückverfolgbar. Angebliche Bankmitarbeiterinnen oder -mitarbeiter melden sich und bringen Opfer dazu, Überweisungen zu tätigen.

Phishing-Betrug auf Kleinanzeigenplattformen trat auch im Jahr 2023 auf. Opfer möchten private Gegenstände auf Kleinanzeigenplattformen verkaufen. Kriminelle stellen den Kontakt zu den Opfern her und bekunden scheinbares Kaufinteresse. Die Kriminellen wirken seriös und ernsthaft interessiert. Schließlich wird von ihnen 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. In Wirklichkeit geben die Betroffenen eine Zahlung frei und überweisen Geld an die Kriminellen.

Der sogenannte Tochter-Sohn-Trick ist dem Bundeskriminalamt seit dem Jahr 2021 bekannt. Kriminelle verschicken per SMS oder WhatsApp eine Nachricht an die Geschädigten. Darin geben sie sich als angebliche Tochter oder angeblicher 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 Zahlungsempfänger ausländische Konten übermittelt. Die Opfer überweisen im Glauben, der Tochter oder dem Sohn Gutes zu tun. Zumeist erfolgt der Transfer in Echtzeit. Mittels Installierung einer Ermittlungsgruppe, koordiniert durch die Abteilung 7.2 des Bundeskriminalamts, und durch entsprechende Präventionsarbeit wird versucht, dieses Phänomen einzudämmen.

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

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

Erpressungen im Internet (§§ 144, 145 StGB)

2023 wurden 3.891 Erpressungen im Internet angezeigt. Das ist eine Steigerung von 13,6 Prozent gegenüber dem Vorjahr (3.424 angezeigte Fälle). Besonders auffällig ist hierbei die niedrige Aufklärungsquote von lediglich fünf Prozent.

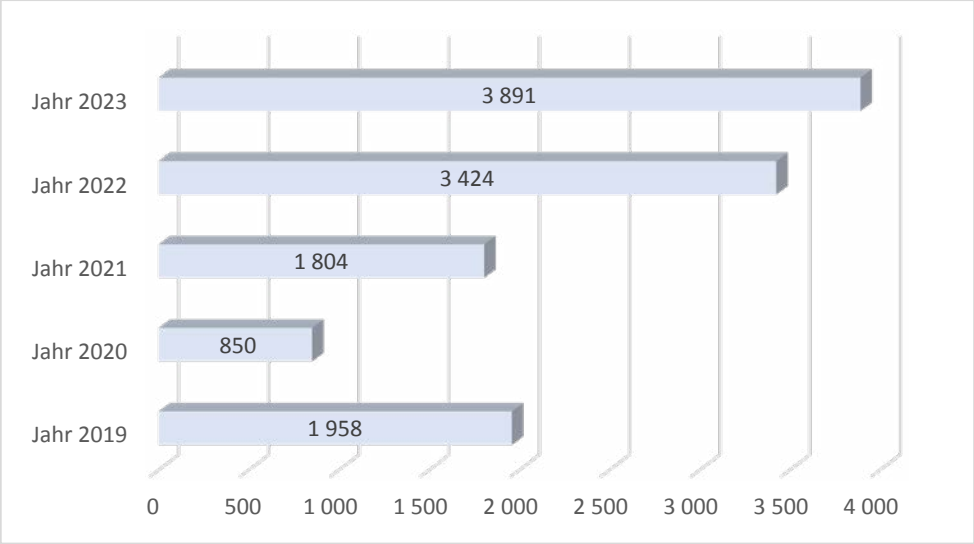

Abbildung 8:
Erpressung im Internet - § 144 StGB (Erpressung), 145 StGB (Schwere Erpressung)

Erpressung im Internet stieg im Berichtsjahr als Geschäftsmodell krimineller Gruppierungen weiter an. Wie eine Evaluierung der Anzeigen nach §§ 144 und 145 StGB durch die im Bundeskriminalamt eingerichtete Arbeitsgruppe „ARGE – Erpressungsmails“ zeigt, sind organisierte Tätergruppen nicht nur durch das Versenden von Massenerpressungsmails, sondern auch durch Sextortion, im großen Stil überregional und transnational aktiv. So machen Sextortion-Fälle einen beachtlichen Teil der angezeigten Erpressungen im Internet aus. Das Bundeskriminalamt hat auf diese Entwicklung reagiert und gemeinsam mit den Landeskriminalämtern eine einheitliche und strukturierte Vorgehensweise zur Bekämpfung der Gruppierungen hinter diesen Sextortion-Fällen festgelegt.

Delikt	Angezeigte Fälle 2022	Angezeigte Fälle 2023	Geklärte Straftaten 2022	Geklärte Straftaten 2023
		Internetbetrug		
§ 146 StGB	23856	28975	8418	8287
§ 147 StGB	2885	3579	912	1168
§ 148 StGB	888	1515	484	1017
Internetbetrug Gesamt	27629	34069	9814	10472
		Sonstige Kriminalität im Internet		
§ 105 StGB	450	373	201	206
§ 106 StGB	270	307	106	113
§ 107 StGB	1057	1209	911	1040
§ 107a StGB	437	470	407	432
§ 115 StGB	83	48	76	42
§ 207b StGB	2	0	2	0
§ 218 StGB	1	0	0	0
§ 223 StGB	241	150	200	119
§ 224 StGB	29	41	17	20
§ 228 StGB	1	1	1	1
§ 231 StGB	38	63	19	19
§ 232 StGB	29	36	27	35
§ 241a StGB	1	2	0	0
§ 283 StGB	138	135	129	123
§ 27 SMG	740	785	573	600
§ 28 SMG	8	12	7	10
§ 28a SMG	43	64	35	55
§ 30 SMG	29	34	28	33
§ 31 SMG	0	1	0	1
§ 31a SMG	2	0	2	0
§ 32 SMG	1	0	1	0
§ 3a VerbotsG	2	2	2	2
§ 3b VerbotsG	1	0	1	0
§ 3d VerbotsG	6	12	5	12
§ 3g VerbotsG	909	729	886	717
§ 3h VerbotsG	62	59	56	58
§ 4 NPSG	15	76	14	65

Tabelle 5: Jahresvergleich 2022/2023 angezeigte Fälle von Cybercrime im weiteren Sinn nach Paragraphen

3.4 Dunkelziffer und Anzeigeverhalten

Die Dunkelziffer im Bereich der Internetkriminalität ist, wenn man internationale Studien berücksichtigt, besonders hoch. Viele Betroffene scheuen die Anzeige bei der nächsten Polizeidienststelle, teils aus Scham, Angst vor Reputationsverlust oder weil angenommen wird, dass der Fall ohnehin nicht verfolgt werden könnte.
Jedoch kann mit jedem angezeigten Vorfall die Beweismittellage zu verdächtigen Tätergruppen weiter verdichtet werden. Außerdem verbessert die Anzahl der Anzeigen die frühere Erkennung von neuen Massenphänomenen für die ermittelnden Strafverfolgungsbehörden. Ebenso können Präventionsmaßnahmen zeitnaher gesetzt und mit zielgerichteten Warnhinweisen an die Bevölkerung die Anzahl der Geschädigten reduziert werden. Eine Wiedererlangung abhanden gekommener Vermögenswerte gelingt jedoch selbst nach internationaler Ausforschung der Täter nur in den seltensten Fällen. Deshalb gebührt im Bereich des Internetbetrugs der Verhinderung von Straftaten durch verstärkte Bewusstseinsbildung und Aufklärung erhöhte Aufmerksamkeit. Die Täter nutzen menschliche Schwächen wie Gier und Sehnsüchte nach Anerkennung oder Beziehungen aus, um sich zu bereichern. Auch im Jahr 2023 blieb Social Engineering ein maßgeblicher Angriffsvektor.

4 Ermittlungs-erfolge (Beispiele)

4.1 OP Torman

Im März 2023 wurde das Landeskriminalamt (LKA) Niederösterreich von einer ausländischen Dienststelle über einen aktuellen Versuch zur Vergabe eines Auftragsmordes im Darknet verständigt. Ein vorerst unbekannter Täter versuchte unter dem Pseudonym „sunnyboy“, in einem Darknet-Forum einen Auftragsmörder zur Ermordung einer weiblichen Person in Niederösterreich zu finden. Aufgrund der vorliegenden Erkenntnisse war bekannt, dass bereits erste Zahlungen mittels Kryptowährungen erfolgt sind. Im Zuge der ersten Erhebungen durch das LKA Niederösterreich konnte das potentielle Opfer ausgeforscht und Sicherungsmaßnahmen eingeleitet werden.

Für die weiteren komplexen Ermittlungen wurden die Fachbereiche Darknet- und Blockchain-Ermittlungen des Bundeskriminalamts/C4 beigezogen. Aufgrund der technischen Versiertheit des Verdächtigen und der zahlreichen Maßnahmen zur Verschleierung seiner Identität mussten aufwendige Ermittlungsmaßnahmen durchgeführt werden. Im Rahmen der gemeinsamen Ermittlungen konnten schließlich zahlreiche Indizien und Beweise gesichert werden, die zur Ausforschung des Verdächtigen geführt haben. Im Zuge der Hausdurchsuchung und der Festnahme des Verdächtigen – mit Unterstützung der Observationseinheiten und dem EKO Cobra der DSE – wurden weitere Beweise sichergestellt, die den Verdacht erheblich erhärteten. Die involvierten Ermittlerinnen und Ermittler aus dem In- und Ausland wurden aufgrund der erfolgreichen Ausforschung und Festnahme des Verdächtigen sowie der dadurch verhinderten Ermordung einer Mutter aus Niederösterreich vom Bundesminister für Inneres geehrt.

In der Hauptverhandlung am Landesgericht Wr. Neustadt im November 2023 zeigte sich der Angeklagte am Ende geständig und wurde zu 15 Jahren Freiheitsstrafe verurteilt. Das Urteil war zum Zeitpunkt der Berichterstellung noch nicht rechtskräftig.

