Bundesministerium
Inneres

Bundeskriminalamt

Cybercrime Report 2022

Lagebericht über die Entwicklung von Cybercrime

Cybercrime Report 2022

Lagebericht über die Entwicklung von Cybercrime

Wien, im Mai 2023

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres, Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
+43 1 24836 985025
Bundeskriminalamt.at
Autor: MR Klaus Mits
Fotonachweis: BMI/Bundeskriminalamt
Layout: Armin Halm
Druck: Digitalprintcenter des BMI, Herrengasse 7, 1010 Wien
Wien, im Mai 2023

Vorwort

Die zunehmende Digitalisierung unseres Lebens ist zum einen ein großer Segen, zum anderen bergen die Fortschritte der Technologie aber natürlich auch ihre Gefahren. Jede mit noch so guter Absicht entwickelte Software kann zweckentfremdet werden und durch das professionelle und adaptive Verhalten der Kriminellen eine Gefahr für die Informations- und Kommunikationstechnik an sich darstellen, oder aber auch als Mittel zum Zweck verwendet werden, um klassische Delikte in den digitalen Raum zu verlagern.

Mit dem nachfolgenden Cybercrimereport stellen wir Ihnen Informationen zu aktuellen Bedrohungslagen und diversen Deliktsformen zur Verfügung. Außerdem bringen wir Licht in den oft undurchsichtigen Dschungel des Internets, indem wir die gängigsten Termini für Sie aufbereitet haben.

In diesem umfassenden Feld der Cyberkriminalität sind unsere strategischen Ziele zum einen die Verbesserung der Rahmenbedingungen zur Eindämmung von Cybercrime sowie die Bewusstseinsbildung und Förderung der Eigenverantwortung bei der Nutzung des Internets. Zum anderen sind es die Bereitstellung von personellen, technischen und logistischen Ressourcen zur zielgerichteten Bekämpfung von Cybercrime sowie die Stärkung der Resistenz gegen kriminelle Cyberangriffe auf die Wirtschaft und schnelle, wirksame Reaktionen auf solche Vorfälle.

Es gilt, sich sowohl national als auch international zu vernetzen und die gemeinsame Kooperation zu forcieren, um den Tätern jeden Tag aufs Neue aufzuzeigen, dass das Internet kein rechtsfreier Raum ist. Die Umsetzung von EU-Cybersicherheitsstrategien sowie nationalen Strategien des Bundeskanzleramts und des Bundesministeriums für Inneres zeigen, dass wir am richtigen Weg sind, eine einheitliche Legistik im Kampf gegen die Cyberkriminalität zu entwickeln. Dadurch können wir die bereits gut funktionierenden Systeme und Ansätze, aber auch unsere täglichen Ermittlungen noch weiter verbessern und noch professioneller werden.

Unser Dank gilt allen Ermittlerinnen und Ermittlern, die tagtäglich unermüdlich im Einsatz sind, um Cyberkriminelle auszuforschen und vor Gericht zu bringen und unseren Partnerinnen und Partnern, die gemeinsam mit der Polizei an einem soliden und stetig wachsenden Sicherheitsnetzwerk arbeiten.

Ihr

Mag. Gerhard Karner, Bundesminister für Inneres, Mag. Dr. Franz Ruf, MA, Generaldirektor für die öffentliche Sicherheit und General Mag. Andreas Holzer, MA,Direktor des Bundeskriminalamtes

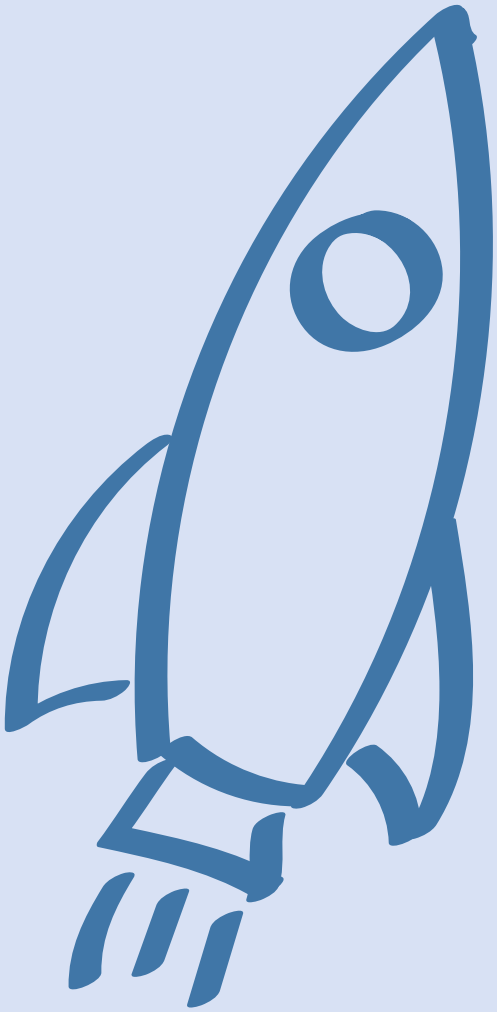
Mag. Gerhard Karner
Bundesminister für Inneres

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

Mag. Andreas Holzer, MA
Direktor des Bundeskriminalamtes

Inhalt

1 Einleitung



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

Die Ergebnisse aus den Analysen basieren auf Informationen, die in der fachlichen Zentralstelle des Bundeskriminalamtes, dem Cybercrime Competence Center (C4), zusammenlaufen, wie den gesammelten Meldungen, Anzeigen, Statistiken aus internationalen Kooperationen, Informationsaustausch mit Mitgliedsstaaten, Ausbildungen, Positionspapieren sowie Studien von Dritten. Die Bestandsaufnahme der quantitativen Daten und qualitativen Inhaltsanalysen fand zu Beginn des Erscheinungsjahres statt, da auf die Verfügbarkeit der Daten von Jänner bis Dezember 2022 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 erneut hohen Anstiegs von Cybercrime-Delikten (plus 30,4 Prozent im Vergleich zum Vorjahr) und einer damit einhergehenden abnehmenden Aufklärungsquote (minus drei Prozentpunkte) konnten im Jahresvergleich bei absoluter Betrachtung mehr als 3.300 Straftaten zusätzlich aufgeklärt werden.

Die Personalrekrutierung von IT-Fachleuten für die geplante Reform des C4 gestaltete sich auch im Berichtsjahr mit den bestehenden Ressourcen als herausfordernd und führte zu einer Fokussierung im internen Wissensaufbau durch zahlreiche pandemiebedingte Online-Schulungen und dem Entwurf neuer Ausbildungskonzepte.

Die Aufbauorganisation und ihre Abläufe sind aufgrund der technischen Komplexität mit ständigem Wissensaufbau 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 vermehrte Eigenverantwortung der Bürgerinnen und Bürger und auf präventive Maßnahmen als Schwerpunkt gesetzt. Deshalb werden im Bericht die wichtigsten Phänomene im Detail genannt, fallweise mit vorbeugenden Handlungsempfehlungen ergänzt und das richtige Anzeigeverhalten beschrieben.

2 Entwicklungen, Trends und Beispiele

In der Meldestelle des C4 wurden im Laufe des vergangenen Jahres vermehrt Angriffe auf Computersysteme oder Netzwerke mit Hilfe von Schadsoftware, insbesondere Flubot-SMS auf Android-Smartphones, registriert. Ebenso kam es zu zahlreichen Erpressungsversuchen auf Unternehmen unter Verwendung pornografischer Darstellungen Minderjähriger und der Drohung, Kontaktdaten und Lichtbilder der erpressten Empfängerinnen und Empfänger zu veröffentlichen. Genaue Auswertungen und Analysen zur Polizeilichen Kriminalstatistik (PKS) 2022 finden sich in Kapitel 3 wieder.

2.1 Covid-19-Pandemie und ihre Auswirkungen

Auch 2022 setzten sich Betrugshandlungen aufgrund des pandemiebedingt veränderten Einkaufverhaltens fort. Durch Malspam, Phishing und Ransomware teilte man in Aussendungen von Fake-Mails vermeintlicher Paket-Zustelldienste mit, dass aufgrund von Covid-19 keine Zustellungen möglich seien und die E-Mail-Empfängerin beziehungsweise der E-Mail-Empfänger entweder per Direktlink oder per Dateianhang die Optionen zum Paketempfang auswählen könne. Beim Öffnen des Links beziehungsweise Dateianhangs wurde dann die Schadsoftware (zum Beispiel AZORult, Emotet, Nanocore RAT, Trick-Bot) am Zielcomputer installiert.

Insgesamt wird über die letzten Jahre ein sehr starker Anstieg bei Anzeigen im Bereich von Internetbetrug über das Tatmedium Internet verzeichnet. Durch die zunehmende Arbeitsteilung und Vernetzung der Tätergruppen, vor allem im Ransomware-Bereich, wird eine erfolgreiche Strafverfolgung erschwert.

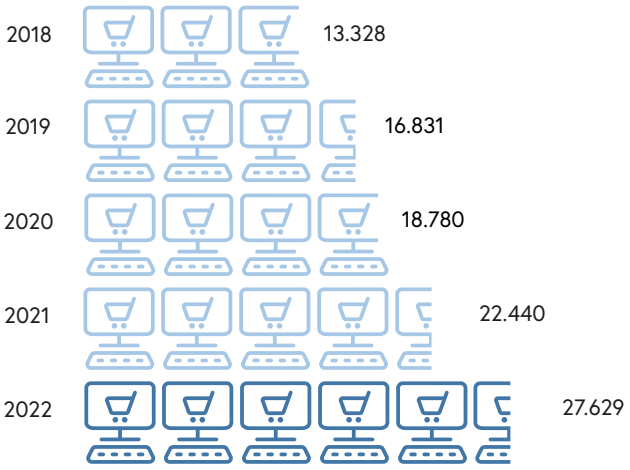
2.2 Internetbetrug

Straftaten im Bereich des Internetbetrugs stellten auch im Jahr 2022 eine große Herausforderung für die österreichische Polizei dar. Das Deliktsfeld Internetbetrug setzt sich aus einer Vielzahl von Modi Operandi zusammen, beginnend bei Anrufbetrügereien, scheinbaren Gewinnversprechen und Investments bis hin zu Love Scams, Phishing Attacken oder betrügerischen Vorgehensweisen im Onlinehandel. Bei den ausführenden Personen handelt es sich, neben wenigen Einzeltätern, meist um organisierte Tätergruppen, die die Anonymität des Internets gezielt als Schutz nutzen. Mit geringem Aufwand können potenzielle Opfer, in breiter Masse, erreicht und hohe Geldsummen lukriert werden.

Laut PKS-2022 wurden im Berichtsjahr 27.629 Delikte im Bereich des Internetbetrugs angezeigt, dies bedeutet im Vergleich zum Vorjahr eine weitere Steigerung von 23,1 Prozent. Hingegen muss festgestellt werden, dass die Aufklärungsquote im gleichen Zeitraum um 1,7 Prozentpunkte gesunken ist. Dieses Ergebnis spiegelt die Entwicklung

der vergangenen Jahre wider und wird vor allem auf die Verschleierungsmöglichkeiten im Internet und professionell agierenden Tätergruppierungen zurückgeführt.

Um sich diesem negativen Trend entgegenzusetzen, fokussiert sich das Bundeskriminalamt einerseits auf die Konzipierung präventiver Maßnahmen, mit dem Ziel, die Bevölkerung durch Vermittlung von Information auf aktuelle Betrugsphänomene aufmerksam zu machen und zu sensibilisieren. Andererseits wird zur erfolgreichen Durchführung repressiver Handlungen durch die Kriminalpolizei die internationale Zusammenarbeit mit ausländischen Behörden weiter verstärkt.



Entwicklung des Internetbetruges. Jahresvergleich 2018 bis 2022 in Österreich

2022 wurde im Bundeskriminalamt ein datenbankunterstütztes Lagebild Betrug, ansässig in der Abteilung 7 – Ermittlungsunterstützung, installiert. Durch die tägliche Auswertung und Beobachtung der Betrugslandschaft in Österreich werden zeitnah aktuelle Entwicklungen festgestellt sowie neue Betrugsmodi erkannt und definiert. Durch die daraus resultierenden Ergebnisse konnten 2022 bereits erste Erfolge im Bereich der Prävention und Repression erzielt werden:

Eine Form des Anrufbetrugs wird als „der falsche Polizeibeamte“ bezeichnet. Allein durch diesen Modus wurden im Jahr 2022 mehr als 15 Millionen Euro Schaden verursacht. Da die Täter nicht saisonabhängig agieren, stellt sich dieses Phänomen als ganzjährliche Problematik dar. Zielgruppe dieser Betrugsform sind explizit betagte Menschen beziehungsweise Personen im pensionsfähigen Alter. Die Geschädigten werden telefonisch kontaktiert und die Täter geben sich als Polizistinnen oder Polizisten aus. Durch Ausübung psychischen Drucks und der Darstellung fiktiver Sachverhalte werden die Geschädigten dazu gebracht, finanzielle Vorleistungen durchzuführen.

