

# Cybercrime Report 2021

Lagebericht über die Entwicklung von  
Cybercrime

# Cybercrime Report 2021

Lagebericht über die Entwicklung  
von Cybercrime

Wien, 2022



[www.bundeskriminalamt.at/cybercrime](http://www.bundeskriminalamt.at/cybercrime)

#### **Impressum**

Medieninhaber, Verleger und Herausgeber:  
Bundesministerium für Inneres, Bundeskriminalamt  
Josef-Holaubek-Platz 1, 1090 Wien  
+43 1 24836 985025 (Single Point of Contact)  
[bundeskriminalamt.at](http://bundeskriminalamt.at)  
Druck: Digitaldruckerei des BMI, Herrengasse 7, 1010 Wien  
Wien 2022

## Inhalt

<b>Vorwort</b>	<b>5</b>
<b>1 Einleitung</b>	<b>6</b>
Über die Broschüre	7
<b>2 Entwicklungen, Trends und Beispiele</b>	<b>8</b>
Überblick über 2021	9
Die Pandemie und ihre Auswirkungen	9
Internetbetrug	9
Crime as a Service	10
Blockchain, Kryptos und NFTs	11
NFT (Non-fungible-tokens)	11
FluBot	12
Fraud Calls und Call-Bots	15
Tochter-Sohn Trick über WhatsApp-Nachrichten	16
Bezahldienst Trick	16
Transportdienst Trick	16
Präventionstipps	17
Phishing	17
Ransomware	18
RDDoS-Angriffe	22
Suchtgifthandel im Darknet	22
Auswirkungen der COVID-19 Pandemie auf den Online-Suchtmittelhandel	23
Pornographische Darstellungen Minderjähriger	24
<b>3 Jahresrück-blick</b>	<b>26</b>
Zahlen und Fakten im Überblick	27
Cybercrime im engeren Sinn (IKT als Angriffsziel)	28
Cybercrime im weiteren Sinn (IKT als Tatmittel)	29
Dunkelziffer und Anzeigeverhalten	31
<b>4 Aufbauorganisation und Abläufe</b>	<b>33</b>
Nationale und internationale Koordinierungs-, Ermittlungs- und Meldestelle	34
Meldestelle	34
Digitales Beweismittelmanagement (DBM)	36
IT-Forensik	37
Fahrzeugforensik und Automotive-IT	39
Entwicklung und Innovation	40
Wissensvermittlung durch Ausbildung und internationalen Austausch	41

ZASP - Zentrale Anfragestelle für Social Media und Online Service Provider.....	41
Erstattung einer Anzeige.....	43
<b>5 Cybercrime-Bekämpfung in den Bundesländern .....</b>	<b>45</b>
Best practices .....	46
Kärnten.....	46
Salzburg.....	47
<b>6 Kooperation und Prävention .....</b>	<b>49</b>
Unterstützung der klein- und mittelständischen Unternehmenslandschaft.....	50
Prävention im Zeichen der Pandemie.....	50
CyberKids.....	51
<b>7 Strategie und Ausblick.....</b>	<b>53</b>
Kriminaldienstreform 2.0.....	54
<b>8 Strategy and Outlook.....</b>	<b>56</b>
“Kriminaldienstreform 2.0”.....	57
<b>9 Glossar.....</b>	<b>59</b>

## Vorwort

Liebe Leserinnen, liebe Leser!

Die Anzahl an Cybercrime-Delikten steigt seit Jahren stetig an. Besonders die Covid-19-Pandemie haben Kriminelle ausgenutzt und ihre Vorgehensweisen angepasst. Durch die Möglichkeit sich das Fachwissen, das es für die Begehung vieler Delikte braucht, zuzukaufen, wird es auch weniger technikaffinen Tätern ermöglicht ihre illegalen Machenschaften umzusetzen. Durch die verschiedenen Verschleierungsmöglichkeiten im Internet werden die Ermittlungen zudem zusätzlich erschwert, was die Polizei vor große Herausforderungen stellt.

Eine Voraussetzung für die nachhaltige Bekämpfung von Cybercrime sind die rechtlichen Rahmenbedingungen. Darüber hinaus muss eine verbesserte Bewusstseinsbildung für mehr Sicherheit und Eigenverantwortung im Internet gewährleistet sein. Eine Stärkung der Widerstandsfähigkeit gegen kriminelle Cyber-Angriffe vor allem in der Wirtschaft und eine schnelle, wirksame Reaktion auf Cybervorfälle muss ausgebaut werden. Aber auch den Strafverfolgungsbehörden müssen die notwendigen personellen, technischen und logistischen Ressourcen zur zielgerichteten Cybercrime-Bekämpfung zur Verfügung stehen.

Die politischen und rechtlichen Rahmenbedingungen sind für diese Thematik in der EU und global gesehen sehr unterschiedlich. Das Bemühen für die in diesem Bericht genannten, konkreten Problembereiche auch umfassende, strategische Ansätze zu entwickeln, wird fortgesetzt. Aus kriminalpolizeilicher Sicht werden weiterhin jene operativen Maßnahmen umgesetzt, die im Rahmen der Leitlinien von EU-Cybersicherheitsstrategien, nationalen Strategien im Bundeskanzleramt und innerhalb des Bundesministeriums für Inneres entwickelt werden.