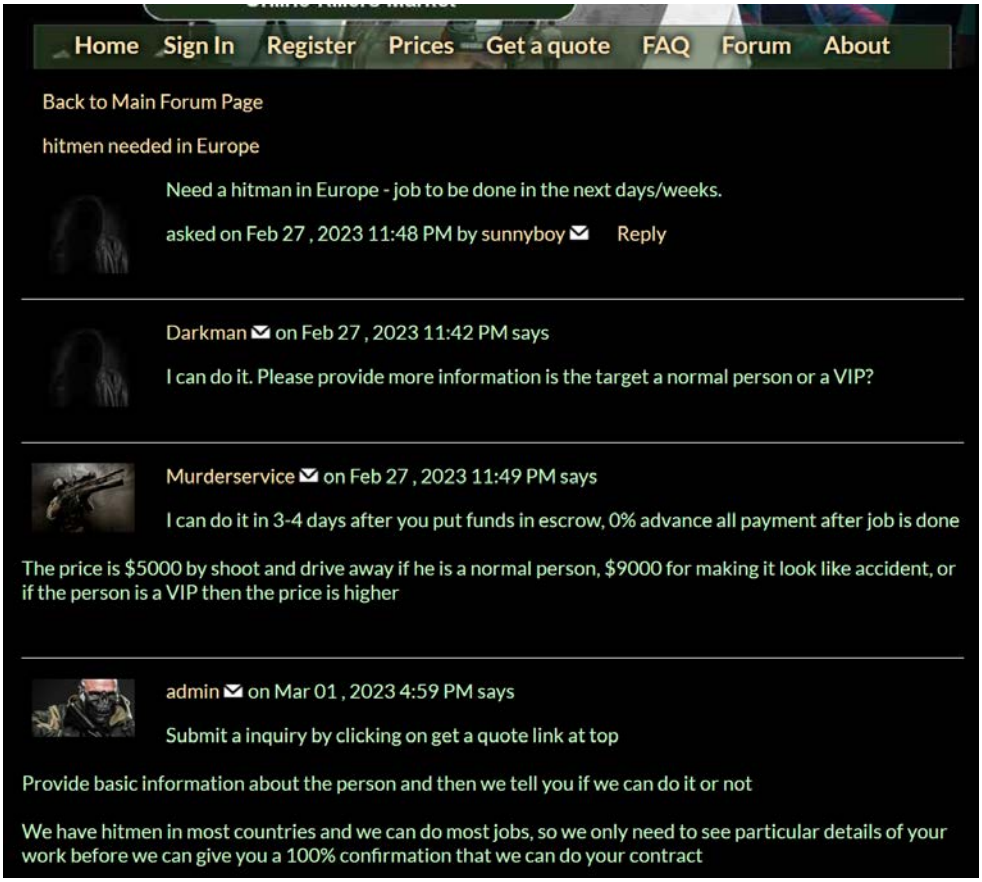

Abbildung 9:
Screenshot eines Darknet-Forums samt einschlägiger Kommunikation

4.2 Ransomware-Angriffe erfolgreich aufgearbeitet

Ransomware-Angriffe auf Unternehmen richten weltweit nicht nur große Schäden an, sondern stellen auch für die Polizei eine Herausforderung dar. Die Qualität der Angriffe steigt kontinuierlich und wenn sich diese aus Tätersicht als erfolgreich erweisen, sind die Reaktion und Aufarbeitung zeit- und kostenintensiv.

Die Vorgehensweise bei Ransomware-Angriffen hat sich von der Ausgangslage geändert. Anfangs handelte es sich um einfache Lösegeldforderungen, die sich 2022 zu einer Multifaktor-Erpressung entwickelten. Die Daten werden beim Angriff nicht mehr nur verschlüsselt, sondern auch durchforstet und exfiltriert, um den Opfern anschließend mit der Veröffentlichung der Daten im Internet oder Übermittlung an ein Konkurrenzunternehmen zu drohen. Die Angriffe erfolgen zum Teil über E-Mails mit einer Schadsoftware als An-

hang oder durch das Nützen von Sicherheitslücken. Die von den Kriminellen geforderten Geldbeträge liegen zwischen wenigen Tausend Euro und zweistelligen Millionenbeträgen.

Das Referat IT-Ermittlungen (vormals Soko Clavis) des C4 im Bundeskriminalamt koordiniert und ermittelt schwerpunktmäßig Ransomware-Fälle in ganz Österreich. Da sich Ransomware-Angriffe nicht auf nationale Bereiche beschränken, ist eine internationale Zusammenarbeit notwendig. Die international agierende Ransomware-Gruppe „LockBit", die für den Angriff auf acht österreichische Unternehmen verantwortlich war, wurde Gegenstand von Ermittlungen. Von den Ransomware-Angriffen waren Unternehmen in zahlreichen Ländern betroffen, unter anderem in Japan.

Wenn gleichartige Fälle länderübergreifend auftreten, schließen sich Verbindungsbeamtinnen und -beamte bei Europol im Wege der Joint Cybercrime-Action-Taskforce (J-CAT) zu eigens eingerichteten Teams zusammen. So auch in diesem Fall, bei dem eine erfolgreiche Kooperation zwischen dem C4 und der japanischen Polizei etabliert werden konnte. Nach einem anfänglichen Informationsaustausch beschlossen Japan und Österreich direkt zusammenzuarbeiten, weshalb Cyber-Ermittler aus Japan für eine Woche im C4 in Wien zu Gast waren. In tagelanger Arbeit wurden Analysen durchgeführt und Erfahrungen ausgetauscht. Ein erheblicher Teil des Datenmaterials konnte in der Folge entschlüsselt und der Schaden beträchtlich reduziert werden. Durch internationale Kooperation konnten somit verschlüsselte Daten aus Ransomware-Angriffen entschlüsselt und den Opfern geholfen werden.

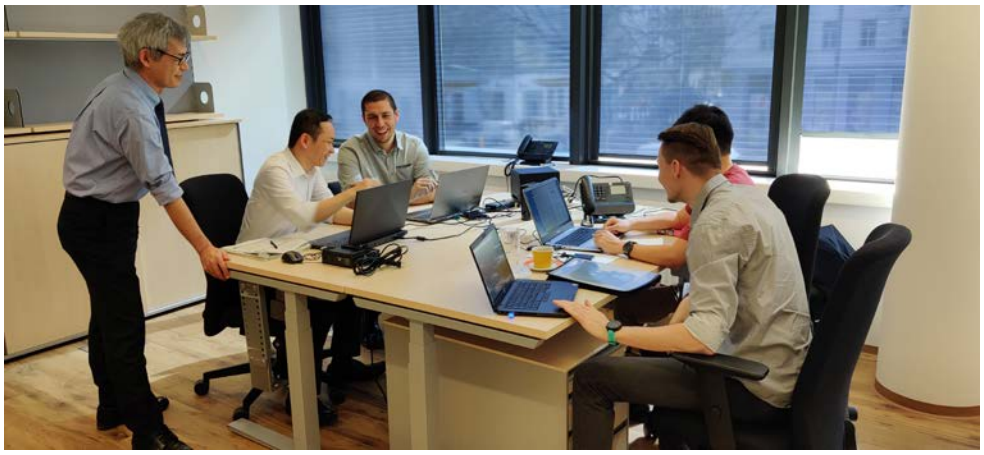

Bild 1:
Mitarbeiter des Cybercrime-Competence-Centers mit Kollegen der japanischen Polizei in Wien

5 Aufbau-organisation und Abläufe

5.1 Nationale und internationale Koordinierungs-, Ermittlungs- und Meldestelle

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

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

5.2 C4-Meldestelle

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

Anfragen erhält die Meldestelle wie ursprünglich vorgesehen von den behördeneigenen Dienststellen und zunehmend in Form von Mitteilungen durch Bürgerinnen und Bürger, Unternehmen sowie nationalen und internationalen Polizeidienststellen.

Im Jahr 2023 erreichten 15.304 Anfragen die Meldestelle, wobei 11.183 davon einen Bezug zu Cybercrime hatten. Damit kann eine Abnahme im Vergleich zum Vorjahr festgestellt werden, die sich einerseits auf verstärkte Präventionstätigkeiten seitens der Kriminalpolizei und nichtstaatlichen Organisationen sowie ein verbessertes Bewusstsein in der Bevölkerung zurückführen lässt, andererseits auch auf eine Diversifizierung der Meldemöglichkeiten für Unternehmen und Bevölkerung.

Beispielhaft können in diesem Zusammenhang folgende Seiten erwähnt werden:
https://www.onlinesicherheit.gv.at/Themen/Erste-Hilfe/Meldestellen.html
https://www.watchlist-internet.at/
https://www.ombudsstelle.at/
https://www.wko.at/it-sicherheit/cyber-security-hotline

https://zara.or.at/de/beratungsstellen
https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/Beschwerde_Meldung.de.html
https://www.stopline.at/de/home
https://dsn.gv.at/402/

Die allgemeinen Steigerungsraten im Cybercrime-Bereich korrelieren somit im Jahr 2023 nicht unmittelbar mit den in der Meldestelle des C4 verzeichneten Eingängen. Die Internetkriminalität steigt laut Polizeilicher Kriminalstatistik nach wie vor deutlich an, ein Phänomen, das sich von Jahr zu Jahr wiederholt.

In ihrer zentralen Funktion als Cybercrime-Schnittstelle innerhalb polizeiinterner Strukturen sowie als Meldestelle für die Bevölkerung und Wirtschaft agiert die Meldestelle als Koordinierungs- und Informationszentrum für diesen Themenkreis. Zusätzlich umfasst diese Tätigkeit auch 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 erfolgte einerseits durch die fortlaufende Kooperation mit unterschiedlichen Institutionen aus dem Bereich der Wirtschaft und 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 Europäischen Cybercrime Center (EC3) und den jeweiligen High-Tech Crime Units anderer Staaten (NCPs) fungiert, konnte auch 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 Tele-fonmeldungen	Relevante Web-Frontend Meldungen	Summe aller Meldungen
2023 01	1076	91	40	1320
2023 02	1016	48	53	1262
2023 03	1978	65	163	2291
2023 04	761	22	80	880
2023 05	672	33	68	933
2023 06	518	44	99	1020
2023 07	472	49	81	905
2023 08	567	52	110	989
2023 09	506	51	83	953
2023 10	664	52	129	1188
2023 11	558	49	131	1610
2023 12	563	58	99	1953

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

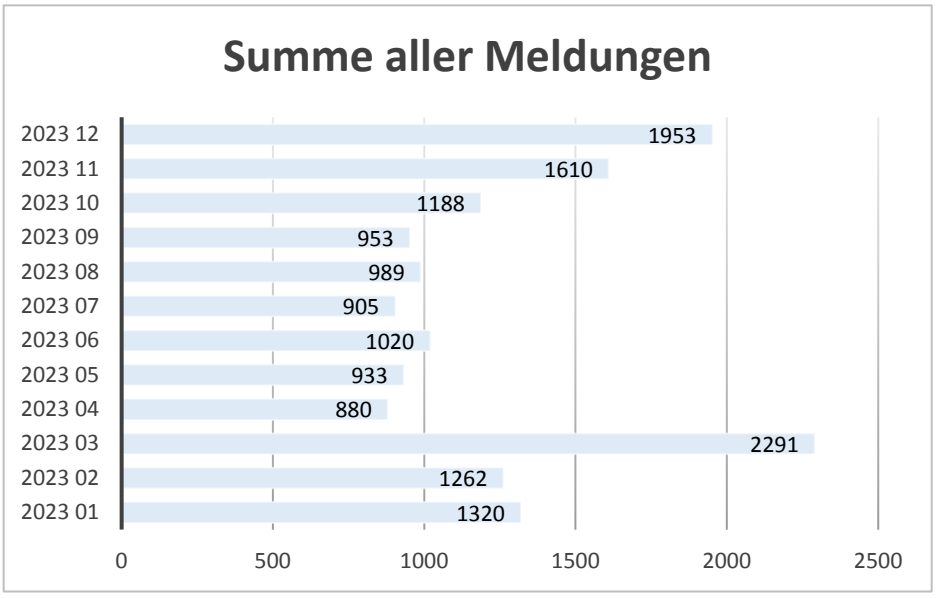

Abbildung 10:
Gesamtanzahl der Meldungen an die C4-Meldestelle nach Monaten (Jahresverlauf)

5.3 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 sowie Technik und der Justiz.