Durch die Ermittlungsunterstützung wurde zur Verhinderung dieser Straftat ein Präventionsmodell konzipiert. Im Mai 2022 wurde dieses im Zuge einer „Gemeinsam.Sicher“-Aktion in Kooperation mit der Wirtschaftskammer Österreich (WKO), den österreichischen

Banken sowie den Präsidenten des Seniorenrates Österreichs vorgestellt. So konnten dadurch bereits beträchtliche Schäden verhindert werden.

Erstmalig trat im Dezember 2021 ein weiteres Phänomen auf: Die Täter bezeichnen sich selbst als Mitarbeiterinnen und Mitarbeiter von internationalen Polizeibehörden, wie Interpol, Europol oder „Federal Police Department". Die Kommunikation erfolgt ausschließlich in englischer Sprache. Die Täter bedienen sich sogenannter Call-Bots zur telefonischen Kontaktaufnahme und konfrontieren die Opfer mit einer englischsprachigen Tonbandaufnahme. Die auf dem Display erscheinende Nummer ist mit technischen Mitteln gefälscht. Die Opfer werden aufgefordert eine bestimmte Tastenkombination einzugeben, wobei das Telefonat anschließend an die Täter weitergeleitet wird. Die Betroffenen werden verunsichert, in dem durch die Täter behauptet wird, sie wären in eine Straftat verwickelt. Auf diese Weise werden die Opfer dazu gebracht, den Download einer Remotesoftware auf ihrem Smartphone durchzuführen, Gelder auf Konten von Money Mules zu überweisen oder Bargeld bei Bitcoin-Automaten auf Wallets einzuzahlen.

Durch die Zusammenarbeit des Bundeskriminalamtes mit einem international agierenden Hinweisgeber konnte ein betrügerisches Call Center in Indien lokalisiert werden. Auf Betreiben Österreichs wurde eine Kooperation zwischen Interpol, Indien und Deutschland aufgebaut. Die indischen Polizeibehörden führten eine Hausdurchsuchung durch. Bei dieser kam es zu mehreren Verhaftungen sowie Sicherstellungen von Beweismaterial mit direkter Auswirkung auf Österreich. Seit September 2022 ist dieses Phänomen im gesamten Bundesgebiet nicht mehr existent.

2.3 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 beispielsweise Verschlüsselungstrojaner, aber darüber hinaus auch um spezielle Dienstleistungen zur Geldwäsche, für Übersetzungen oder für den vermeintlichen „Opfer-Support". Auch die Nutzung von Bot-Netzwerken, die sogenannten „Distributed Denial of Service (DDoS)"-Angriffen oder zum Versand von Spam E-Mails dienen, kann vermehrt beobachtet werden. Ebenso wurde ein Anstieg beim Inverkehrbringen von Falschgeld, Online-Kindesmissbrauch-Material, Kreditkartendaten und gefälschten Urkunden bemerkt.

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 zukaufen zu können. Mit einem „Ransomware as a Service"-Modell (RaaS) lassen sich nach wie vor beträchtliche Gewinne erzielen.

2.4 Blockchain, Kryptos und NFTs

Kryptowährungen, insbesondere der Bitcoin, existieren seit mittlerweile 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 den Tätern genutzt werden. Eine Vielzahl von Polizistinnen und Polizisten in den Polizeiinspektionen, den Landeskriminalämtern (LKA) 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 die Blockchain 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 sowie Nutzerinnen und Nutzern alles offen. Ein stetiges Weiterbilden in diesem Bereich ist daher für die ermittelnden Polizistinnen und Polizisten von großer Bedeutung.

2.5 FluBot

FluBot ist eine technisch hoch entwickelte Malware auf Smartphones mit Android-Betriebssystem, die auf unterschiedlichste mobile Anwendungen ausgerichtet ist, sich auf Banking-Apps beziehungsweise Mobile Wallets (Kryptowährungen) konzentriert und Zugangsdaten ausspäht.

Aufgrund der hohen Bedrohungslage wurden seitens des Bundeskriminalamtes bereits im Jahr 2021 zahlreiche mediale Kampagnen gestartet, um die Bevölkerung zu warnen und präventiv aufzuklären.

Die FluBot-Malware verbreitet sich massenhaft über SMS (Smishing), deren Nachrichteninhalt sich beispielsweise auf eine vermeintliche Paketsendung bezieht. Mit der SMS wird ein Link übermittelt, der beim Anklicken den Download der schädlichen Applikation einleitet.

Bei der Aufklärung der technischen Hintergründe konnte das C4 wertvolle Aufklärungsarbeit leisten und zum Verständnis der Funktionsweise maßgeblich beitragen. Nach einer massiven Welle im Vorjahr, wurden auch 2022 Fälle beobachtet. Im Mai 2022

gelang unter Federführung der niederländischen Polizei und Koordinierung Europols ein entscheidender Schlag gegen die technische Infrastruktur der Malware. Strafverfolgungsbehörden aus Australien, Belgien, Finnland, Ungarn, Irland, Spanien, Schweden, der Schweiz, den Niederlanden und den Vereinigten Staaten waren an der erfolgreichen Operation beteiligt (https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones).

2.6 Tochter-Sohn-Trick über WhatsApp-Nachrichten

Den Opfern wird über WhatsApp eine Nachricht, zum Beispiel „Hallo Mama, das ist meine neue Telefonnummer", übermittelt. Die Betrügerinnen und Betrüger geben sich als Kind der Empfängerinnen sowie Empfängern 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 bestimmten Empfänger überweisen. Das Geld würde so bald wie möglich zurückgezahlt. Die Empfängerinnen und Empfänger sind zumeist Money Mules im europäischen Ausland.

2.7 Bezahldienst-Trick

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

2.8 Transportdienst-Trick

Ebenfalls auf Kleinanzeigen-Plattformen kursiert ein weiterer Trick. Die Täter nehmen Kontakt auf und geben an, an der vom Opfer angebotenen Ware interessiert zu sein. Aufgrund des derzeitigen Aufenthaltsortes der vermeintlichen Käuferin oder des vermeintlichen Käufers, der zumeist angeblich im Ausland weilt, kann die Ware jedoch nicht persönlich abgeholt werden. Die angebliche Käuferin oder der angebliche Käufer macht jedoch den Vorschlag, die Ware mit einem Shipping-Dienst (Transportdienst) abholen zu lassen. Den Kaufpreis hätte dieser Transportdienst in bar dabei, um diesen bei Abholung zu übergeben. Im Verlauf dieses angeblichen Kaufes erhält das Opfer vom angeblichen Transportdienst die Aufforderung per Link eine Versicherung abzuschließen und die

Kosten vorerst auszulegen. Bei der Abholung der Ware würden dann auch die Kosten für diese Versicherung von der Käuferin oder vom Käufer übernommen und somit bezahlt werden. Bei dieser Betrugsform bestätigen gutgläubige Opfer tatsächlich Zahlungen an den Täter, ohne dass dieser je die Ware abholen lässt.

2.9 Phishing

Phishing E-Mails/-Websites traten gehäuft, oft in Zusammenhang mit den bereits erwähnten FluBot-SMS, in Erscheinung. Der berühmteste Fall zur Jahresmitte war wohl der Betrug mit FinanzOnline: E-Mails mit der falschen Absende-Mail-Adresse finanzOnline@bmf.gv.at versprachen Steuerrückerstattungen von über tausend Euro. Folgte man dem Link, gelangte man auf eine Phishing-Webseite, die die Eingabe von persönlichen Informationen und Kreditkartendaten forderte.

Alle größeren Bankinstitute in Österreich waren mittels Phishings von Zugangsdaten für eBanking 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".

2.10 Ransomware

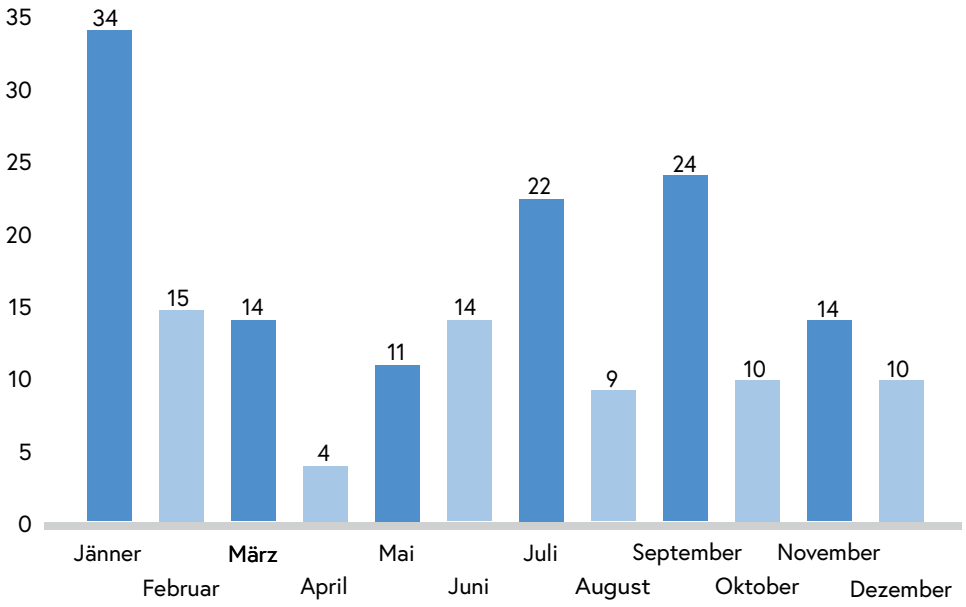
Die Agentur der Europäischen Union für Cybersicherheit ENISA definiert Ransomware als eine „Bedrohung beziehungsweise einen Angriff, bei dem Angreifer die Kontrolle über die Vermögenswerte eines Angriffszieles übernehmen und ein Lösegeld im Austausch für die Wiederherstellung der Verfügbarkeit der Vermögenswerte fordern".

Tatsächlich geht es aber nicht mehr bloß um einen einfachen Austausch. Im Jahr 2022 entwickelte sich die Bedrohungslage verstärkt von einer einfachen Lösegeldforderung hin zu einer „Multifaktor-Erpressung". Daten werden nicht nur verschlüsselt, die Tat geht oft mit einem Exfiltrieren der Daten und der Drohung, diese im Internet zu veröffentlichen oder einem Konkurrenzunternehmen zu übermitteln, einher.

In Österreich werden, bei den Polizeidienststellen angezeigte, Ransomware Fälle im C4 zentral erfasst und analysiert. Fälle, bei denen im Zuge der Analysen Gemeinsamkeiten festgestellt werden, beziehungsweise welche derselben Tätergruppierung zuzuordnen sind, werden zentral mit den involvierten Polizeidienststellen koordiniert, bearbeitet oder es erfolgt eine Unterstützung bei der Fallbearbeitung. Bei Bedarf erfolgt eine

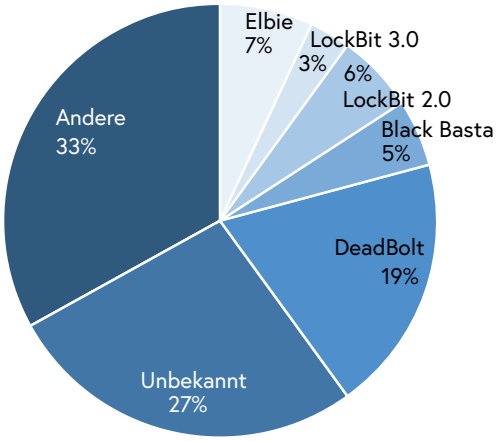
Aktenübernahme durch das C4. So ist ein größtmöglicher Gesamtüberblick betreffend Ransomware-Angriffe in Österreich gewährleistet. Nachgeordnete Dienststellen profitieren von den im C4 durchgeführten Analysen beziehungsweise dem gebündelten Know-how. Eine internationale Koordination sowie Spurenabgleiche erfolgen durch das C4 oder unter dessen Mitwirkung.

Insgesamt wurden im Jahr 2022 österreichweit 181 Fälle von zur Anzeige gebracht.