Die Auswahl, Inbetriebnahme und laufende Betreuung moderner Auswertesoftware gehört 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 und 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.

Bild 2:
Serverlandschaft des C4

Mithilfe spezieller Programme zur Sichtung großer Datenmengen wurden 2023 insgesamt 73 neue Fälle mit einem Analyseausgangsdatenvolumen von über 94 Terabyte erstellt. Zusätzlich wurden über 120 separate virtuelle Maschinen zur Beweismittelsichtung und fallbezogenen Recherche in Betrieb genommen, womit über 950 Ermittlerinnen und Ermittler im Bundeskriminalamt und den LKA Zugriff auf eine moderne Arbeitsumgebung zur Strafverfolgung erhalten haben. Im größten Einzelfall kooperieren mehr als 350 Ermittlerinnen und Ermittler sowie Dolmetscherinnen und Dolmetscher.

2023 stellte eine der wesentlichen Herausforderungen die Modernisierung und Optimierung der vorhandenen Speicher- und Rechenkapazität sowie die Verbesserung der Vernetzung mit weiteren Dienststellen dar. Daneben wurde die enge Zusammenarbeit mit dem Team des Projekts SeILE (Schaffung einer IKT-Lösung für kriminalpolizeiliche Ermittlungen) fortgeführt sowie mit technischen Proof of Concepts unterstützt. Des Weiteren wurde die technische Mitarbeit bei operativen Fallbearbeitungen im Cybercrime Competence Center und darüber hinaus intensiviert.

5.4 C4-Forensik

Die Auswertung von IT und Speichermedien stellte die betroffenen Forensikerinnen und Forensiker erneut vor große Herausforderungen, sowohl im Bereich der IT-Forensik wie auch der mobilen Forensik. Nach wie vor sind unzählige Geräte mit beträchtlichen Datenmengen aufzubereiten, um die ressourcenintensive Unterstützung der Ermittlerinnen und Ermittler zu gewährleisten. Wie aus der Statistik ersichtlich, war die IT-Forensik im Jahr 2023 mit einer starken Zunahme der auszuwertenden Datenmenge konfrontiert. Dies lässt sich durch den Umstand erklären, dass nach pandemiebedingter Abnahme die Zahl der Hausdurchsuchungen und der hiermit einhergehenden Auswertungen im Jahr 2023 deutlich gestiegen sind.

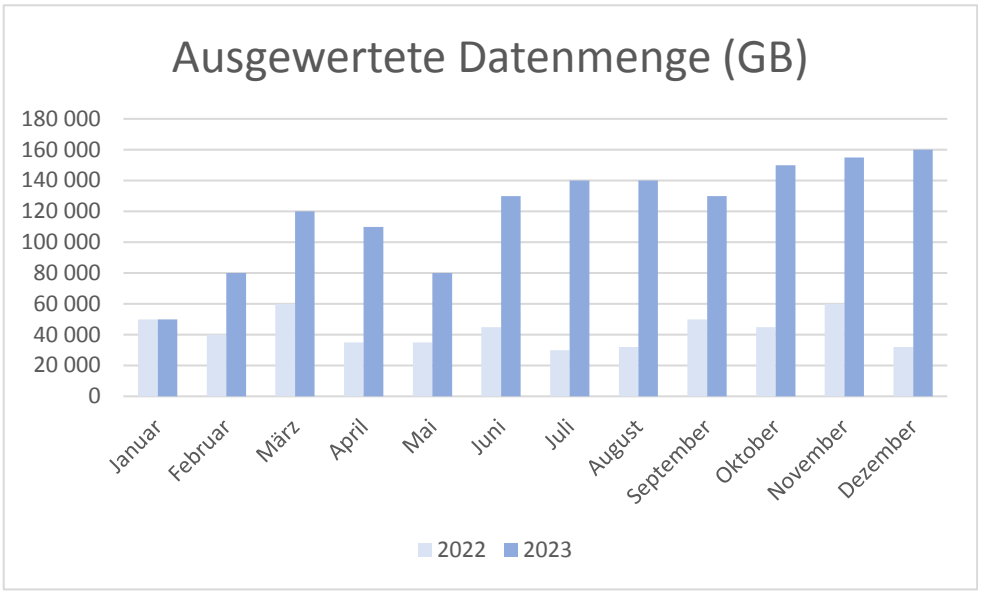

Abbildung 11:
IT-Forensik – Ausgewertete Datenmengen in GB

Wie bereits in den Vorjahren war auch 2023 der Support der C4-Forensik ein unverzichtbarer, wesentlicher Bestandteil strafrechtlicher Ermittlungen. Der elektronischen Beweismittelsicherung im C4 und den Landeskriminalämtern kommt weiterhin maßgebliche Bedeutung in der Ermittlungsarbeit zu. Die Gesamtmenge an ausgewerteten Daten im Bereich der Forensik belief sich 2023 auf 1.572 Terabyte (TB).

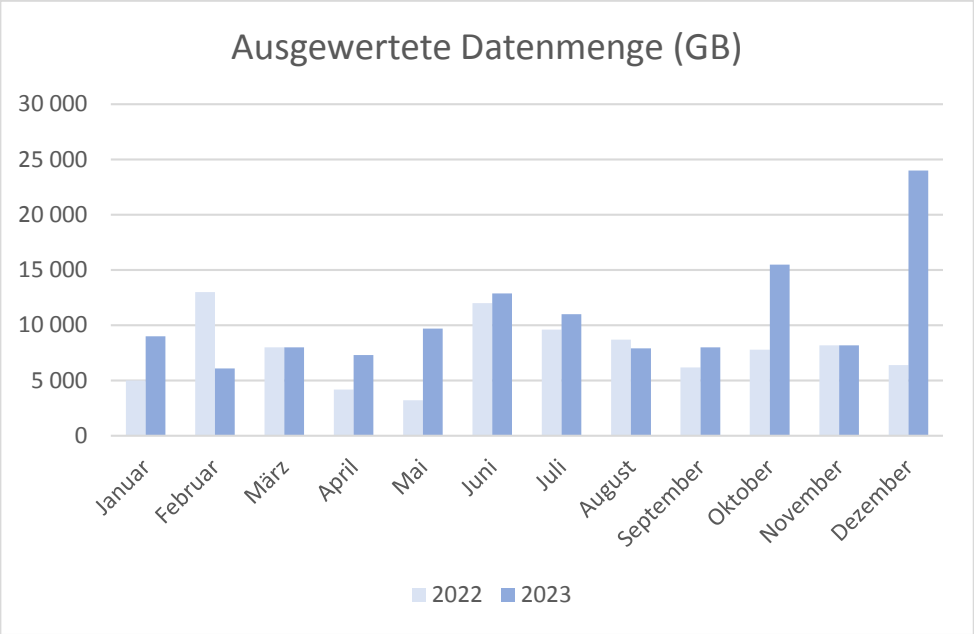

Abbildung 12:
Mobile Forensik –
Ausgewertete Datenmengen
in GB

Aufgrund der rasanten technischen Entwicklung und der eingesetzten Schutzmechanismen wird die Auswertung diverser Medien immer schwieriger. Herstellerspezifische Systeme mit ausgeprägten Verschlüsselungsverfahren stellen die elektronische Beweissicherung fortwährend vor große Herausforderungen. Sowohl im Bereich der mobilen Forensik wie auch der IT-Forensik werden Datensicherungen und Auswertungen immer komplexer. Das C4 sieht sich zunehmend mit umfassenden Auswertungen von Smartphones und Clouds konfrontiert, die zum Teil von den LKA nicht mehr bewältigt werden können. Die auszuwertenden Datenmengen (Festplatten, Netzwerkdaten, auch bei Mobiltelefonen) bleiben auf hohem Niveau.

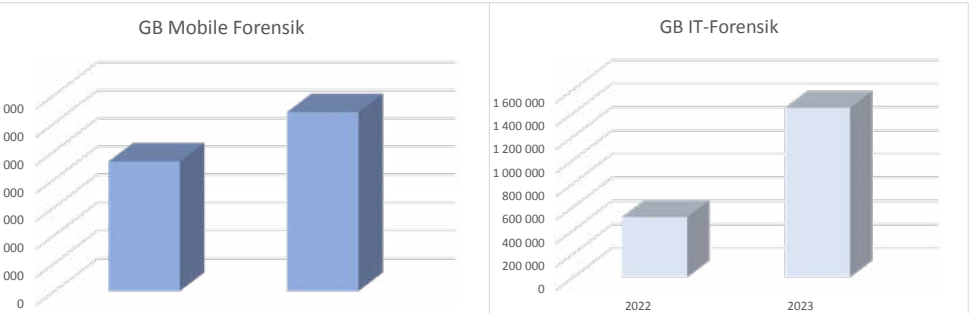

Abbildung 13:
Mobile Forensik
und IT-Forensik –
Gegenüberstellung der
ausgewerteten Datenmengen
der Jahre 2022 und 2023.

Das zeit- und ressourcenaufwendige Chip-Off-Verfahren, bei dem Memory-Chips von ihrer Hardware physisch entfernt werden, sowie der Bereich Kfz-Forensik, können nur zentral im C4 durchgeführt werden. Im Jahr 2023 konnten 139 Chip-Off-Verfahren durchgeführt werden.

Bei vielen schweren Straftaten sowie im Bereich der organisierten Kriminalität oder bei der grenzüberschreitenden Schwerkriminalität besteht ein direkter oder indirekter Bezug zu einem Kraftfahrzeug, wenn dieses als Transport- und/oder Tatmittel verwendet wurde. Dem Kraftfahrzeug kommt dabei ein hoher Stellenwert als Beweismittel zu. Die Informationen, die während des Betriebes automatisch generiert und gespeichert werden, können bei entsprechend fachgerechter Auswertung und Aufbereitung für kriminalpolizeiliche Ermittlungen und letztendlich für das Strafverfahren von enormer Bedeutung sein. Durch die Bediensteten des Fachbereiches Kfz-Forensik/Automotive IT des C4 werden bundesweit gerichtsverwertbare Beweisaufnahmen für alle Dienststellen des Bundesministeriums für Inneres und der Landespolizeidirektionen durchgeführt. Darüber hinaus wirken die Bediensteten der Kfz-Forensik aktiv an Schwerpunktaktionen und operativen Einsätzen mit, wenn die sofortige Sicherung von Beweismitteln notwendig erscheint und Anordnungen der Staatsanwaltschaften vollzogen werden müssen.

5.5 Entwicklung und Innovation

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

Eine der Aufgaben des Referates 4 - Entwicklung und Innovation - ist es, genau diese Unterstützung zu leisten. Dies umfasste im Jahr 2023 komplexe mathematische Analysen von Geldflüssen in diversen Kryptowährungen, Analysen von forensischen Artefakten, Entschlüsselungen von Daten und Datenträgern und zahlreiche andere Hilfestellungen. In mehreren Fällen wurden die Ermittlungen durch die Erstellung von Scripts und Tools unterstützt.

Bild 3: Entwicklung neuer Tools (© www.freepik.com)

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

Eine weitere Aufgabe des Referates 4 ist die Beobachtung und Analyse neuer Technologien auf ihre Bedeutung für die kriminalpolizeiliche Arbeit. Hier wurde einer der Schwerpunkte auf KI gesetzt. Speziell zu diesem Thema, aber auch in vielen anderen Bereichen, ist die Zusammenarbeit mit nationalen und internationalen Polizeiorganisationen, aber auch mit Forschungseinrichtungen, entscheidend. Deshalb wurde sowohl in mehreren nationalen als auch internationalen Projekten, Arbeitsgruppen und Gremien mitgearbeitet.

Speziell im Cybercrime-Bereich gewinnt die Präventionsarbeit immer mehr an Bedeutung, da sich zum Beispiel sehr viele Betrugsdelikte durch entsprechende Bewusstseinsbildung und daraus folgende Vorsicht verhindern ließen. Deshalb wurden auch im Jahr 2023 zahlreiche diesbezügliche Veranstaltungen von Ministerien, der Wirtschaftskammer und weiteren relevanten Organisationen mit Expertise unterstützt.

5.6 Wissensvermittlung durch Ausbildung und internationalen Austausch

Cyberkriminalität ist zu einer der größten Bedrohungen für die Gesellschaft geworden und erfordert eine entsprechende Reaktion seitens der Strafverfolgungsbehörden. Eine zentrale Komponente in diesem Kampf ist die Ausbildung von Polizeibeamtinnen und Polizeibeamten. 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 Polizeibeamtinnen und Polizeibeamte, die sich mit Cyberkriminalität befassen, unerlässlich. Dies umfasst nicht nur Kenntnisse über Computersysteme und Netzwerke, sondern auch über Verschlüsselungstechnologien, Forensik und digitale Beweissicherung. Ohne diese Kenntnisse können sie Schwierigkeiten haben, komplexe Cyberverbrechen zu verstehen und angemessen darauf zu reagieren. Eine fundierte Ausbildung ermöglicht den Polizeibeamtinnen und Polizeibeamten, die ihnen zur Verfügung stehenden Werkzeuge und Techniken voll auszuschöpfen, um Täter zu identifizieren und Beweise zu sammeln, die vor Gericht auch verwertbar sind.

Das C4 des Bundeskriminalamts führt bereits seit 2012 eine umfassende Ausbildung von Bezirks-IT-Ermittlerinnen und -Ermittlern durch. Mittlerweile unterstützen mehr als 350 speziell ausgebildete Kolleginnen und Kollegen durch fachgemäße Erstmaßnahmen und Ermittlungen auf lokaler Ebene. Die Vortragenden kommen vor allem aus den relevanten Fachbereichen des Bundeskriminalamts, der DSN, dem BAK sowie aus den Landeskriminalämtern.

Einem größeren polizeilichen Bereich wird das Thema Cybercrime zielgruppengerecht insbesondere im Rahmen der kriminaldienstlichen Aus- und Fortbildung sowie in den Grundausbildungslehrgängen zugänglich gemacht.

2023 wurde in enger Abstimmung mit dem Bundesministerium für Justiz eine eigene Ausbildungsreihe für Staats- und Bezirksanwältinnen und -anwälte und in der Folge auch für Richterinnen und Richter entwickelt, die im Sinne einer zielgerichteten Strafverfolgung speziell auf technische Hintergründe und hiermit einhergehende Ermittlungsmöglichkeiten im Cyber-Bereich abzielt. Ziel war es, einem möglichst großen Personenkreis Cybercrime-Grundkompetenzen zu vermitteln. Die Ausbildungen fanden jeweils in Form von Webinaren mit rund 18 Unterrichtseinheiten statt, wodurch es möglich war, einschlägiges kriminalpolizeiliches Fachwissen bundesweit an bis zu 250 Staatsanwältinnen und Staatsanwälte, 160 Bezirksanwältinnen und Bezirksanwälte sowie 85 Richterinnen und Richter weiterzugeben.

Bild 4:
„Symposium Neue Technologien“ (NT 2023) in Stuttgart, Deutschland (© Landeskriminalamt Baden-Württemberg)

Wissensvermittlung und Vernetzung findet selbstverständlich auch auf internationaler Ebene statt. So kamen im Mai 2023 rund 200 Expertinnen und Experten aus Wissenschaft, Wirtschaft und Sicherheitsbehörden bei dem vom C4 des Bundeskriminalamts mitorganisierten internationalen „Symposium Neue Technologien“ (NT 2023), um sich über die Auswirkungen der Digitalisierung auf die Kriminalitätsbekämpfung und die Arbeit der Polizei auszutauschen.

Unter dem Motto „Digitale Tools – Analoge Verbrechen: Und die Polizei?“ veranstalteten das Landeskriminalamt Baden-Württemberg, das C4 des Bundeskriminalamts, die schweizerische Bundespolizei fedpol und das Bayerische Landeskriminalamt gemeinsam das Symposium, das mittlerweile zum zehnten Mal stattfand.

Die äußerst erfolgreiche Veranstaltung umfasste zahlreiche Themen, von Extremismus und Hass im Netz bis hin zu Sprachmodellen der KI, Deep Fakes, Big Data, Predictive Policing und dem Metaverse. Expertinnen und Experten aus unterschiedlichen Disziplinen präsentierten ihre Erkenntnisse und vertieften sie in Diskussionsrunden.

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

Bei vielen Ermittlungen sind internationale Anfragen an Social-Media-Plattformen und ausländische Diensteanbieter im Internet erforderlich. In der Vergangenheit wurden diese von der jeweils ermittelnden Polizeidienststelle in Österreich selbst durchgeführt, jedoch gab es dazu keinen einheitlichen Prozessablauf und keine Handlungsanleitung. Durch unterschiedliche Rechtsauslegungen der Gesetzesmaterien kam es daher oftmals zu keiner Beantwortung der gestellten Anfrage beziehungsweise wurden langwierige Rückfragen seitens der Anbieter geführt. Solche Zeitverzögerungen wirkten sich nachteilig auf die Ermittlungen aus. Durch die gewonnenen Informationen mittels Provideranfragen können im Anlassfall, insbesondere bei Fällen schwerer Kriminalität, Täter rascher ausgeforscht werden. Aus diesem Grunde wurde das C4 beauftragt, eine zentrale Anfragestelle für Social Media und Online-Service-Provider, kurz ZASP, einzurichten. Das Ziel war einheitliche, klare und einfach geregelte Ablaufprozesse künftig zentral abzuwickeln und das dort gewonnene Know-how den ermittelnden Polizistinnen und Polizisten zur Verfügung zu stellen. Mit der Umsetzung des Projektes entstand eine verstärkte Unterstützung für die einzelnen Ermittlungsbereiche und es konnte ein höherer Output generiert werden. Ebenso plädierten zahlreiche Diensteanbieter ihrerseits aus-

drücklich auf eine zentrale Kontaktstelle in den jeweiligen europäischen Staaten, um die an sie gestellten Anfragen gezielter abarbeiten zu können. Die ZASP steht nicht nur im regelmäßigen Austausch mit Vertreterinnen und Vertretern der Social-Media-Anbieter, sondern ist auch Ansprechstelle für Anfragen aller Polizeidienststellen Österreichs und der Justiz.