Monatliche Entwicklung der Ransomware-Fälle 2022 in Österreich

Die Angriffe erfolgten sowohl auf Privatpersonen, EPU (Ein-Personen-Unternehmen), KMU (kleine und mittlere Unternehmen), Konzerne, Bildungseinrichtungen, Gesundheitswesen, Gemeinde- und Stadtverwaltungen. Rund 30 unterschiedliche Tätergruppierungen führten die Angriffe durch. Dass sich Täter auf bestimmte Bereiche konzentrieren, konnte nicht festgestellt werden.



Ramsomware-Arten und deren prozentuale Verteilung in Österreich

Rund 27 Prozent der Angriffe konnten keiner bestimmten Tätergruppierung zugeordnet werden. Gründe dafür sind, dass einige der Betroffenen zum Zeitpunkt der Anzeigeerstattung bereits mit Wiederherstellungsmaßnahmen begonnen oder diese bereits abgeschlossen hatten und daher keine verwertbaren Spuren vorhanden waren.

In 34 Fällen konnte die Ransomware-Art „DeadBolt" festgestellt werden. Dabei werden NAS-Speichersysteme der Marke QNAP angegriffen, die vorwiegend im privaten beziehungsweise EPU- und KMU-Bereich verwendet wird. Weitere Häufungen wurden bei „Elbie", „LockBit 2.0" und „Black Basta" beobachtet.

2.11 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 Angreiferinnen und Angreifer den DDoS-Angriff zuerst durch, um Lösegeld zu verlangen. Andere wiederum schicken zuerst eine Lösegeldforderung und drohen ihren Opfern darin mit einem DDoS-Angriff. Im zweiten Fall sind Angreiferinnen und Angreifer möglicherweise technisch gar nicht in der Lage, den Angriff durchzuführen. Das Restrisiko kann in vielen Fällen jedoch kaum eingeschätzt werden. Von einer leeren Drohung auszugehen, bleibt meist riskant.

In diesem Zusammenhang gab es vereinzelt Attacken auf österreichische Unternehmen, wobei Unternehmen aus unterschiedlichen Wirtschaftsbereichen betroffen waren.

2.12 Suchtgifthandel im Darknet

Seit mehreren Jahren hat sich der Onlinehandel mit verbotenen Suchtmitteln, auch in Österreich, zu einer gängigen Begehungsform der Suchtmittelkriminalität etabliert. Sowohl Einzeltäter als auch kriminelle Organisationen verwenden das Darknet und vermehrt auch anderen Onlineplattformen zur Abwicklung ihres organisierten Suchtmittelhandels und generieren damit ihre illegalen Gewinne. Von der Kontaktaufnahme, über Verkaufsverhandlungen bis hin zur Bezahlung wird der gesamte Ablauf über verschlüsselte Netzwerke abgewickelt. Ermittlungen haben gezeigt, dass der Online-Drogenhandel den Straßenhandel nicht verdrängt, sondern ergänzt hat. Vielmehr wird der Handel auf Onlineplattformen dazu genutzt, illegale Suchtmittel höherer Qualität zu erwerben, um diese im Straßenverkauf gewinnbringend weiterzuverkaufen. Wie sehr Österreich vom Online-Suchtmittelhandel betroffen ist, zeigen die nachstehenden Zahlen: Seit September 2016 werden durch den deutschen Zoll Schwerpunktkontrollen bei den zu exportierenden Briefsendungen durchgeführt. Dabei wurden im internationalen Briefzentrum Frankfurt am

Main Postsendungen, die illegales Suchtmittel zum Inhalt hatten, vom Zollfahndungsamt sichergestellt. Adressiert waren die Briefsendungen an Empfängerinnen und 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 Destinationen wie Großbritannien, Frankreich oder Australien. Vom zweiten Halbjahr 2019 bis Ende 2021 führte Österreich die Reihung sogar konstant an erster Stelle an. Auch in Österreich werden im Zuge von Kontrollen regelmäßig Postsendungen mit illegalen Suchtmitteln festgestellt. Im Jahr 2022 konnten vom Zollamt Österreich 1.474 Sendungen mit Suchtmittel sichergestellt werden. Folgeermittlungen zu den bisherigen Sicherstellungen ergaben, dass die Suchtmittel der aufgegriffenen Briefsendungen meist über Darknet-Marktplätze bestellt wurden. Es wird angenommen, dass rund zwei Drittel der sichergestellten Sendungen ursprünglich aus den Niederlanden stammen, diese teilweise über die Grenze nach Deutschland gebracht werden und dort in den Postweg gelangen.

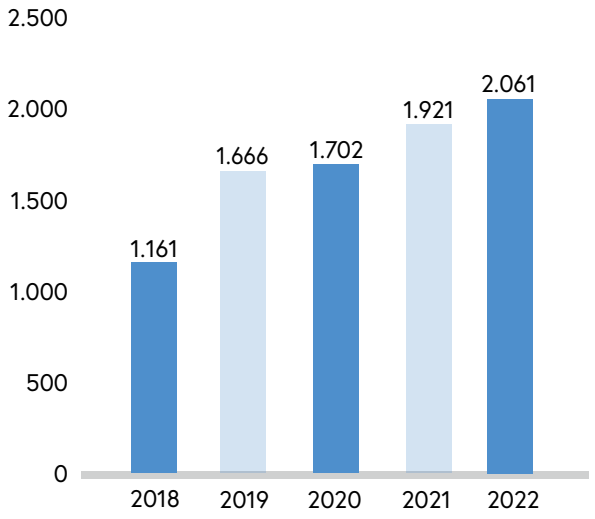
Um dieser Begehungsform der Suchtmittelkriminalität entgegenzutreten, wurde zu deren Bekämpfung im Jahr 2018 ein spezialisiertes Referat im Büro zur Bekämpfung der Suchtmittelkriminalität im Bundeskriminalamt eingerichtet. Dieses führt unter anderem schwerpunktmäßig Ermittlungen gegen in Österreich aufhältige Online-Suchtmittelhändlerinnen und -händler und koordiniert polizeiliche Maßnahmen gegen Käuferinnen sowie Käufer. Neben den operativen Ermittlungsmaßnahmen werden von diesem Fachreferat, auch im Wege des internationalen polizeilichen Informationsaustausches, fortwährend aktuelle Entwicklungen analysiert und darauf abgestimmte Konzepte entwickelt. Dadurch wurde festgestellt, dass zur Bekämpfung dieser Kriminalitätsform, die Zerschlagung der Vertriebswege eines der effektivsten Mittel darstellt. Die auf Darknet-Marktplätzen veräußerten, illegalen Suchtmittel, werden in erster Linie über den herkömmlichen Postweg versendet. Daher werden seit Beginn 2020 die operativen Ermittlungen mit Schwerpunktkontrollen der Postwege kombiniert. Diese Kontrollmaßnahmen erfolgen in enger Kooperation mit der österreichischen Zollverwaltung und verliefen bis dato sehr erfolgreich. Im Jahr 2023 werden diese Maßnahmen weiter fortgeführt und intensiviert.

2.13 Pornographische Darstellungen Minderjähriger

2022 war das Jahr mit einer neuen Rekordzahl übermittelter Verdachtsmeldungen. Es kam zur Übermittlung von 10.130 Verdachtsmeldungen durch US-amerikanische Internet -Service-Provider an das Bundeskriminalamt, was einen absoluten Spitzenwert in der langjährigen Kooperation zwischen den National Center for Missing & Exploited Children (NCMEC) und dem zuständigen Referat darstellt. NCMEC fungiert hier als internationale Drehscheibe und stellt im Speziellen das Bindeglied zwischen den jeweiligen Anbietern und den Strafverfolgungsbehörden der einzelnen Staaten dar.

Online-Inhalte werden vor allem in den USA von Internet-Service-Provider auf pornographische Inhalte überprüft. Inhalte, die der Tathandlung des „Kindesmissbrauch Online“ zuzuordnen sind, werden bei einem entdeckten Fall gesichert und der betroffene Account gesperrt. Damit einhergehend erfolgt eine entsprechende Verdachtsmeldung an die zuständigen Stellen des jeweiligen Landes, dem der Verursacher zugeordnet werden kann.

Entwicklung der Anzahl der Anzeigen wegen pornografischer Darstellung von Minderjährigen von 2018 bis 2022



Positiv hervorzuheben ist, dass es dem zuständigen Referat im Bundeskriminalamt in Zusammenarbeit mit den Landeskriminalämtern gelungen ist, basierend auf den übermittelten NCMEC-Meldungen, 780 Verdächtige zu identifizieren und entsprechend zur Anzeige zu bringen. So blieb trotz steigender Fallzahlen (plus 7,3 Prozent im Jahresvergleich) die Aufklärungsquote im Bereich des § 207a StGB (Pornographische Darstellungen Minderjähriger) nahezu konstant hoch.

Entwicklung der angezeigten Straftaten, der geklärten Fälle und der Aufklärungsquote betreffend der pornografischen Darstellung von Minderjährigen von 2013 bis 2022.

§ 207a StGB (Pornographische Darstellungen Minderjähriger)	Straftatenanzahl	Anzahl geklärt	Aufklärungs-quote
Jahr 2013	551	480	87,1 %
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 %
Veränderung z VJ	7,3 %	6,4 %	-0,7 %-Punkte

3 Jahresrück-blick

3.1 Zahlen und Fakten im Überblick

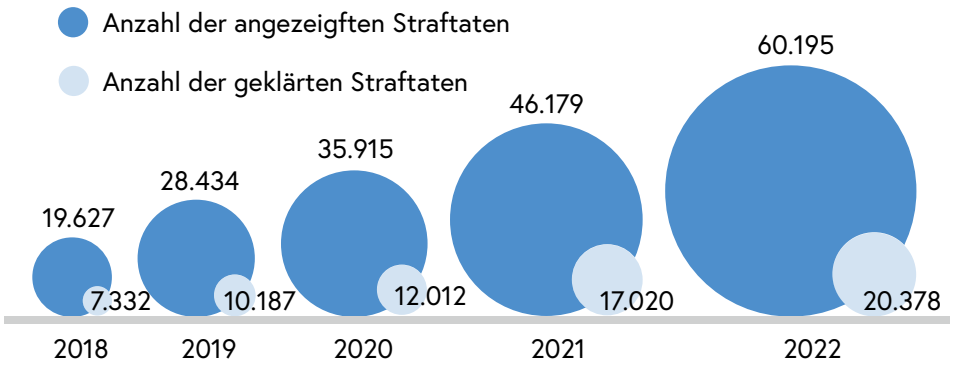
Wie bereits im Vorjahr spiegeln sich Faktoren wie die Covid-19-Krise und beispielsweise rechtliche Herausforderungen deutlich in der Kriminalitätsentwicklung wider. Eine starke Zunahme der begangenen Straftaten im Cybercrime-Bereich konnte auch im Jahr 2022 beobachtet werden. Dieser Trend wurde in den Anfangsmonaten des Jahres durch die Pandemie und seit geraumer Zeit durch die anhaltende Verlagerung vieler Lebensaspekte in die digitale Welt zusätzlich verstärkt.

Entwicklung der Anzahl von Cybercrime-Fällen von 2018 bis 2022 in Österreich

Jahr	Anzahl der angezeigten Straftaten	Anzahl der geklärten Straftaten	Aufklärungsquote (gerundet)
2018	19.627	7.332	37,4 %
2019	28.434	10.187	35,8 %
2020	35.915	12.012	33,4 %
2021	46.179	17.020	36,9 %
2022	60.195	20.378	33,9 %

Die Entwicklung der Internetkriminalität in den letzten fünf Jahren zeigt, dass mit 60.195 Anzeigen und somit einer kräftigen Zunahme von 30,4 Prozent gegenüber dem Vorjahr, erneut ein neuer Spitzenwert erreicht wurde (2021: 46.179). Der Aufwärtstrend setzt sich erwartungsgemäß kontinuierlich fort: Im Vergleich zum Jahr 2018 wurden mehr als dreimal so viele Straftaten angezeigt. Bedingt durch den starken Zuwachs 2022 ging die prozentuelle Aufklärungsquote um drei Prozentpunkte im Vergleich zum Vorjahr zurück. In absoluten Zahlen konnten jedoch 3.358 zusätzliche Straftaten erfolgreich aufgeklärt werden, was einer bedeutenden Steigerung entspricht.

Entwicklung der angezeigten und geklärten Cybercrime-Fälle von 2018 bis 2022 in Österreich



In der PKS wird im Sinne internationaler Vereinbarungen (in Anlehnung an die Budapester Konvention) eine Einteilung von Cybercrime vorgenommen.

3.2 Cybercrime im engeren Sinn (IKT als Angriffsziel)

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

2022 wurde bei Tatbeständen zu Cybercrime im engeren Sinn ein deutlicher Gesamtanstieg der Anzeigen in Höhe von 44,5 Prozent gegenüber dem Vorjahr verzeichnet.

Massive Steigerungen wurden erneut beim betrügerische Datenverarbeitungsmissbrauch § 148a StGB registriert, worunter der NFC-Betrug mit missbräuchlich verwendeten Bankomatkarten fällt. Mit über 18.000 angezeigten Fällen entspricht das einer Steigerung von 45,2 Prozent im Vergleich zu 2021.

Beträchtliche Steigerungsraten wurden auch bei § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem, plus 88,7 Prozent) und § 225a StGB (Datenfälschung, plus 73,9 Prozent) verzeichnet. Trotz der massiven Zunahme konnten 4.723 Straftaten aufgeklärt werden und das Vorjahresniveau von 2.895 aufgeklärten Fällen um 63,1 Prozent in diesem Bereich übertroffen werden. Die relative Aufklärungsquote konnte 2022 im Vergleich zum Vorjahr um 2,4 Prozentpunkte auf 21,1 Prozent erhöht werden.

Delikt	Angezeigte Fälle 2021	Angezeigte Fälle 2022	Geklärte Straftaten 2021	Geklärte Straftaten 2022
§ 107c StGB	395	402	299	305
§ 118a StGB	952	1 796	165	183
§ 119 StGB	14	12	11	10
§ 119a StGB	58	64	4	16
§ 126a StGB	354	375	64	59
§ 126b StGB	95	109	12	4
§ 126c StGB	540	525	46	99
§ 148a StGB	12 701	18 441	2182	3680
§ 225a StGB	375	652	112	367
GESAMT	15484	22376	2895	4723

Cybercrime im engeren Sinn, Vergleich der angezeigten und geklärten Straftaten der Jahre 2021 und 2022.

Beschreibung der Delikte von Cybercrime im engeren Sinn:
§ 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)

3.3 Cybercrime im weiteren Sinn (IKT als Tatmittel)

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

Der Internetbetrug stellt zahlenmäßig den größten Faktor im Bereich der Cyberkriminalität dar und ist auch maßgeblich für den letztjährigen Gesamtanstieg der Delikte verantwortlich. Fast die Hälfte der Internetdelikte fallen auf Betrugsdelikte: 2022 wurden 27.629 Fälle von Internetbetrug angezeigt, ein Plus von 23,1 Prozent. Mit der fortschreitenden Digitalisierung verlagern sich Betrugsdelikte immer mehr ins Internet. Für die Täter ist es ein Leichtes, aufgrund technischer Anonymisierung sowie Verschleierung der Finanzflüsse Betrugshandlungen unerkannt durchzuführen. Zusätzlich können durch den weltweiten Zugang zum Internet immer mehr Menschen als potenzielle Opfer angesprochen werden. Der Bestellbetrug – sowohl auf Seiten der Käuferinnen und Käufer, als auch Verkäuferinnen und Verkäufer – gehört hierbei zum größten Bereich, gefolgt von unbefugten Abbuchungen von Bankkonten der Opfer. Auch der Anrufbetrug (zum

Beispiel „falscher Polizist“) und international agierende Call Center trieben die Statistik in die Höhe, ebenso der digitale Investmentbetrug.

Unter sonstiger Kriminalität im Internet werden Straftaten verstanden, die ihren Tatort im Internet haben. Ausgenommen sind Cybercrime im engeren Sinn, der Internetbetrug, pornographische Darstellungen Minderjähriger (§ 207a StGB) und die Anbahnung von Sexualkontakten zu Unmündigen (§ 208a StGB, 110 angezeigte Fälle 2022). Auch bei der sonstigen Kriminalität wurde 2022 ein Anstieg der Delikte verzeichnet. Der Grund hierfür liegt in der zunehmenden Verlagerung klassischer Strafrechtsdelikte ins Internet. Gleichzeitig werden sogenannte „Crime-as-a-Service“-Leistungen im Darknet angeboten. Dabei handelt es sich vorwiegend um Hackingtools oder Erpressungstrojaner. Ebenso wurde ein vermehrter Vertrieb von Falschgeld, Kindermissbrauch-Online, Kreditkartendaten und gefälschten Urkunden wahrgenommen. § 207a StGB (Pornographische Darstellungen Minderjähriger) verzeichnete einen Zuwachs von 7,3 Prozent im Jahresvergleich (2.061 angezeigte Fälle 2022). Durch die im Darknet angebotenen Dienste stiegen vor allem Erpressungen mit Ransomware und Massenerpressungsmails sehr stark an, meist begleitet von Geldforderungen in Bitcoins.

Deutliche Zunahmen sind auch bei § 105 StGB (Nötigung) mit 450 Anzeigen und § 106 StGB (Schwere Nötigung) mit 270 Anzeigen zu verzeichnen. Ebenso stiegen Anzeigen nach § 223 StGB (Urkundenfälschung) und § 3g Verbotsgesetz (Wiederbetätigung).

SMS-Nachrichten wurden vermehrt zum Daten-Phishing verwendet: Es kursierten mehrere Spam-Kampagnen, die einen Hinweis auf eine angebliche „Zustellbenachrichtigung“ und weiterführende Links enthielten. Verstärkt wurden hier Links von nicht existenten Zahlungsdienstleistern verwendet. Gegen Jahresende — in der Vorweihnachtszeit — war auch wieder die saisonal beobachtbare Anzahl an kriminellen Webshops (Fake- und Phishing-Shops) deutlich angestiegen. Auch waren wiederholt 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.

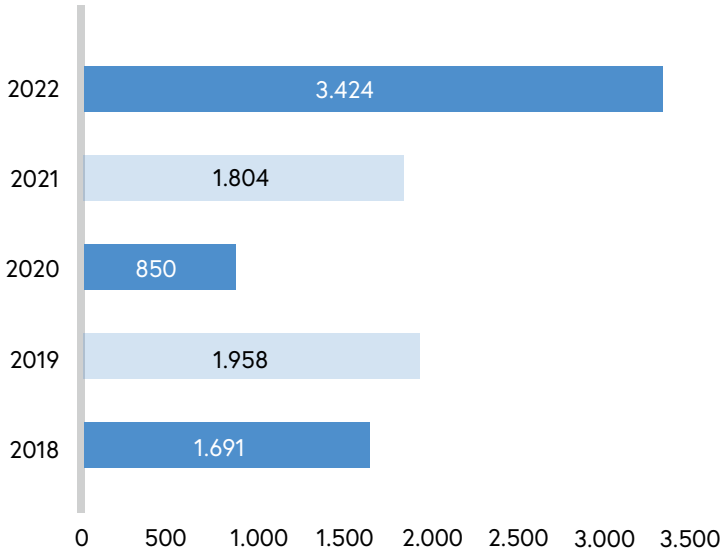
Erpressungen im Internet (§§ 144, 145 StGB)

2022 wurden 3.424 Erpressungen im Internet angezeigt. Das ist eine Steigerung von 89,8 Prozent gegenüber dem Vorjahr (1.804 angezeigte Fälle).

Erpressung im Internet ist als Geschäftsmodell krimineller Gruppierungen im Steigen begriffen. 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.

Entwicklung der Erpressung im Internet von 2018 bis 2022 in Österreich



Cybercrime im weiteren Sinn, Vergleich der angezeigten und geklärten Straftaten der Jahre 2021 und 2022.

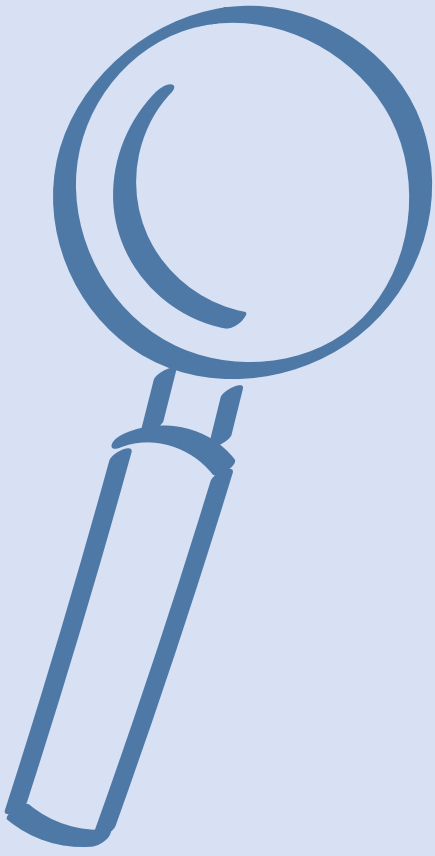
Delikt	Angezeigte Fälle 2021	Angezeigte Fälle 2022	Geklärte Straftaten 2021	Geklärte Straftaten 2022
		Internetbetrug		
§ 146 StGB	19224	23856	7138	8418
§ 147 StGB	2246	2885	701	912
§ 148 StGB	970	888	509	484
Gesamt	22440	27629	8348	9814
		Sonstige Internetkriminalität		
§ 105 StGB	47	450	30	201
§ 106 StGB	23	270	17	106
§ 107 StGB	1303	1057	1124	911
§ 107a StGB	459	437	423	407
§ 115 StGB	88	83	80	76
§ 207b StGB	9	2	9	2
§ 218 StGB	18	1	12	0
§ 223 StGB	87	241	60	200

§ 224 StGB	25	29	19	17
§ 228 StGB	0	1	0	1
§ 231 StGB	37	38	19	19
§ 232 StGB	16	29	10	27
§ 241a StGB	1	1	0	0
§ 283 StGB	262	138	246	129
§ 27 SMG	1201	740	941	573
§ 28 SMG	15	8	15	7
§ 28a SMG	45	43	40	35
§ 30 SMG	31	29	29	28
§ 31 SMG	1		1	
§ 31a SMG	1	2	1	2
§ 32 SMG		1		1
§ 3a VerbotsG	3	2	2	2
§ 3b VerbotsG		1		1
§ 3d VerbotsG	2	6	2	5
§ 3g VerbotsG	651	909	624	886
§ 3h VerbotsG	84	62	80	56
§ 4 NPSG		15		14

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 2022 blieb Social Engineering ein maßgeblicher Angriffsvektor.

4 Ermittlungs-erfolge



4.1 Darknet: Meldedaten-Leak

Ermittlerinnen und Ermittler des C4 konnten im Zuge zweijähriger, hochintensiver Ermittlungsarbeit im Rahmen der Sonderkommission (SOKO) HERA einen Tatverdächtigen ausforschen, der für den Datendiebstahl von so gut wie allen in Österreich wohnhaften Menschen verantwortlich gemacht wird. Er gelangte an knapp neun Millionen österreichischer Meldedatensätze und bot sie im Internet zum Verkauf an.

Screenshot von einem Darknet-Forum

Im Mai 2020 bot eine unbekannte Person unter dem Pseudonym „DataBox“ im Szene-Forum Raidforums.com den Datensatz „Austrian Registration Data“ zum Verkauf an. Der Inhalt dieses Datenpaketes sei „der volle Name, das Geschlecht, die komplette Adresse und das Geburtsdatum von vermutlich jedem Bürger“ in Österreich. Es handelte sich um knapp neun Millionen Datensätzen. Im selben Zeitraum bot der Hacker ähnliche Datensätze aus Italien, Kolumbien und den Niederlanden an. Kurz darauf starteten die Expertinnen und Experten des C4 im Bundeskriminalamt die Erhebungen zu diesem Datenleck. Weitere Ermittlungen bestätigten die Echtheit des Datensatzes.

Im Zuge einer internationalen Polizeiaktion gegen den Handel mit illegalen Daten konnten vorhandene elektronische Spuren einer bestimmten Person zugeordnet werden. Es handelte sich um einen polizeilich international bekannten Hacker. In Zusammenarbeit mit den niederländischen Sicherheitsbehörden ermöglichten die Ermittlungen im November 2022 die Festnahme des Hackers. Die niederländische Polizei sowie die dortige Justiz führen das Ermittlungsverfahren gegen den Tatverdächtigen. Ihm werden dutzende weitere illegale Aktivitäten im Internet angelastet.