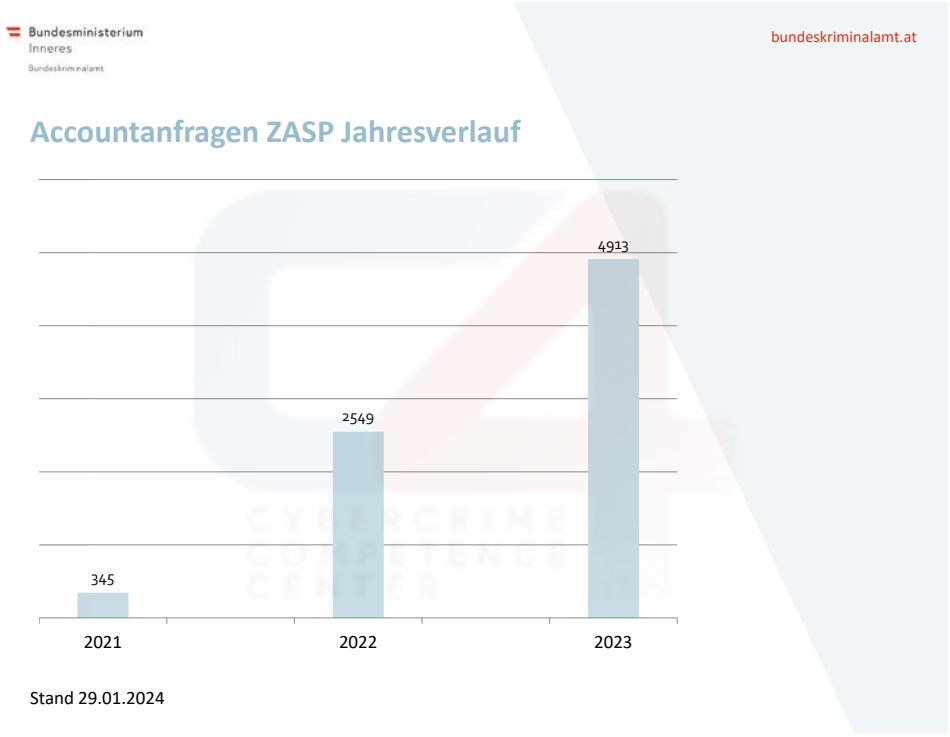

Abbildung 14: Accountanfragen im Jahresverlauf

Mit 1. September 2020 wurde im C4 ein Probebetrieb mit den Bundesländern Niederösterreich, Burgenland und Tirol sowie dem Bundesministerium für Justiz und dem Social-Media-Diensteanbieter Meta gestartet. Vor dem Start des Projekts gab es in Österreich 20 bis 40 Prozent positive Rückmeldungen von Online-Service-Providern. Durch das Vorhaben konnte die Quote positiver Beantwortungen deutlich gesteigert werden. Eine Entwicklung, die den internationalen Standards in diesem Bereich entspricht. Aufgrund positiver Evaluierung wurde der Probebetrieb mit 15. Februar 2022 in einen Vollbetrieb für das gesamte Bundesgebiet übergeleitet. Seit Oktober 2022 können auch Anfragen an Microsoft und seit August 2023 Anfragen an TikTok über die ZASP gestellt werden.

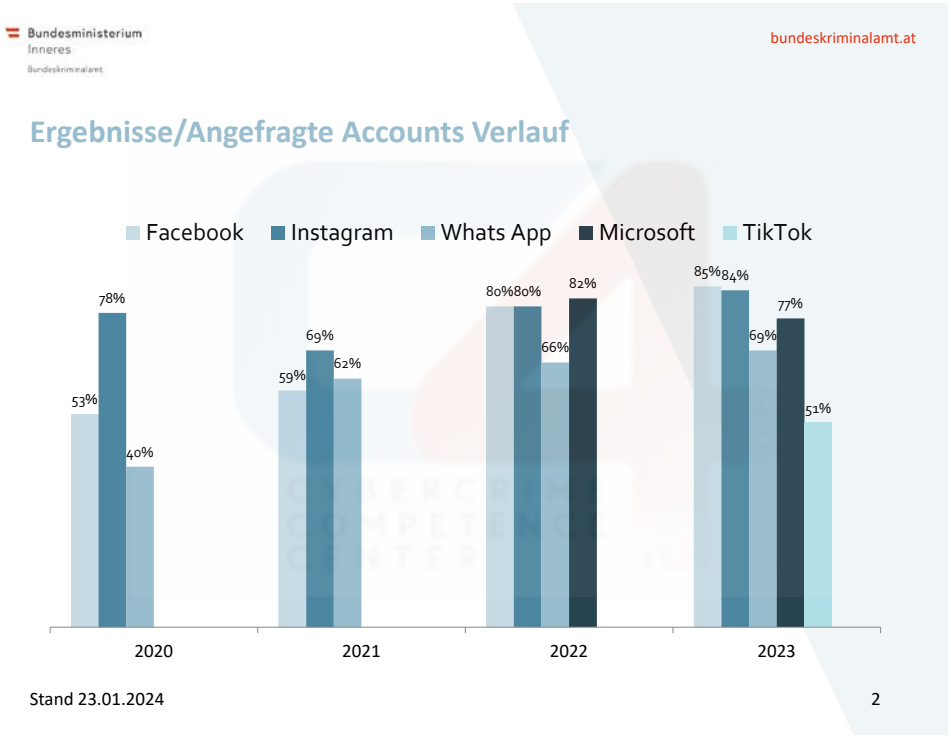

Abbildung 15: ZASP-Erfolgsquote im Jahresvergleich

2023 wurden insgesamt 3.331 Anträge über die ZASP abgewickelt und dabei 4.898 Accountanfragen gestellt. Im gleichen Zeitraum langte von Facebook zu 85 Prozent, von Instagram zu 84 Prozent, von WhatsApp zu 69 Prozent, von Microsoft zu 77 Prozent und von TikTok zu 51 Prozent ein Ergebnis aufgrund einer gestellten Accountanfrage ein.

Zu den Tatbeständen Betrug (2.695), Erpressung (1.180), Freiheit/Nötigung/gefährliche Drohung (191), Cybercrime im engeren Sinn (205) und sexuelle Integrität (90) wurden 2023 die meisten Accountanfragen gestellt.

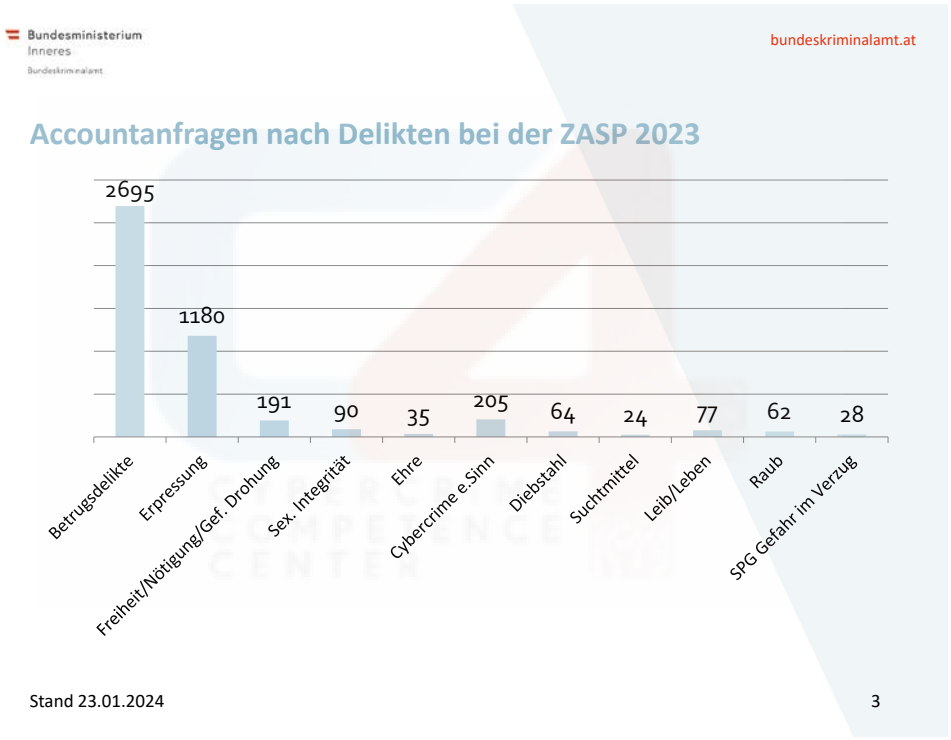

Abbildung 16: Accountanfragen nach Delikten 2023

Nach Etablierung der ZASP kann diese kriminalpolizeiliche Einheit als ein erfolgreiches Beispiel für zukunftsgerichtete Kooperationen zwischen Behörden und Kommunikationsplattformen angesehen werden.

So konnte im Mai 2023 eine Amokdrohung an einer Wiener Schule mit Hilfe der ZASP geklärt werden. Im November 2023 konnten Hinweise zu einem unbekannten Täter nach einem angekündigten Amoklauf über soziale Medien an einer Vorarlberger Schule eingeholt werden, nachdem durch die ZASP eine Anfrage beim Diensteanbieter eingereicht wurde. Weiters konnten ebenso mit Hilfe der ZASP sachdienliche Hinweise zu diversen Raubdelikten, Vergewaltigungen, Körperverletzungen und Sachbeschädigungen ermittelt 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

6 Rechtliche Herausforderungen aus Sicht der Kriminalpolizei

6.1 Anpassung des Cyber-Strafrechts

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

6.2 Datenschutz-Grundverordnung und „WHOIS" Abfragen

Domainnamen wie „www.bundeskriminalamt.at" machen Informationen im Internet leichter auffindbar. Die dafür benötigten Domänen können bei Registries und Registraren angemietet werden. „WHOIS"-Abfragen im Internet führten in der Vergangenheit häufig noch direkt zum Inhaber einer Domäne und zu einer technischen Kontaktperson. Diese Domainnamen zählen zu den Grundbausteinen des Internets. Personenbezogene Auskünfte sind für weiterführende Ermittlungen von hoher Bedeutung und waren bis zum Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 auch öffentlich zugänglich. Durch die Vielzahl von Registries und Registraren, die für die Verwaltung von Domainnamen zuständig sind, ergeben sich weitere Herausforderungen bei den Nachforschungen. Waren vormals nur einfache Abfragen in öffentlichen Datenbanken erforderlich, müssen bei Auskunftsersuchen an internationalen Standorten verwaltungstechnisch höchst aufwändige Prozesse durchlaufen werden. Diese erheblichen Ermittlungshürden werden als Folge der DSGVO auch in technischen und rechtlichen Gremien mit der Dachorganisation der Domänenverwaltung ICANN behandelt. Bis dato konnten keine von diesen Organisationen in Aussicht gestellten Konzepte final umgesetzt werden. Weitere Informationen: https://www.icann.org/public-comments/epdp-phase-2-addendum-2020-03-26-en.

6.3 Carrier Grade NAT-Problematik

Aufgrund der häufigen Nutzung der Carrier Grade NAT-Technologie, bei der mehreren Internetnutzerinnen und Internetnutzer zeitgleich idente IP-Adressen vom Netz Provider

zugewiesen werden, können viele Straftaten nicht geklärt und auch die Verfasserinnen und Verfasser von Hasspostings sowie Fakenews nicht ausgeforscht werden. Dies führt im Rahmen der Ermittlungen zu erheblichen Problemen bei der Zuordnung und Identifizierung krimineller Userinnen und Usern, wenn vom Netzanbieter die üblichen Protokollierungen beispielsweise aufgrund der fehlenden rechtlichen Rahmenbedingungen nicht gespeichert werden dürfen und daher nicht übermittelt werden können. Überdies gibt es international und auch auf europäischer Ebene selbst zwischen den einzelnen Mitgliedstaaten sehr große Unterschiede in deren rechtlichen Rahmenbedingungen zu dieser Thematik.