4.2 Klärung einer grenzüberschreitenden Einbruchsserie in Österreich und der Schweiz

Beginnend mit Oktober 2021 wurden in Vorarlberg vermehrt Einbruchsdiebstähle in Firmen verübt, wobei große Mengen Kupfer und Altmetall gestohlen wurden. Im Zuge der durchgeführten Ermittlungen ergaben sich konkrete Tatzusammenhänge zu gleichartigen Einbruchsdiebstählen in den Schweizer Kantonen St. Gallen, Thurgau und Zürich. Durch einen ständigen, gegenseitigen Informationsaustausch und durchgeführte Spurenabgleiche wurde festgestellt, dass eine vorerst unbekannte Tätergruppierung offensichtlich grenzüberschreitend aktiv war. Zudem wurden in der Schweiz mehrere Einbruchsdiebstähle in metallverarbeitende Firmen verübt, wobei auch Kleintransporter zum Abtransport des Altmetalls gestohlen wurden.

Täter beim Abtransport von Altmetall

Die zuständigen Kolleginnen und Kollegen des LKA Vorarlberg hatten lange keine Ermittlungsansätze und übermittelten mehrere scheinbar unbrauchbare Bild- und Videodateien an das C4. Die Aufzeichnungen stellten ein nicht näher identifizierbares Kraftfahrzeug (Kfz) dar, das vermutlich zur Begehung der Straftaten verwendet wurde. Durch die forensische Videobearbeitung konnten die Aufnahmen insoweit optimiert werden, dass individuelle Merkmale des Kfz erkennbar und somit die Marke und Type feststellbar waren. Ferner wurden Aufschriften des Kfz erkennbar. Unter Einsatz von Open Source Intelligence konnte das Kfz einer Mietwagenfirma im Umkreis der Tatörtlichkeiten eindeutig zugeordnet werden. Schließlich konnten der Fahrzeugmieter ausgeforscht und konkrete Tatzusammenhänge in die Schweiz aufgezeigt werden.

Tatfahrzeug mit gestohlenen Kupferkabeln.

Die Grundlage zur Klärung dieser Serie wurde mit der gelungenen Auswertung von Überwachungsbildern eines Tatfahrzeuges durch die Multimedia-Forensik des C4 geliefert.

Der ausländischen Tätergruppierung konnten schließlich 175 Einbruchsdiebstähle in Vorarlberg, Tirol und der Schweiz (Kantone St. Gallen, Thurgau, Zürich, Luzern, Aargau und Appenzell) nachgewiesen werden, wobei der verursachte Gesamtschaden über 1,2 Millionen Euro betrug und sich aus dem Wert des Diebesgutes in Höhe von 818.000 Euro und dem Sachschaden von 423.000 Euro zusammensetzt.

Die Mitglieder dieser Gruppierung, die neben den Einbruchsdiebstählen von Kupfer und Altmetallen auch weitere Firmen- und Geschäftseinbruchsdiebstähle verübten, konnten festgenommen und in die Justizanstalt Feldkirch eingeliefert werden.

Als Abnehmer des Kupfers und Altmetalls wurde ein Altmetallhändler aus Götzis ausgeforscht. Er wird beschuldigt, den Tätern Kupfer und Altmetall im Wert von rund 220.000 Euro abgekauft zu haben. Er ist geständig, Kupfer und Altmetall erworben und gewinnbringend weiterverkauft zu haben, bestreitet jedoch die großen Mengen.

Bei Hausdurchsuchungen an den Firmen- und Privatadressen des Abnehmers konnten 69.000 Euro Bargeld, ein Porsche Panamera und ein Porsche Carrera 911 sichergestellt werden. Weiters wurden gefälschte Dokumente und Bankunterlagen sichergestellt, die eine hohe Liquidität des Abnehmers beweisen sollten. Dadurch gelang es ihm, von verschiedenen Privatpersonen Kredite im Gesamtumfang von rund 625.000 Euro zu erlangen. Die gefälschten Unterlagen verwendete der Beschuldigte, um Aufschübe von eingeforderten Rückzahlungen zu erwirken. Ein Teil des gestohlenen Geldes brachte er in seine Firma ein, den anderen Teil verbrauchte er privat. Er wurde wegen des Verdachtes

der Hehlerei und des schweren Betruges angezeigt und ebenfalls in die Justizanstalt Feldkirch eingeliefert.

Die ausgezeichnete, grenzüberschreitende Zusammenarbeit des LKA Vorarlbergs mit den Kolleginnen und Kollegen der Schweizer Polizei darf in diesem Zusammenhang besonders betont werden, ohne der die Klärung der angeführten Straftaten Ende 2022 nicht gelungen wäre.

4.3 OP – Satoshi

Oftmals werden illegal erworbene Gelder in Kryptowährungen investiert und mithilfe von Money Mules unterschiedlicher Ebenen zu Verschleierungszwecken rund um den Erdball transferiert, bis zu einem bestimmten Zeitpunkt die Umwandlung in Echtwährung und Auszahlung erfolgt.

Bei den Ermittlungen gegen einen Geldwäscher zeigte sich, dass nach wie vor eine bedeutende Anzahl von Menschen das Internet und die sozialen Medien nützen, um einen profitablen Nebenjob zu suchen. Ein Umstand der auch Täter auf den Plan ruft, die Money Mules (beschönigend „Finanzagenten“ genannt) anwerben. Um seriös zu wirken, wurden im gegenständlichen Fall von den Tätern gefälschte Webseiten verwendet und Verträge an Interessenteninnen und Interessenten übermittelt. Kommuniziert wurde über den Nachrichtendienst Telegram und gelegentlich über WhatsApp.

Der Money Mule wurde aufgefordert, sich bei einer Kryptobörse, österreichische Money Mules meist bei einem österreichischen Exchanger/Kryptobörse, zu registrieren. Zunächst erhielten sie eine Testüberweisung von einem 2nd Level Money Mule auf das Bankkonto. Später folgten weitere Überweisungen. Dabei handelte es sich durchwegs um betrügerisch erworbene Gelder. Der Money Mule wurde im Chat von den Tätern angewiesen, die Gelder in Form von Bitcoins über Bitpanda an eine bestimmte BTC-Adresse zu transferieren.

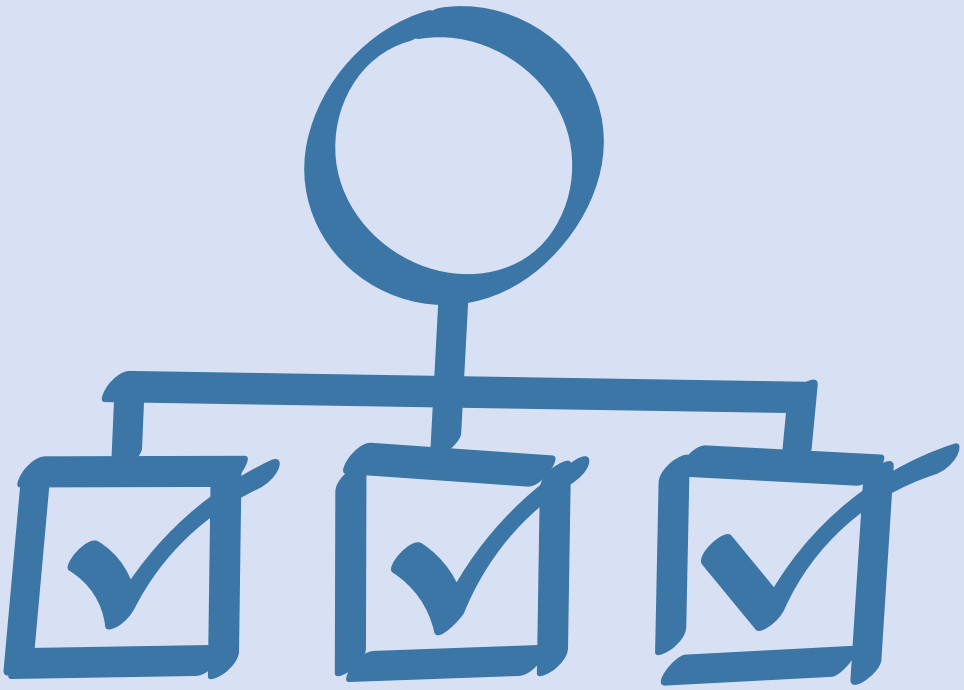
Zu einem späteren Zeitpunkt, nach einigen erfolgten Transaktionen, wurde der Money Mule von den Tätern angewiesen ein Online-Bankkonto, meist bei deutschen Instituten sowie einen Account bei einem weiteren Exchanger, zu eröffnen. Dabei handelte es sich um keinen österreichischen Kryptobörsen/Exchanger.

Die Täter transferierten dann Bitcoin, die sie zuvor von einem 1st Level Money Mule erhalten hatten, auf die Deposit BTC-Adresse eines 2nd Level Money Mules. Das Auszahlen geschah in einem Folgeschritt. Der 2nd Level Money Mule wurde via Telegram-Chat angewiesen, die erhaltenen BTC in Euro umzuwandeln und dann auf ein Bankkonto eines 1st Level Money Mule zu überweisen. Dazu wurde das Online-Konto benötigt.

Dem 1st Level Money Mule wurde suggeriert, dass es sich hierbei um Investitionen von Kundinnen und Kunden handelt. Durch die vielen Transaktionen sollte die Herkunft der Gelder weitgehend verschleiert und somit „gewaschen“ werden.

Die widerrechtlich erlangten Vermögenswerte stammten aus Betrugshandlungen (Modus: Fake Shops und Bestellbetrug) sowie aus Phishing-Attacken. Die Schadenssumme in dem geschilderten Fall belief sich auf rund 1,5 Millionen Euro. Aufgrund umfangreicher Ermittlungsarbeit gelang es dem C4, eine weit verzweigte Struktur offenzulegen und den Modus Operandi näher zu beleuchten.

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 auf der Homepage des Bundeskanzleramtes 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 2022 erreichten 17.857 Anfragen schriftlich und telefonisch die Meldestelle, wobei 15.053 davon einen Bezug zu Cybercrime hatten. Damit konnte erneut eine deutliche Zunahme im Vergleich zum Vorjahr festgestellt werden (15.202 gesamt beziehungsweise 13.183 relevant im Jahr 2021). Die allgemeinen Steigerungsraten im Cybercrime-Bereich während des Vergleichszeitraumes spiegeln sich somit auch hier wider. Auch das C4 ist nicht vor Attacken gefeit und so kam es im Juli des Berichtsjahres zu einer versuchten Überflutung der Meldestelle mit gefälschten Verständigungs-Mails, die auch in der Statistik deutlich ablesbar ist und als Eingänge ohne Relevanz protokolliert wurden.

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 beim Thema Cybercrime erfolgte einerseits durch die fortlaufende Kooperation mit unterschiedlichen Institutionen aus dem Bereich der Wirtschaft und Vereinen, wie beispielsweise der WKO oder der Initiative „Watchlist Internet“. Ebenso führen Erstanalysen der eingehenden Meldungen zu schnellen Informationsweitergaben betreffend 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.

Beispiel einer gefälschten Verständigungsmail.

Von: FBI Home Ltd. <fbi-home@xxyyzz.at>
Gesendet: Montag, X. Jänner 2022 23:59
An: abuse@c********e.com
Cc: *BMI II/BK-SPOC-against-cybercrime <against-cybercrime@bmi.gv.at>
Betreff: Abuse complaint [IP: xxx.xxx.xxx.xxx] Hourly Alert

Hello,

Stop this abusive host (IP: xxx.xxx.xxx.xxx) of scanning my system(s).

The complete information to stop this abusive host (IP: xxx.xxx.xxx.xxx) is given by THIS report.

My systems are located within these ASNs:
ASxxxx, ASxxxx, ASxxxx, ASxxxx, and ASxxxx.
(the corresponding IP subnets and IPv6 prefixes are listed in the attached networks.txt)

See the attached firewall log, that is also given directly to law enforcement authorities.

Any replies will be dropped automatically.

- Doing Portscanning without permission (Opt-in) is a criminal offence. -
- My personality has nothing to say nor it is needed at all. -
---

Da die Meldestelle zudem als Drehscheibe zu anderen internationalen Dienststellen und Polizeieinheiten wie dem INTERPOL Digital Crime 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

Berichts-monat	Anzahl der relevanten E-Mail-Meldungen	Anzahl der E-Mail-Eingänge - Ohne Relevanz	Anzahl der Telefon-Meldungen	Summe der relevanten Meldungen (mit Cybercrime Bezug)	Summe aller Meldungen
2022 01	1.159	127	63	1.222	1.349
2022 02	1.091	95	78	1.169	1.264
2022 03	822	88	61	883	971
2022 04	847	53	91	938	991
2022 05	1.180	210	66	1.246	1.456
2022 06	954	55	84	1.038	1.093
2022 07	2.058	1.757	62	2.120	3.877
2022 08	1.997	85	42	2.039	2.124
2022 09	1.000	182	38	1.038	1.220
2022 10	945	39	75	1.020	1.059
2022 11	1.151	66	38	1.189	1.255
2022 12	1.103	47	48	1.151	1.198

Monatliche Übersicht aller Meldungen an die C4 Meldestelle 2022.

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 LKAs sowie das Fallmanagement als Schnittstelle zwischen Forensikerinnen und Forensikern, Ermittlerinnen und Ermittlern sowie Technikerinnen und Technikern als auch 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 Ermittlerinnen und Ermittler sowie Forensikerinnen und Forensikern
- Etablierung einer Schnittstelle zwischen beteiligten kriminalpolizeilichen Fachbereichen zur optimierten, reibungsfreien Fallbearbeitung

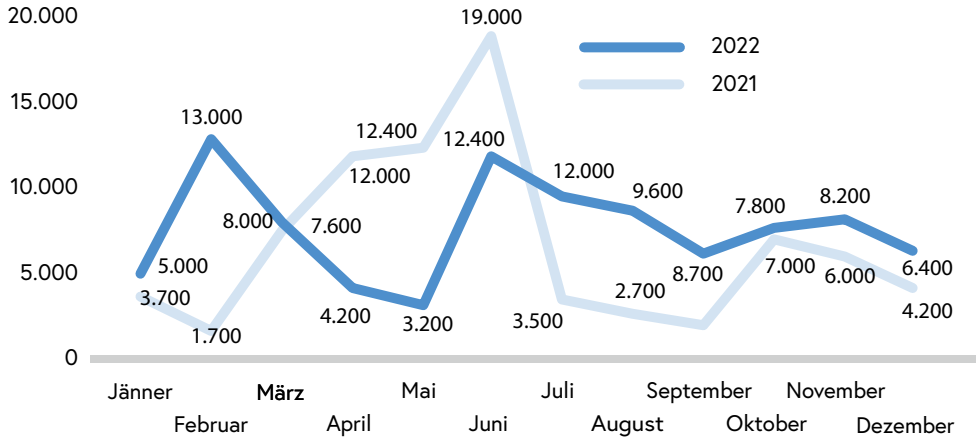
- Auswahl und Einsatz moderner Software und performanter Hardware, um große digitale Beweismittelmengen überhaupt erst durchsuch- und bearbeitbar zu machen

Mithilfe spezieller Programme zur Sichtung großer Datenmengen wurden 2022 insgesamt 31 neue Fälle mit einem Analyseausgangsdatenvolumen von über 85 Terabyte erstellt. Zusätzlich wurden über 100 separate virtuelle Maschinen zur Beweismittelsichtung und fallbezogenen Recherche in Betrieb genommen, womit insgesamt über 700 Ermittlerinnen und Ermittler im Bundeskriminalamt und den LKAs Zugriff auf eine moderne Arbeitsumgebung zur Strafverfolgung erhalten haben. Im größten Einzelfall kooperieren mehr als 300 Ermittlerinnen und Ermittler sowie Dolmetscherinnen und Dolmetscher.

2022 stellte eine der wesentlichen Herausforderungen die Vorbereitung auf einen eventuellen, langanhaltenden Stromausfall im örtlichen Rechenzentrum sowie weitere Optimierungen der vorhandenen Rechenkapazität dar. Daneben wurde die enge Zusammenarbeit mit dem Team des Projekts SeILE (Schaffung einer IKT-Lösung für kriminalpolizeiliche Ermittlungen) intensiviert sowie mit technischen Proof of Concepts unterstützt.

5.4 C4-Forensik

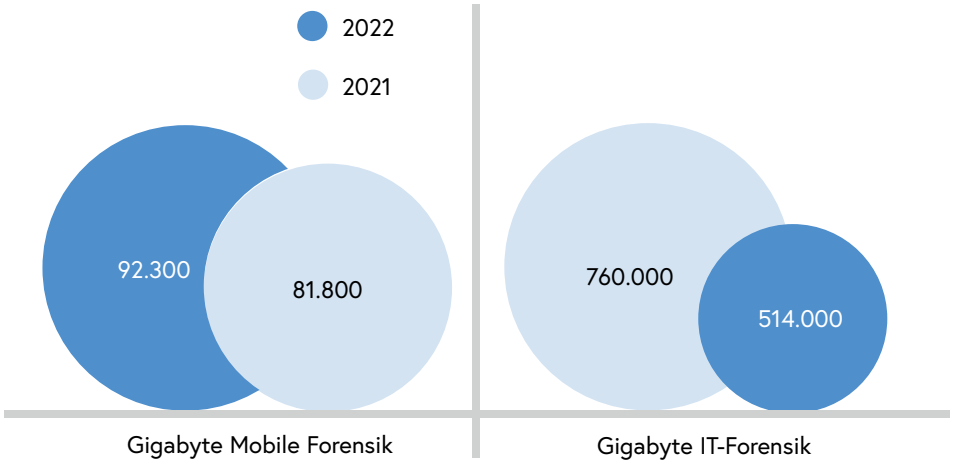
Die Auswertung von IT und Speichermedien stellte die betroffenen Forensikerinnen und Forensiker erneut vor große Herausforderungen, gerade im Bereich der mobilen Forensik. Nach wie vor sind unzählige Geräte mit beträchtlichen Datenmengen aufzubereiten, um die ressourcenintensive Unterstützung der Ermittlerinnen und Ermittler zu gewährleisten. Wie aus der Statistik ersichtlich ist, war die mobile Forensik im Jahr 2022 mit einer Zunahme der auszuwertenden Datenmenge konfrontiert.



Mobile Forensik, monatlich ausgewertete Datenmengen in Gigabyte, Vergleich 2021 und 2022.

Wie bereits in den Vorjahren war auch 2022 der Support der C4 IT-Forensik ein unverzichtbarer, wesentlicher Bestandteil strafrechtlicher Ermittlungen. Zwar fanden im Jahresvergleich weniger Hausdurchsuchungen als 2021 statt, wodurch die abnehmende Datenmenge im Bereich der IT-Forensik erklärt werden kann, jedoch stieg der durch die Verschlüsselung der Geräte verursachte Aufwand. Der elektronischen Beweismittelsicherung im C4 und den LKAs kommt weiterhin maßgebliche Bedeutung in der Ermittlungsarbeit zu.

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 LKAs nicht mehr bewältigt werden können. Die auszuwertenden Datenmengen (Festplatten, Netzwerkdaten, auch bei Mobiltelefonen) bleiben trotz Rückgang der Fallzahlen der IT-Forensik im Jahresvergleich auf hohem Niveau.



Mobile Forensik und IT-Forensik – Gegenübwerstellung der ausgewerteten Datenmengen der Jahre 2021 und 2022.

Das zeit- und ressourcenaufwendige Chip-Off-Verfahren, bei dem Memory-Chips von ihrer Hardware physisch entfernt werden, kann nur zentral im C4 durchgeführt werden. 2022 wurden 100 solcher Verfahren durchgeführt.

Im Bereich der Fahrzeugforensik/Automotive IT, die sich als eigener Fachbereich innerhalb der IT-Forensik entwickelt hat, waren abermals steigende Anforderungen zur digitalen Beweismittelsicherung aus Fahrzeugsystemen erkennbar. Durch die zunehmende Digitalisierung in der Fahrzeugindustrie stellen die im Fahrzeug gespeicherten Daten ein wichtiges Beweismittel für das Strafverfahren dar, wodurch Kfz-Systeme zunehmend in

den Fokus von Ermittlungen gerückt sind. Während beispielsweise die Zahl der Auswertungen in Zusammenhang mit Kfz-Diebstahl und -Verschiebungen rückläufig waren, kam es erneut zu vielfachen Auswertungen im Kontext von schweren Straftaten.

Ein erneuter Anstieg von Anfragen konnte in Zusammenhang mit schweren und tödlichen Verkehrsunfällen festgestellt werden, wobei der Schwerpunkt auf die Sicherung von Crash-Daten (EDR-Event Data Recorder) gerichtet war. Diese Crash-Daten können mit herkömmlichen Untersuchungsschritten maßgeblich zur Rekonstruktion des Unfallhergangs beitragen, da wichtige digitale Informationen über Fahrmanöver in engem zeitlichen Zusammenhang mit dem Unfallereignis analysiert werden.

5.5 Entwicklung und Innovation

2022 gab es wieder zahlreiche Herausforderungen, bei denen die Spezialistinnen und Spezialisten des Referates „Entwicklung und Innovation“ sowohl die Ermittlerinnen und Ermittler als auch die Forensikerinnen und Forensikern unterstützen konnten. In mehreren Fällen waren es wieder große Datenmengen, in denen Ermittlungsansätze zu finden waren. Zum einen waren es am Anfang Ermittlerinnen und Ermittler, die auf Basis des Gefundenen Sachverhalte präzisieren und Täter(gruppen) identifizieren konnten. Zum anderen warfen sich nach Übermittlung der Berichte an die Staatsanwaltschaft von dort noch Fragen auf, die nach weiterer Analyse der Daten beantwortet werden konnten.

Ein in zahlreichen Fällen vorkommender Modus Operandi ist das Fälschen der Telefonnummer der Anruferinnen und Anrufer. Um diese Vorgehensweise besser verstehen zu können, wurde die Thematik wissenschaftlich aufbereitet und mehreren betroffenen Ermittlungsdienststellen präsentiert, was zu einer Verbesserung der Einschätzung von Sachverhalten führte. In diesem Zusammenhang wurde auch Anpassungsbedarf auf rechtlicher Seite identifiziert, der es ermöglichen würde, Opfer besser zu schützen und Täter schneller ausforschen zu können. Die erforderlichen Änderungen werden von den zuständigen Stellen ausgearbeitet und dem Gesetzwerdungsprozess zugeführt.

Die Zusammenarbeit in Forschungsprojekten bildete auch 2022 einen Schwerpunkt. Aufgrund der rapiden technischen Entwicklung ist es laufend notwendig, die Ermittlungsmethoden und -werkzeuge anzupassen, um den Anschluss an die Tätergruppierungen nicht zu verlieren. Da praktisch alle Polizeibehörden bei der Bekämpfung von Delikten, die durch die Digitalisierung begünstigt oder überhaupt erst möglich werden, vor identen Herausforderungen stehen, wird sowohl in Österreich als auch international intensiv zusammengearbeitet. Dies betrifft nicht nur Polizei- und Justizbehörden untereinander, sondern auch Forschungseinrichtungen. Die Europäische Kommission legt gesteigerten Wert auf das Bündeln von Ressourcen und Anstrengungen, um die vorhandenen Mittel möglichst optimal einzusetzen.

5.6 Wissensvermittlung durch Ausbildung und internationalen Austausch

Bereits seit über zehn Jahren findet eine grundlegende Ausbildung von Bezirks-IT-Ermittlerinnen und -Ermittlern statt. Mittlerweile unterstützen mehr als 300 speziell ausgebildete Polizistinnen und Polizisten durch fachgemäße Erstmaßnahmen und Ermittlungen auf lokaler Ebene. Die Vortragenden werden aus Expertinnen und Experten der LKAs und dem Bundeskriminalamt rekrutiert. Einem größeren polizeilichen Bereich wird das Thema Cybercrime insbesondere im Rahmen der Kriminaldienstfortbildungsrichtlinie (KDFR) sowie in den Grundausbildungslehrgängen zugänglich gemacht.

Zu Beginn des Jahres 2022 wurde der Ausbildungsbereich durch Covid-19 und den damit verbundenen Schutzmaßnahmen erneut vor große Herausforderungen gestellt. Präsenzkurse konnten nur teilweise und mit Einschränkungen abgehalten werden. Das C4 hat unter Nutzung der eigenen Webinar-Plattform die geeigneten Module der Bezirks-IT-Ermittlerschulung als Fernlehre angeboten. Zusätzlich fanden auch sogenannte C4-Fachvorträge, die sich an einen erweiterten Personenkreis richten, statt. In diesem Online-Format wird regelmäßig aktuelles Wissen zu unterschiedlichen Cybercrime-Themen an alle interessierten Ermittlerinnen und Ermittler sowie Vertreterinnen und Vertreter der Staatsanwaltschaften vermittelt. Für Staats- und Bezirksanwältinnen und -anwälte wurde in enger Abstimmung mit dem Bundesministerium für Justiz eine eigene Ausbildungsreihe entwickelt, die im Sinne einer zielgerichteten Strafverfolgung speziell auf technische Hintergründe und hiermit einhergehende Ermittlungsmöglichkeiten im Cyber-Bereich fokussiert. Der Start der Ausbildungsmodule, die einen fundierten Einblick in beispielsweise digitale Ermittlungen, Internetbetrug, sozialen Medien, Darknet, Kryptowährungen geben, war im Jänner 2023.