6.4 Pseudoanonyme Transaktionen von virtuellen Währungen

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

6.5 Sicherstellung von Mobiltelefonen ohne richterliche Bewilligung verfassungswidrig

Der Verfassungsgerichtshof (VfGH) hat in seinem Urteil vom 14. Dezember 2023 festgestellt, dass die Sicherstellung von Mobiltelefonen in Strafverfahren ohne eine vorhergehende richterliche Bewilligung verfassungswidrig ist. Dies verstoße gegen das Datenschutzgesetz und das Recht auf Privatleben. Grundrechtseingriffe müssen verhältnismäßig sein. Die Schwere des Eingriffs darf nicht größer sein, als die Bedeutung des Ziels, das erreicht werden soll. Grundsätzlich sei es ein legitimes Ziel, Datenträger sicherzustellen und auszuwerten, um Straftaten zu verfolgen. Auch stellt die rasche

Verbreitung neuer Kommunikationstechnologien die Kriminalitätsbekämpfung vor besondere Herausforderungen, doch entsprechen die angefochtenen Bestimmungen der Strafprozessordnung nicht den Anforderungen von § 1 Datenschutzgesetz und Art. 8 EMRK. Der VfGH ist der Ansicht, dass eine so weitgehende Maßnahme wie eine Sicherstellung von Datenträgern einer richterlichen Bewilligung bedarf. Nur so kann überprüft werden, ob die gesetzlichen Voraussetzungen für die Sicherstellung und Auswertung vorliegen und ob die Sicherheitsbehörden ihre Befugnisse einhalten. Gemäß VfGH-Urteil sind die §§ 110 Abs. 1 Z 1 und Abs. 4 sowie 111 Abs. 2 StPO daher als verfassungswidrig aufzuheben. Die Aufhebung tritt mit Ablauf des 31. Dezember 2024 in Kraft. Bis dahin ist die Gesetzgebung gefordert, die betreffenden Gesetzesstellen zu „reparieren". Für die Kriminalpolizei stellt sich vor allem die Gefahr von Beweisverlust, sollte hinkünftig nicht mehr das gesamte Endgerät gesichert werden dürfen. Es müsste bereits bei der Sicherung von Daten, bei der noch keine Analyse des Datenbestandes angestellt wird, eine Einschränkung stattfinden. Es besteht dadurch die Gefahr, dass bei Vorhandensein mehrere Applikationen, die demselben Zweck dienen (beispielsweise E-Mail-Applikationen unterschiedlicher Anbieter wie GMX, Yahoo, Microsoft), nicht alle applikationsspezifischen Daten mitgesichert werden. Eine Einschränkung auf spezielle Applikationen und Datentypen kann stattdessen im Zuge der Datenaufbereitung stattfinden.

6.6 Vorratsdatenspeicherung

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

7 Exkurs: Cyber-Kompetenz & Cybersicherheitsvorfälle

Im Zuge eines großen Cybersicherheitsvorfalles in Kärnten wurde das Thema Cyber-Kompetenz sowie die korrekte und professionelle Bearbeitung entsprechender Sachverhalte in den Fokus gerückt. Anlassbezogen wurden im Zuge einer Kooperation zwischen der Direktion Staatsschutz und Nachrichtendienst (DSN) sowie dem LKA Kärnten zwei Projekte gestartet, die sich mit dieser Thematik beschäftigen. Eines der beiden Projekte hat dabei den Schwerpunkt auf die Vermittlung von Cyber-Kompetenz im Bereich betreffender Organisationen – und dort vor allem im Bereich von Führungskräften und Leitungspositionen – gelegt. Das zweite Projekt beschäftigt sich mit der Bearbeitung von Cybersicherheitsvorfällen und deckt fachlich fundiert alle Schritte ab, die die Polizei beim ersten Angriff prioritär bearbeiten und prüfen muss, um eine korrekte Sicherstellung von digitalen Beweismitteln sowie die professionelle Durchführung des Einsatzes sicherstellen zu können.

7.1 Cyber-Kompetenz

Große Unternehmen und Organisationen weisen eine Vielzahl an Bedürfnissen auf. So finden sich dabei die unterschiedlichsten Disziplinen wie Qualitätsmanagement, Risikomanagement oder Prozessmanagement. Eine Disziplin „Cybermanagement" findet sich jedoch meistens nicht. Durch Cybersicherheitsvorfälle wie bei Angriffen mittels Ransomware können Unternehmen und Organisationen schwer und nachhaltig beeinträchtigt werden.

Ursache großangelegter Angriffe können sowohl Lücken im Bereich der IT-Security wie auch menschliche Schwachstellen sein, die täterseitig durch den gezielten Einsatz von Social Engineering ausgenutzt werden. Ebenso oft liegt der Problematik auch das Fehlen einer gewissen Cyber-Kompetenz in den Reihen der Entscheidungsträgerinnen und Entscheidungsträger zugrunde. Aber was ist Cyber-Kompetenz überhaupt und wie kann sie dabei helfen, derartige Herausforderungen zu managen? Cyber-Kompetenz beschreibt das tiefergehende Verständnis hinsichtlich der Entwicklungen, Problemstellungen, Möglichkeiten und Grenzen der Digitalisierung.

Sie hat direkten Bezug zu den Bereichen Cybersicherheit und Cyberkriminalität. Wie im nachfolgenden Aufbau zu erkennen ist, stellen einfache Kenntnisse und das Erlangen einer gewissen Awareness die Grundlagen dar, die allen Mitarbeiterinnen und Mitarbeitern nähergebracht werden sollte. Im mittleren Cyber-Kompetenz-Bereich liegen bereits ein erhöhtes Fachwissen und Fertigkeiten vor, um den Herausforderungen der Digitalisierung besser gewachsen zu sein.

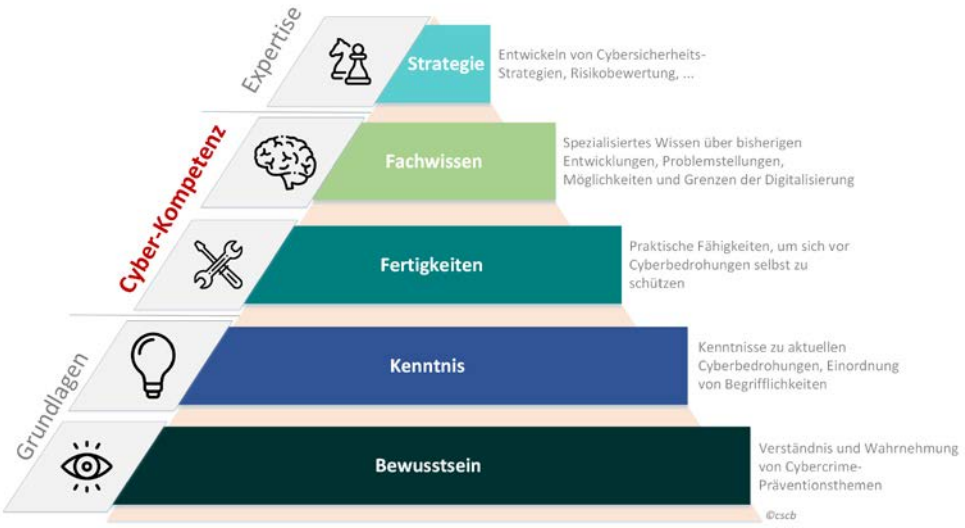

Abbildung 17:
Die verschiedenen Ebenen der Cyber-Kompetenz

Operative und strategische Cyber-Entscheidungen sollten daher nur dann getroffen werden, wenn auch die entsprechende Kompetenz vorliegt. Ein Mangel kann sich in vielen Bereichen negativ auswirken, zu erheblichen Problemen und Sicherheitsschwachstellen bis zum gänzlichen Stillstand eines Unternehmens oder einer Organisation führen.

Cyber-Kompetenz muss dabei vor allem zuerst „Top-down" aufgebaut werden und bei den Führungskräften beginnen, da diese einen maßgeblichen Einfluss auf viele Bereiche im Unternehmen beziehungsweise der Organisation haben. Ein Fehlen von entsprechender Cyber-Kompetenz kann zu den unterschiedlichsten Problemen führen. Diese Probleme können überall zutage treten, beispielsweise im Finanz- oder Logistikbereich, bei der Beschaffung von Gütern und Dienstleistungen.

Die einschlägige Schulung von Mitarbeiterinnen und Mitarbeitern ist ein wichtiges Thema und bildet die Basis im Kampf gegen Cyberkriminalität und bei der Erreichung einer besseren IT-Sicherheit in Unternehmen. Unter Umständen werden durch Entscheidungsträgerinnen oder Entscheidungsträger verursachte Fehler bei fehlender Cyber-Kompetenz nicht erkannt und führen dann langfristig zu großen Problemen. Aus diesem Grund muss das Initiieren von Cyber-Kompetenz gesamt-organisatorisch erfolgen, um langfristige Erfolge in diesem Bereich sicherzustellen.

Cyber-Kompetenz ist dabei aber nicht nur eine Angelegenheit der jeweiligen IT-Abteilung, sondern eine Aufgabe für die gesamte Organisation. Alle Mitarbeiterinnen und Mitarbeiter tragen zur Cybersicherheit bei und müssen entsprechend regelmäßig geschult und sensibilisiert werden. Praktische und theoretische Ausbildungen, Zertifizierungen,

Simulationsübungen und Awareness-Kampagnen können dabei wirksame Instrumente darstellen. Die Folgen von falschen, kurzfristigen operativen Entscheidungen können in der Regel zeitnah repariert oder ausgeglichen werden, da die Effekte dieser Handlungen zumeist unmittelbar sichtbar sind. Die Auswirkungen falscher strategischer Entscheidungen machen sich jedoch erst viel später bemerkbar und können oft viel schwerer korrigiert werden.

7.2 Cybersicherheitsvorfälle

Unter einem Cybersicherheitsvorfall versteht man den intentionalen Angriff auf die Vertraulichkeit, Verfügbarkeit und/oder die Integrität von Daten oder IT-Systemen im großen Ausmaß. Zur Sicherstellung einer professionellen Strafverfolgung ist die Polizei als Sicherheitsbehörde auf eine korrekte Sicherung von digitalen Beweismitteln angewiesen. Damit im Zuge der Erstbearbeitung alle Beweismittel für die spätere Bearbeitung und Strafverfolgung korrekt und vollständig vorliegen, ist es wichtig, bereits von Anfang an die korrekten Fragen zu stellen und richtigen Maßnahmen zu treffen. Dabei können Cybersicherheitsvorfälle nicht nur im Bereich der kritischen Infrastruktur auftreten, die Zuständigkeit liegt bei der Direktion Staatsschutz und Nachrichtendienst und den Landesämtern Staatsschutz und Extremismusbekämpfung“ (LSE), sondern auch in anderweitigen Unternehmen oder Organisationen, die dann in den Zuständigkeitsbereich der Polizeiinspektionen und des jeweiligen Landeskriminalamts fallen.