Das C4 hat an internationalen Veranstaltungen teilgenommen bzw. hat solche auch selbst organisiert.

So nahmen beispielsweise IT-Ermittlerinnen und -Ermittler sowie Forensik-Expertinnen und -Experten vom Assistenzbereich 6 aller Landeskriminalämter, aus den Bezirken sowie den Fachabteilungen des Bundeskriminalamtes an der zweitägigen Fachtagung „IT-Beweismittelsicherung“ teil, die vom C4 des Bundeskriminalamtes in enger Kooperation mit dem European Cybercrime Center (EC3) bei Europol und dem Bundesministerium für Landesverteidigung im Oktober 2022 in Wien organisiert wurde. Thema waren die neuesten Entwicklungen im Cyber-Bereich und die damit einhergehende, wirksame Bekämpfung der Cyber-Kriminalität. Fachvorträge vor dem ausgewählten Publikum und ein reger Meinungsaustauch zu Caller ID Spoofing, FluBot, Ransomware, Darknet, Internetbetrug und hiermit zusammenhängende Analyse- und Ermittlungsmöglichkeiten wurden unter enger Einbindung von Europol ermöglicht.

Auf internationaler Ebene im Themenbereich Aus- und Fortbildung hinsichtlich Cybercrime vertritt das C4 Österreich in der European Cybercrime Training and Education Group (ECTEG).

Fachtagung für IT-Beweismittelsicherung in der Maria-Theresien-Kaserne.

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

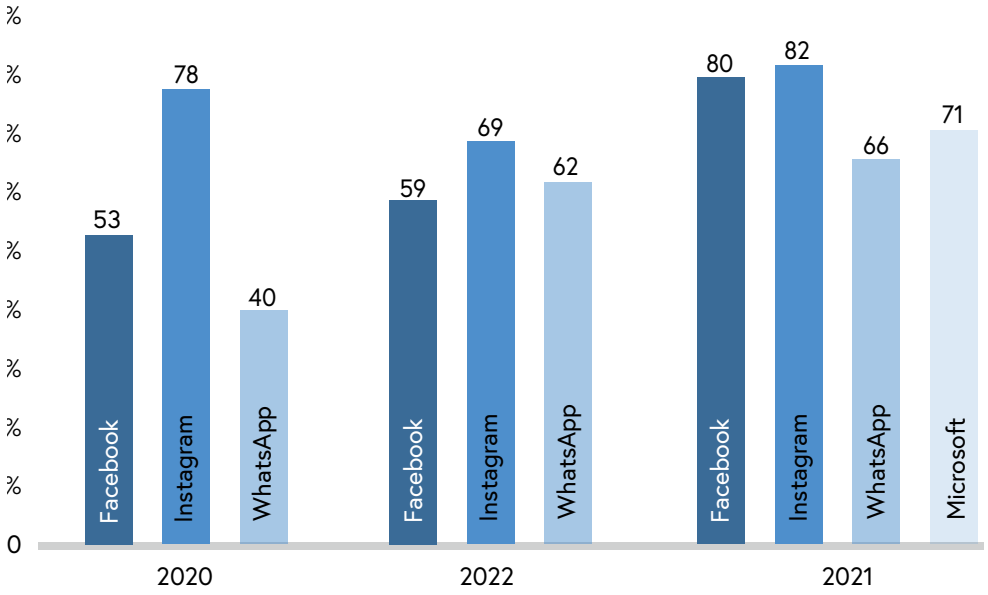
Bei vielen Ermittlungen sind internationale Anfragen an Social-Media-Plattformen und ausländische Diensteanbieter im Internet erforderlich. In der Vergangenheit wurden diese von der jeweils ermittelnden Polizeidienststelle in Österreich selbst durchgeführt, jedoch gab es dazu keinen einheitlichen Prozessablauf 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 es, 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 Umsetzung des Projektes entstand eine verstärkte Unterstützung für die einzelnen Ermittlungsbereiche und es konnte ein höherer Output generiert werden. Ebenso plädierten zahlreiche Diensteanbieter ihrerseits ausdrücklich 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.

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 Start des Projektes gab es in Österreich allgemein 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 über die ZASP gestellt werden.

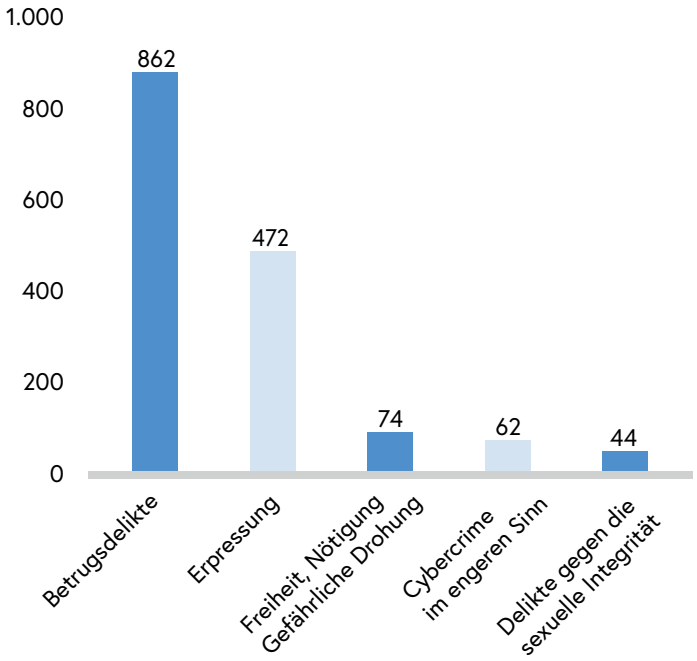


ZASP-Erfolgsquote in Prozent – Vergleich der Jahre 2020, 2021 und 2022.

2022 wurden insgesamt 1.689 Anträge über die ZASP abgewickelt und dabei 2.534 Accountanfragen gestellt. Im gleichen Zeitraum langte von Facebook zu 80 Prozent, von Instagram zu 82 Prozent, von WhatsApp zu 66 Prozent und von Microsoft zu 71 Prozent ein Ergebnis aufgrund einer gestellten Accountanfrage ein.

Zu den Tatbeständen Betrug (862), Erpressung (472), Freiheit/Nötigung/Gefährliche Drohung (74), Cybercrime im engeren Sinn (62) und Sexuelle Integrität (44) wurden 2022 die meisten Anträge gestellt.

ZASP-Anfragen nach Deliktsfeldern 2022 - Top 5.



Die neue kriminalpolizeiliche Einheit kann als ein erfolgreiches Beispiel für zukunftsgerichtete Kooperationen zwischen Behörden und Kommunikationsplattformen angesehen werden.

Künftig 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 Cybercrime-Bekämpfung auf Bundesebene

6.1 Herausforderungen auf Länderebene

Zu den großen polizeilichen Herausforderungen im Bereich der Cybercrimebekämpfung auf Landesebene gehören in technischer Hinsicht nach wie vor die großen Datenmengen vor allem im Bereich der Mobilforensik. Hier werden skalierbare Speicherlösungen benötigt, bei der aus Sicherheitsgründen auch eine entsprechende Redundanz gegeben sein muss.

Hindernisse im kriminalpolizeilichen Bereich stellen seit geraumer Zeit die von Tätern verwendeten Anonymisierungsdienste (VPN, VPS) dar, die die Verfolgung der digitalen Spuren erheblich erschweren beziehungsweise zum Teil sogar unmöglich machen. Hier gilt es, die technische Infrastruktur der Kriminalpolizei entsprechend zu modernisieren und Ermittlerinnen und Ermittler am aktuellsten Stand fortzubilden. Im Bereich der zunehmend komplexen Cybercrimeermittlungen ist ferner das länderübergreifende Zusammenwirken betroffener Organisationseinheiten erforderlich.

Überdies ist in den Bundesländern wie auch in den Zentralstellen eine steigende Problematik im Bereich des Personal-Recruitings festzustellen. Hier steht der öffentliche Dienst in einem oft ungleichen Wettbewerb mit der Privatwirtschaft, beispielsweise im Hinblick auf finanzielle Aspekte. Nichtsdestotrotz ist der Anspruch an die fachliche Qualifikation gestiegen, weshalb der Bereich der Aus- und Fortbildungen laufend erweitert und bundesweit entsprechende Anreize für Interessentinnen und Interessenten geschaffen werden müssen.

Das Problemfeld Ransomware bleibt nach wie vor herausfordernd. Erfahrungsgemäß greifen von Ransomware-Angriffen betroffene Unternehmen auf spezialisierte IT-Expertinnen und -Experten zur Systemreaktivierung zurück, die mit den Spezialistinnen und Spezialisten der Kriminalpolizei meist im laufenden Austausch bleiben. In Sachen Täterkommunikation (Darknet) erfahren die Betroffenen professionelle Unterstützung durch das LKA.

Der Anlagebetrug mit virtuellen Währungen, aber auch andere Formen des Internetbetrugs waren 2022 wie in den Vorjahren stets präsent.

Der Bereich der Fahrzeugforensik zeichnet sich durch immer umfangreichere Informationen aus, die zur besseren Aufklärung von Sachverhalten beitragen können, aber auch einen erhöhten Personalbedarf in der Auswertung mit sich bringen.

6.2 Oberösterreich

Für Oberösterreich kann das seit Jänner 2022 laufende Pilotprojekt „Cyber.Crime.Neu. Denken“ erwähnt werden, das auch im Zuge der stattfindenden Kriminaldienstreform vorgestellt wurde.

Hierbei werden drei verschiedene Ansatzpunkte verfolgt:

IT-Forensik

- Davon sind Aufgaben und Tätigkeiten der Forensik umfasst, wie sie der Assistenzbereich 6 „IT- Beweissicherung“ bis dato wahrgenommen hat und die einer laufenden Bewertung unterzogen werden.

Cybercrime-Ermittlungen

- Hier wurde ein neuer Weg eingeschlagen, bei dem nach Vorbild der kooperativen Fallbearbeitung des Bundeskriminalamtes nicht mehr zwischen „Cybercrime im engeren Sinn“ und „Cybercrime im weiteren Sinn“ unterschieden wird und komplexe Ermittlungen von der neu eingerichteten Cybercrime-Einheit durchgeführt werden. Von den Dienststellen aus OÖ werden alle Sachverhalte mit Cybercrime-Bezug an diese Einheit gemeldet, die innerhalb von längstens 48 Stunden eine Ermittlungsempfehlung rückübermittelt. In dieser Rückmeldung wird eine rechtliche Einstufung des Sachverhaltes vorgenommen und der Sachbearbeiterin oder dem Sachbearbeiter die ermittlungsseitigen Möglichkeiten aufgezeigt.

- Statistik Cybercrime-Einheit LKA Oberösterreich für das Jahr 2022:
  - Ermittlungsanleitungen und Rückmeldungen 7.368
  - Hotline-Telefonauskünfte 5.100
  - Anfragen Social Media und Online Service Provider 520
  - Anzahl Zugriffe auf Cybercrime-Inhalte über die bereitgestellte Plattform 13.532

Cybercrime Training Center

- Sämtliche Vorbereitungen für den Betrieb eines Cybercrime-Training-Centers wurden abgeschlossen. In diesem sollen alle Polizistinnen und Polizisten der Polizeiinspektionen Grundschulungen im Bereich Cybercrime bekommen. Dabei soll den Teilnehmerinnen und Teilnehmern in Kleingruppen von zehn Personen Grundwissen in praxisorientierten-Schulungen vermittelt werden. Kriminaltaktisches Vorgehen und gesetzeskonformes Handeln bei Hausdurchsuchungen mit Schwerpunkt „Digitale Beweismittel“ soll ebenfalls unterrichtet werden.

7 Kooperation und Kriminal-prävention

7.1 Cybercrime Prävention: Neue Herausforderungen

Die letzten drei Jahre, die von der Covid-19-Pandemie geprägt waren, haben sich in vielerlei Hinsicht auf die Menschen ausgewirkt. Der verstärkte Trend zu Home-Office und einer allgemein höheren Online-Präsenz ließen auch die Anzahl der Delikte und die unterschiedlichen Deliktsformen in diesem Bereich in die Höhe schnellen. Insbesondere Betrugsdelikte haben sich zu einem großen Teil ins Internet verlagert. Dies stellt die Polizei vor neue Herausforderungen.