Neben den obligatorischen Erstmaßnahmen gibt es bei betroffenen Unternehmen und Organisationen sehr oft Missverständnisse hinsichtlich des Umfangs und der Art und Weise polizeilicher Arbeit im Bereich von Cybersicherheitsvorfällen. Eine genaue Kenntnis darüber ist jedoch im Ernstfall entscheidend, um eine schnellstmögliche und professionelle Hilfeleistung sicherstellen zu können und auch als Betroffener selbst richtig reagieren zu können. Die Polizei führt im Zuge dieser Erstmaßnahmen alles durch, was für eine korrekte Strafverfolgung und Ausforschung der Täter erforderlich ist. Dazu gehören zum Beispiel digitale Ermittlungen, digitale Forensik und klassische Ermittlungsarbeit. Auch Cyber-Prävention und interne Verständigungen (Berichtspflichten) fallen in den Zuständigkeitsbereich der Polizei.

Auf der anderen Seite gibt es jedoch viele Aufgaben, die im Verantwortungsbereich des betroffenen Unternehmens/Organisation verortet sind. Dazu gehören beispielsweise die Entschlüsselung von Daten, die durch Ransomware kompromittiert wurden, sowie die Schulung und das Training von Mitarbeiterinnen und Mitarbeitern im Hinblick auf deren Cyber-Kompetenz. Auch Meldepflichten wie Meldungen an die Datenschutzbehörde oder

die NIS-Behörde fallen in die Zuständigkeit des betroffenen Unternehmens beziehungsweise der Organisation. Wichtig ist aber vor allem, dass sich gefährdete Unternehmen und Organisationen schon lange vor einem Cybersicherheitsvorfall mit dem möglichen Szenario beschäftigen und Vorkehrungen treffen. Dazu gehören zum Beispiel analoge Notfalllisten mit wichtigen Ansprechpartnerinnen und -partnern und Sicherheitsunternehmen, die Implementierung eines entsprechenden Risikomanagements und dergleichen.

Seitens des BMI wurde ein eigener Folder aufgelegt, der sich mit Cyber-Sicherheitsvorfällen beschäftigt und woraus sich die wichtigsten Maßnahmen und Empfehlungen ergeben, um im Fall des Falles rechtzeitig die korrekten Entscheidungen zu treffen und so das eigene Unternehmen/die eigene Organisation vor unnötigen Schäden bestmöglich schützen zu können und überdies eine effiziente Strafverfolgung sicherstellen zu können.

Über den nachfolgenden QR-Code kann der Folder in digitaler Form heruntergeladen werden:

8 Kooperation und Kriminal-prävention

8.1 Cybercrime-Prävention: Die nächsten Schritte

Die Auswirkungen neuer technologischer Errungenschaften zeigen sich im Alltag als zweischneidiges Schwert. Einerseits tragen Innovationen im Online-Bereich maßgeblich zur Lebensqualität der Bürgerinnen und Bürger bei, andererseits eröffnen sie kriminellen Vorhaben neue Wege und Möglichkeiten. Tätern ist es möglich, weltweit und jederzeit auf Online-Systeme zuzugreifen und ihre Modi Operandi flexibel neuen Gegebenheiten anzupassen.

In diesem Zusammenhang wurde im Jahr 2023 die BMI-interne Strategie „Sicheres Internet" ausgearbeitet, mit der einerseits existierende Präventionsmaßnahmen für den Online-Bereich gebündelt und andererseits erste Schritte für die Entwicklung und Umsetzung neuer Maßnahmen gesetzt wurden. Die stattfindende Zusammenarbeit mit relevanten Organisationen verstärken bereits jetzt die Möglichkeit breiter Informationskampagnen, um der Bevölkerung die größtmögliche Unterstützung zum Schutz vor einschlägigen Delikten im Online-Bereich zur Verfügung zu stellen.

Mit dem Programm „UNDER 18" steht für Kinder und Jugendliche im schulischen Setting eine Möglichkeit zur Verfügung, insbesondere auf Online-Delikte einzugehen. Cyber-Mobbing, Sextorsion und Grooming sind nur einige der Delikte, mit denen sich Kinder und Jugendliche konfrontiert sehen. Das Programm bietet die Möglichkeit, im geschützten Rahmen zu lernen und sich der Gefahren wie auch des Nutzens der digitalen Welt bewusst zu werden. Eine im Programm enthaltene Information für das Lehrpersonal sowie ein Elternabend tragen dazu bei, mögliche Probleme und Gefahren auf mehreren Ebenen zu erkennen und Unterstützung zu leisten.

Für geplante Informationsveranstaltungen sowie Vorträge und Wissenstransfer jeder Art stehen in den Bundesländern geeignete und spezifisch ausgebildete Präventionsbeamtinnen und -beamte zur Verfügung. Diese können über die Landeskriminalämter kontaktiert werden und vor Ort Aufklärung und Unterstützung gewährleisten. Dieses Angebot richtet sich an die gesamte Bevölkerung und kann von Privatpersonen gleichfalls in Anspruch genommen werden wie von Unternehmen oder der öffentlichen Verwaltung.

Präventionstipps

Bleiben Sie unbekannten Personen gegenüber misstrauisch:

- Wenn Sie etwas verkaufen, müssen Sie keine Bezahldetails von sich angeben!
- Wenn Sie ein Familienmitglied unter einer neuen Telefonnummer mit Forderungen nach Geld an Sie wendet, überprüfen Sie die alte Rufnummer oder andere Kontakte!
- Bedenken Sie: Wenn Sie etwas verkaufen, fallen keine Kosten für Versicherung oder Ähnliches an!
- Bestätigen Sie keine Autorisierungsnachrichten (Push-Nachrichten) Ihres Bank-Anbieters, wenn Sie etwas verkaufen!
- Nutzen und überprüfen Sie die von den Kleinanzeigenplattformen empfohlenen Bezahldienste und keine unbekannten Links, deren Herkunft nicht zweifelsfrei feststeht!
- Machen Sie sich mit den auf Kleinanzeigenplattformen angebotenen Bezahldiensten vertraut!
- Ist ein Schaden entstanden, verständigen Sie sofort ihr Banküberweisungsinstitut oder ihren Kreditkartenanbieter und ersuchen Sie um Rückbuchung. Erstatten Sie Anzeige bei der nächsten Polizeidienststelle!
- Bedenken Sie: Die sicherste Bezahlform ist die persönliche Übergabe vor Ort!

Mehr Infos zu gängigen Betrugsformen finden Sie hier:
https://www.bundeskriminalamt.at/202/Betrug_verhindern/start.aspx

8.2 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), rufen Sie den Polizeinotruf 133 an.

Stellen Sie bitte fallrelevante(s) Beweismittel/Datenmaterial wie E-Mails, Chat-Verläufe, Zahlungsbelege, Screenshots, digitale Fotos oder Videos 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 Originalmail 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 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 können.

Wenn es sich um komplexere Tathandlungen handelt, dokumentieren Sie den Tathergang in chronologischer Reihe 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 Daten sind 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 Anzeigeerstattung über die Meldestelle nicht vorgesehen.

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

9 Strategie und Ausblick

Cyberkriminalität ist ein schnell wachsender und sich schnell verändernder Deliktsbereich, der großes Knowhow aller involvierten Kolleginnen und Kollegen verlangt. Folglich muss in den kommenden Jahren die Ausbildung im Cyberbereich weiter forciert werden, das Knowhow bei allen Strafverfolgungsbehörden bis zur Polizeidienststelle verbessert und die Gesellschaft im Umgang mit neuen Technologien zur Wahrung ihrer Sicherheit sensibilisiert werden. Im Rahmen der geplanten Kriminaldienstreform sind sowohl auf Landes- als auch auf regionaler Ebene die entsprechenden organisatorischen Anpassungen zur verbesserten Bekämpfung der Cyberkriminalität vorgesehen und die Einrichtung mehrerer Cybercrime-Trainingscenter angedacht. Dies wurde in Oberösterreich bereits erfolgreich erprobt. Ziel der größten Reform des Kriminaldienstes seit 20 Jahren ist es, die Kriminalitätsbekämpfung weiterzuentwickeln und den Dienst zu modernisieren. Der Bereich der Cyberkriminalität bildet hierbei einen Arbeitsschwerpunkt, auf dem ein besonderer Fokus liegt.

Ein strategischer Schwerpunkt umfasst wie auch in den Vorjahren, die Stärkung der nationalen und internationalen Zusammenarbeit zwischen staatlichen Behörden, maßgeblichen Organisationen und relevanten Unternehmen. Der weitere Ausbau eines innovationsgetriebenen Netzwerkes von Strafverfolgungsbehörden, wissenschaftlichen Einrichtungen und privatem Sektor zur Bekämpfung der Cyberkriminalität soll gerade auf EU-Ebene vorangetrieben werden. Unter Zuhilfenahme von durch Forschungsaktivitäten erzielten Ergebnissen sollen Lösungen erarbeitet werden, die dazu beitragen, die Komplexität der Cyberkriminalität zu bewältigen. Oberstes Ziel bleibt weiterhin die schnelle Erkennung krimineller Phänomene zum Zwecke der Strafverfolgung und zum Schutz der Bevölkerung.

Die Einsatzmöglichkeiten KI sollen im Bereich der Strafverfolgungsbehörden weiter ausgelotet werden. Ebenso sollen Empfehlungen für die Implementierung von Innovationen generiert und diese, dort wo erforderlich und rechtlich möglich, eingesetzt werden.

Hinsichtlich der Umsetzung der europäischen Cybersicherheitsrichtlinie (NIS2), die bis Herbst 2024 in nationales Recht umgesetzt werden muss, versteht sich das Bundesministerium für Inneres als Partner der heimischen Betriebe. Die EU-Richtlinie reguliert, wie Unternehmen, die für das Funktionieren des Staates relevant sind, sich auf potenzielle Cyberattacken vorbereiten beziehungsweise mit Cybercrime-Vorfällen umgehen müssen. Bereits im Vorjahr wurde ein breiter Einbindungsprozess mit den von NIS2 betroffenen Unternehmen gestartet und relevante Stakeholder ins Boot geholt, um Österreich noch cybersicherer zu machen.

Auf europäischer Ebene sollten endnutzerorientierte Vorhaben, die darauf abzielen, eine Struktur zu schaffen, um Beamtinnen und Beamten im Bereich der Strafverfolgung und öffentlichen Sicherheit brauchbare Tools zur Verfügung zu stellen, weiter betrieben und ausgebaut werden.

Nach der erfolgten Anpassung rechtlicher Rahmenbedingungen und einer Erhöhung des Strafrahmens maßgeblicher Paragrafen zur Internetkriminalität, muss die Entwicklung mittelfristig genau beobachtet und im Hinblick auf ihre Auswirkungen evaluiert werden. Eine Aktualisierung der Konzepte zur Bekämpfung von Cybercrime ist laufend vorzunehmen, um auf kurzfristig auftretende Trends zielgerichtet reagieren zu können.

Auf Ebene des C4 wurden im Jahr 2023 sowohl der Bereich der IT-Ermittlungen wie auch der digitalen Beweismittelsicherung (IT-Forensik) personell verstärkt. Die Personalakquise blieb auch 2023 herausfordernd. Eine Tatsache, mit der die Kriminalpolizei in der Cybercrime-Bekämpfung seit Jahren konfrontiert ist. Die Umstrukturierung des Büros 5.2 zur Abteilung 5 „Cybercrime Competence Center“ mit sechs Büros wird aller Voraussicht nach 2024 erfolgen. Für die räumliche Unterbringung und Bereitstellung der technischen Infrastruktur wurde dementsprechend vorgesorgt. Sämtliche Vorbereitungsmaßnahmen sind bereits abgeschlossen.

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

Ende 2022 wurde eine direkte Schnittstelle zwischen den Ersteinschreiterinnen und Ersteinschreitern und dem C4 geschaffen, die es ermöglicht, relevante Informationen und Spuren aus dem digitalen Raum zeitnah zu übermitteln. Dies ist vor allem in Hinblick auf die Sicherung flüchtiger Daten im Zusammenhang mit Phishing oder Malware von essenzieller Bedeutung, um valide Ermittlungsansätze möglichst schnell zu erhalten. Die in diesem Zusammenhang entstandenen technischen Möglichkeiten wurden im Laufe des Jahres 2023 ausgebaut.

10 Strategy and Prospects (English)

Cybercrime is a rapidly growing and rapidly changing crime area, requiring a great know-how of all colleagues involved. For this reason, advanced cybercrime training has to be reinforced in the following years, the knowhow within all law enforcement authorities and all police units has to be enhanced and awareness must be raised in our society in order to remain safe when dealing with new technologies. In the framework of the planned criminal policing reform, appropriate organizational adjustments to improve the fight against cybercrime are planned at both the state and regional levels, and the establishment of several cybercrime training centres is contemplated. This has already been successfully tested in Upper Austria. It is the goal of this largest reform of criminal policing in 20 years to further develop the fight against crime and modernize the service. The area of cybercrime is one of the main focuses of this work, to which special attention is paid.

As in previous years, a strategic focus includes strengthening national and international cooperation between government agencies, and relevant organizations and companies. The further expansion of an innovation-driven network of law enforcement agencies, scientific institutions and the private sector to combat cybercrime is to be expedited, especially at the EU level. Using the results obtained through research activities, solutions will be developed to help manage the complexity of cybercrime. Primary goal remains the rapid detection of criminal phenomena for the purposes of law enforcement and public protection.

The potential applications of artificial intelligence are to be further explored in the area of law enforcement. Likewise, recommendations for the implementation of innovations are to be generated and used where necessary and legally possible.

At the European level, end-user-oriented projects aimed at creating a structure to provide usable tools to law enforcement and public security officers should be pursued and developed.

Following the adjustment of the legal framework and an increase in the range of penalties for relevant paragraphs on cybercrime, developments must be closely monitored in the medium term and evaluated in terms of their impact. The concepts for combating cybercrime must be updated on an ongoing basis in order to be able to respond to short-term trends in a targeted manner.

Within the C4 staffing levels were increased in 2023 in the areas of IT investigations as well as the preservation of digital evidence (IT forensics). Staff acquisition remained challenging in 2023, which is a fact that criminal investigation fighting cybercrime has faced for years.

The restructuring of the sub-department 5.2 into the Department 5 “Cybercrime Competence Center”, with six sub-departments is envisaged for 2024. Accordingly, provisions have been made for the spatial accommodation and technical infrastructure. All preparatory measures have already been completed.

The development of a national, modern technical infrastructure for the criminal investigation sector has been underway for some time. As early as 2021, a project called „SeILE“ (creation of an ICT solution for special criminal investigations) was launched with the involvement of the Ministry of Justice and on the basis of the recommendations of the Court of Audit. This project aims to establish an ICT solution for all those criminal investigation and forensic activities that cannot be carried out in the current digital environment of the Ministry of the Interior for justified security considerations.

At the end of 2022, a direct interface was created between the initial investigators and the Cybercrime Competence Center, which makes it possible to transmit relevant information and traces from the digital space in a timely manner. This is of essential importance, especially with regard to securing volatile data in connection with phishing or malware, in order to obtain valid investigative approaches as quickly as possible. The technical possibilities created in this context were expanded over the course of 2023.

11
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)

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

Behördenwallets

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

Bitcoin

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

Caller-ID-Spoofing

Um ihre wahre Identität zu verschleiern, manipulieren die Kriminellen bei den Betrugsanrufen ihre Telefonnummer. Bei Anrufen eine falsche Nummer anzuzeigen, ist relativ leicht und mit wenig technischem 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 Kriminellen benötigen damit kein tiefgreifendes technisches Wissen zur Straftatbegehung, sondern kaufen sich das fehlende Wissen zu.

Collége 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.

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, den so genannten URL, aufgerufen werden. Um in das Darknet, beispielsweise das Tor Netzwerk, zu gelangen, benötigt man einen speziellen Browser, beispielsweise 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 zu Kindesmissbrauch-Online und weit darüber hinaus.

DDoS-Angriffe

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

Domain Name System (DNS)

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

European Cybercrime Center (EC3)

Das EC3 ist ein Teil von Europol und wurde eingerichtet, um den Mitgliedsstaaten in folgenden drei Bereichen eine signifikante Unterstützung zu bieten:

- Bekämpfung von Cybercrime, begangen durch organisierte Gruppierungen, die beispielsweise durch Online-Betrug große Geldmengen erbeuten.
- Bekämpfung von Formen von Cybercrime, die die Opfer massiv schädigen, beispielsweise sexueller Missbrauch von Kindern.
- 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 dem Internet zu blockieren.

IKT

Der Begriff Informations- und Kommunikationstechnologie (Abkürzung: IKT; alternativ auch IuK) bezeichnet eine 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 sind und mittlerweile als aufgebraucht gelten.

Kryptowährungen und Blockchain

Kryptowährungen sind digitale Zahlungsmittel, die auf verschlüsselten Datensätzen basieren. Mit dieser Form der Zahlungsmittel ist ein digitaler Zahlungsverkehr ohne ein dazwischen geschaltetes 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 und illegalen

Bezahlvorgängen zu beobachten. Insbesondere im Bereich Cybercrime haben sich „Cryptos“, vor allem bei Massenerpressungsmails 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 Form des Internetbetrugs, der sowohl Frauen als auch Männer betreffen kann. Die Kriminellen stellen meist den ersten Kontakt per E-Mail oder über soziale Medien her und versuchen, eine Vertrauensbasis durch zum Beispiel das Zusagen von persönlichen Treffen zu schaffen. In Folge der elektronischen Kommunikation versuchen die Kriminellen ihre Opfer zum Übersenden von Geld und Wertgegenständen zu überreden, indem eine Notsituation vorgetäuscht wird. Tatsächlich existiert die dargestellte, geliebte Person aber nicht, sondern dient nur als Tarnung. Die Kriminellen schrecken dabei auch nicht davor zurück, die Identität und den Internetauftritt von realen Personen dafür zu missbrauchen.

Malspam

Bei Malspam beziehungsweise „Malicious Spam“ handelt es sich um Spam-E-Mails, die zur Verbreitung von Schadsoftware dienen. Diese E-Mails können bereits Schadsoftware oder schädliche Elemente wie Dropper, Downloader beinhalten, die als JavaScript versteckt in komprimierten Dateien oder anderen Datenformaten eingebettet ist. Diese E-Mails können aber auch „nur“ einen Link enthalten, der aktiv von der Empfängerin oder vom Empfänger angeklickt werden muss, damit die schädlichen Komponenten auf dem Gerät installiert werden.

Money Mules

Wie die deutsche Übersetzung der Bezeichung 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 dem Geldwäscheprozess beteiligt ist. Die Anwerbung erfolgt oft über E-Mail.

Network Address Translation (NAT)

Bei Carrier Grade NAT teilt der Provider eine IPv4-Adresse aus dem privaten Adressbereich „10.0.0.0/8“ den Endkundenanschlüssen zu – keine „öffentliche IP-Adresse“ (§ 92 Abs 3 Z 16 TKG). Auf diese Weise spart er mittlerweile sehr rare öffentliche IPv4-Adressen. Zwischen dem privaten Provider-Netz und dem öffentlichen IPv4-Netz vermittelt dann die NAT oder Port Address Translation (PAT). Der dafür zuständige vermittelnde Server kümmert sich um die Adressübersetzung zwischen den privaten und öffentlichen IPv4-Adressen und reicht

die Pakete zwischen den Netzwerken weiter. NAT wurde ursprünglich für lokale Netzwerke wie dem 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, beispielsweise 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 Cyberangriffen verleiten 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 Anrufen mit falschen Identitäten.

Spam

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

Stablecoins

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

Stranded Traveller Scam

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

Trojaner (Trojanisches Pferd)

Als Trojanisches Pferd bezeichnet man ein Computerprogramm oder eine Applikation, das oder die 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)

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

Virus

Bei (Computer-)Viren handelt es sich um die älteste Art von Schadsoftware, die sich selbst 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 ist. Die Umkehrtransformation, das heißt die Zurückgewinnung des Klartextes aus dem Geheimtext, wird Entschlüsselung genannt.

Wallet

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

WHOIS

WHOIS ist ein Service im Internet, der vor allem zur Abfrage von Daten zu Domainnamen genutzt wird. Vor der DSGVO war es uneingeschränkt möglich, Eigentümerinnen und Eigentümern, Ansprechpartnerinnen und Ansprechpartnern 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