Um in diesem Bereich Aufklärung zu leisten und auf die sich immer schneller ändernden Abläufe zu reagieren und aufmerksam zu machen, informiert das Bundeskriminalamt regelmäßig über die gängigsten Social-Media-Kanäle sowie auf der Homepage des Bundeskriminalamtes und stellt adäquate Präventionstipps zur Verfügung. Die Zusammenarbeit mit relevanten Organisationen, wie etwa dem Österreichischen Institut für Angewandte Telekommunikation verstärken die Breite der 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. Cybermobbing, Sextorsion und Grooming sind nur einige der Phänomene, 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 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 Wissenstransfers jeder Art stehen in den Bundesländern geeignete und spezifisch ausgebildete Präventionsbeamtinnen und -beamte zur Verfügung. Diese können über die LKAs kontaktiert werden und vor Ort Aufklärung und Unterstützung leisten. Dieses Angebot richtet sich an die gesamte Bevölkerung und kann von Privatpersonen ebenso in Anspruch genommen werden, wie von Unternehmen oder der öffentlichen Verwaltung.

Das Bundeskriminalamt stellt sich den wachsenden Herausforderungen und verfolgt neue innovative Ideen, um noch flexibler und effizienter auf sich schnell ändernde Anforderungen reagieren zu können. Diesbezüglich wurde 2022 ein neues Projekt zur Verbesserung der bereits existierenden Präventionstätigkeiten im Online-Bereich gestartet, das primär auf die Steigerung der Kompetenzen sowohl von Beamtinnen und Beamten als auch der Bevölkerung abzielt.

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

7.2 Cybercrime Anzeigenerstattung

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

Um sich hierfür optimal vorzubereiten, helfen Ihnen folgende Tipps:

- Wenn es um einen konkreten aktuellen Notfall geht (Angriff auf Leib oder Leben), dann rufen Sie den Polizeinotruf 133 an!
- Stellen Sie bitte fallrelevantes Beweismittel beziehungsweise Datenmaterial wie zum Beispiel E-Mails, Chat-Verläufe, Zahlungsbelege, Screenshots, digitale Fotos oder Videos entsprechend sicher! 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, welche für eine Täterausforschung notwendig sind. Exemplarisch sind dies IP-Adressen über widerrechtliche Zugriffe inklusive Zeitstempel, Logdaten und so weiter. Überprüfen Sie dazu am besten selbst, welche der für die Tat relevanten Daten beim jeweiligen Account-Anbieter beziehungsweise Online Service Provider gespeichert werden und für Sie zugänglich sind, oder deren Bekanntgabe über diesen angefordert werden kann.
- Wenn es sich um komplexere Tathandlungen handelt, dokumentieren Sie den Tathergang in chronologischer Weise und stellen Sie sicher, dass die Geschehnisse zeitlich richtig eingeordnet sind!
- Wenn Sie Probleme haben, die Beweismittel technisch zu sichern beziehungsweise abzuspeichern, bitten Sie eine Person Ihres Vertrauens diese Beweise mit Ihnen gemeinsam zu sichern!
- Stellen Sie die gesicherten Daten der aufnehmenden Beamtin oder dem aufnehmenden Beamten nach Absprache mit diesen in geeigneter Form zur Verfügung (beispielsweise über https://cryptshare.bmi.gv.at)! Die Daten zur Verfügung zu stellen ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.
- Bitte haben Sie Verständnis dafür, dass Sie bei einem ersten Gespräch mit der Polizei nicht unmittelbar auf spezialisierte Cybercrime-Expertinnen und -Experten 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 Vorgangsweisen und Schritte bei Cybercrime-Vorfällen erteilen. Für die formelle Anzeigenerstattung sind in der Regel die örtlich und sachlich zuständigen Polizeidienststellen verantwortlich. Derzeit ist eine formelle Anzeigeerstattung über die Meldestelle nicht vorgesehen.

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

8 Strategie und Ausblick

Cyberkriminalität ist ein schnell wachsender und sich schnell verändernder Deliktsbereich, der großes Know-how aller involvierten Ermittlerinnen und Ermittler verlangt. Folglich muss in den kommenden Jahren die Ausbildung im Cyber-Bereich weiter forciert werden, das Wissen 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 geplant. 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 im Besonderen der 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 Forschungsergebnissen 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 künstlicher Intelligenz sollen im Bereich der Strafverfolgungsbehörden weiter ausgelotet werden. Ebenso sollen Empfehlungen für die Implementierung von Innovationen generiert und diese, dort wo es erforderlich und rechtlich möglich ist, eingesetzt werden.

Auf europäischer Ebene sollten endnutzerorientierte Vorhaben, die darauf abzielen, eine Struktur zu schaffen, um Praktikerinnen und Praktikern 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, 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.

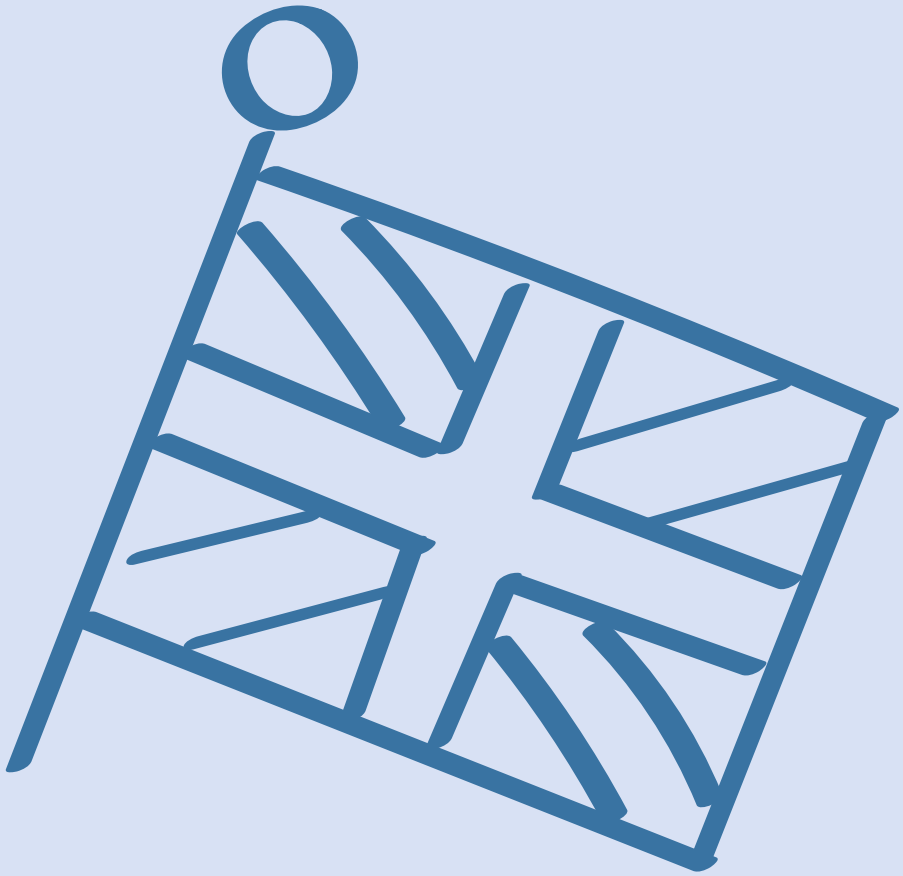
Auf Ebene des C4 wurden im Jahr 2022 sowohl der Bereich der IT-Ermittlungen wie auch der digitalen Beweismittelsicherung (IT-Forensik) personell verstärkt. Die Personalakquise blieb auch 2022 herausfordernd. Eine Tatsache, mit der die Kriminalpolizei

in der Cybercrimebekämpfung seit Jahren konfrontiert ist. Die Umstrukturierung des Büros 5.2 zur Abteilung 5 „Cybercrime Competence Center“ mit insgesamt sechs Büros wird aller Voraussicht nach 2023 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 Projektes wird die Errichtung einer IKT-Lösung für all jene kriminalpolizeilichen Ermittlungs- und Forensik-Tätigkeiten angestrebt, die aus berechtigten Sicherheitsüberlegungen nicht in der aktuellen digitalen Umgebung des BMI ausgeführt werden können.

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 möglichst schnell valide Ermittlungsansätze zu erhalten. Die in diesem Zusammenhang gerade entstehenden technischen Möglichkeiten werden im Laufe des Jahres 2023 ausgebaut.

9 STRATEGY AND PROSPECTS



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. 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 2022 in the areas of IT investigations as well as the preservation of digital evidence (IT forensics). Staff acquisition remained challenging in 2022, 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 2023. 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. 10.

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 just emerging in this context will be expanded in the course of 2023.

10 Glossar

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

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

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

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

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

CaaS (Crime as a Service)
Die für die Begehung einer Straftat benötigten Dienste werden individuell zusammengestellt und online erworben. Dabei handelt es sich vorwiegend um Hackingtools, Schadsoftware, wie beispielsweise Verschlüsselungstrojaner, aber auch um spezielle Dienstleistungen zur Geldwäsche, für Übersetzungen oder für den vermeintlichen Opfer-Support. Die Täter benötigen damit kein tiefgreifendes technisches Wissen zur Straftatbegehung, sondern kaufen sich das fehlende Wissen schlichtweg 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 sowie -ministern im Jahr 2000 gegründete europäische Einrichtung zur Ausbildung der europäischen Polizei.

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

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, der sogenannten URL, aufgerufen werden. Um in das Darknet, beispielsweise das Tor-Netzwerk zu gelangen, benötigt man einen speziellen Browser, wie den Tor-Browser. Daten werden im Darknet anonym und verschlüsselt über verschiedene Server geschickt. Das Darknet war ursprünglich für Personen und Organisationen gedacht, die von Zensur bedroht waren. Heutzutage reicht das Spektrum an illegalen Aktivitäten im Darknet vom Drogen- und Waffenhandel über Dokumentenfälschung, Geldfälschung, Datenhandel bis hin zum Online-Kindesmissbrauch und weit darüber hinaus.

„Distributed Denial of Service"-Angriffe (DDoS-Angriffe)

DDoS-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 Täter auch häufig Geld mit DDoS-Angriffen zu erpressen.

Domain Name System (DNS)

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

European Cybercrime Center (EC3)

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

- Bekämpfung von Cybercrime, begangen durch organisierte Gruppierungen, die beispielsweise durch Onlinebetrug große Geldmengen erbeuten
- Bekämpfung von Formen von Cybercrime, die die Opfer massiv schädigen, wie beispielsweise sexueller Missbrauch von Kindern
- Bekämpfung von Cybercrime inklusive Cyberattacken, die gegen kritische Infrastruktur und Informationssysteme der EU-Mitgliedsstaaten gerichtet 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 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 als auch illegalen Bezahlvorgängen zu beobachten. Insbesondere im Bereich Cybercrime haben sich „Cryptos“, vor allem bei Massenerpressungs-E-Mails und im Suchtgifthandel durchgesetzt. Auch wenn Bitcoin immer noch an erster Stelle rangiert, wird mittlerweile ebenso mit anderen, als „Altcoins“ bezeichneten, Kryptowährungen bezahlt.

Love Scam/Romance Scam

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

Malspam

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

Money Mules

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

Network Address Translation (NAT)

Bei Carrier Grade NAT teilt der Provider eine IPv4-Adresse aus dem privaten Adressbereich „10.0.0.0/8" den 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 Cyber-Angriffen 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.

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 Hackerinnen und Hacker können E-Mails an das Konto des Opfers umleiten und so das weitere Geschehen steuern.

Trojaner (Trojanisches Pferd)

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

Uniform Resource Locator (URL)

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

Virus

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

Verschlüsselung

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

Wallet

Ein Wallet, der englische Begriff für Geldbeutel oder Portemonnaie, ist eine virtuelle Geldtasche, in der Benutzerinnen und Benutzer Bitcoins oder auch 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, das vor allem zur Abfrage von Daten zu Domainnamen genutzt wird. Vor der Datenschutz-Grundverordnung (DSGVO) war es uneingeschränkt möglich Eigentümerinnen oder Eigentümer und die Ansprechpartnerinnen oder Ansprechpartner der Domain sowie IP-Adressen über diesen Dienst abzufragen, da alle Daten öffentlich zugänglich waren.

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 Pornographische Darstellungen Minderjähriger
- § 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