Im Hinblick auf den wachsenden personellen und technischen Bedarf vollzog sich im Laufe des Jahres 2021 der Umzug des Cybercrime Competence Centers und die feierliche Eröffnung an einen neuen Standort, gepaart mit der Bestrebung das C4 zu einer neuen und modernen Cybercrime-Einheit zu formen, um den internationalen Standards und auch den zukünftigen Herausforderungen weiterhin standhalten zu können.

Unser Dank gilt an dieser Stelle allen Ermittlerinnen und Ermittlern, die tagtäglich im Einsatz sind und Großartiges leisten, unseren Partnerinnen und Partnern, die gemeinsam mit der Polizei ein ständig wachsendes Sicherheitsnetzwerk spannen und last but not least Ihnen als Leserin beziehungsweise Leser, da Sie mit dem Studium der Lektüre dazu beitragen das Thema Cybercrime ein Stück öffentlicher zu machen.

Ihr

Mag. Gerhard Karner  
Bundesminister für Inneres

General Mag. Andreas Holzer, MA  
Direktor des Bundeskriminalamtes



Bundesminister für Inneres  
Mag. Gerhard Karner



Direktor des  
Bundeskriminalamtes  
General Mag. Andreas  
Holzer, MA

# 1 Einleitung



## Über die Broschüre

Der vorliegende Bericht liefert den alljährlichen Überblick über Cybercrime in Österreich und beschreibt die kriminalpolizeilichen Maßnahmen im Rahmen der in Österreich geltenden Definitionen und Abgrenzungen. Die Aufgaben der Cybersicherheit und der Cyberabwehr unterliegen den Verantwortungen anderer Organisationen.

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, weil auch auf die Verfügbarkeit der Daten von Jänner bis Dezember 2021 in der Polizeilichen Kriminalstatistik (PKS) Rücksicht genommen werden muss. Diese gibt trotz dem zu verbesserten Anzeigeverhalten mit vermuteten hohen Dunkelziffern die strategischen Leitlinien der exekutiven Maßnahmen vor und dient der stetigen Weiterentwicklung beim Knowhow-Aufbau und der Bekämpfung.

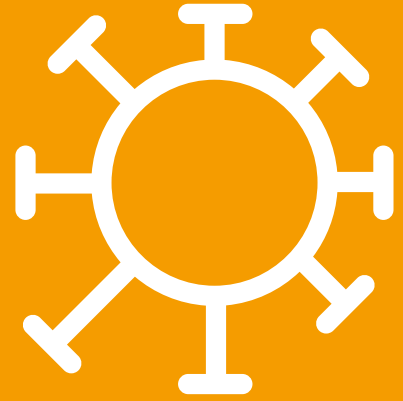
Trotz des erneut hohen Anstiegs von Cybercrime-Delikten (plus 28,6 Prozent im Vergleich zum Vorjahr) konnte die Aufklärungsquote um 3,4 Prozentpunkte gesteigert werden. Insgesamt konnten 2021 im Vergleich zu 2020 im Bereich der Internetkriminalität bei absoluter Betrachtung knapp 5.000 Straftaten zusätzlich aufgeklärt werden. Die Personalrekrutierung von IT-Fachleuten für die geplante Reform des C4 gestaltete sich auch im letzten Jahr mit den bestehenden Ressourcen als besonders schwierig und führt zu einer Fokussierung im internen Wissensaufbau durch zahlreiche pandemiebedingte Online-Schulungen und dem Entwurf neuer Ausbildungskonzepte.

Die Aufbauorganisation und ihre Abläufe sind auch 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 gesetzt 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



## Überblick über 2021

In der Meldestelle des C4 wurden im Laufe des vergangenen Jahres vermehrt Angriffe auf Computersysteme oder Netzwerke mit Hilfe von Schadsoftware, insbesondere Flubot-SMS, registriert. Ebenso läuteten zahlreiche Erpressungsversuche auf Unternehmen unter Verwendung pornografischer Darstellungen Minderjähriger und Kontaktdaten sowie Lichtbilder der erpressten Empfängerinnen und Empfänger das neue Jahr ein. Genaue Auswertungen und Analysen aus der PKS 2021 finden sich in einem eigenen Kapitel wieder.

## Die Pandemie und ihre Auswirkungen

Auch 2021 setzten sich Betrugshandlungen aufgrund des veränderten Einkaufsverhaltens in der Pandemie fort. Durch Malspam, Phishing und Ransomware teilte man in zahlreichen Aussendungen von Fake-Mails vermeintlicher Paket-Zustelldienste mit, dass aufgrund von Covid-19 keine Zustellungen möglich seien und die E-Mail-Empfängerin oder 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.

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

## Internetbetrug

In der Vielzahl der Modi Operandi, die von Anlagebetrügereien, Gewinnversprechen bis zu vorgetäuschten Warenlieferungen reichen, wird das Medium Internet angewandt. Die Vorteile der Anonymität und der geringe Aufwand mit einer Vielzahl von potenziellen Opfern rasch und unkompliziert weltweit in Kontakt zu treten, wird zunehmend durch Kriminelle genutzt. Ermittlungsschritte werden für Strafverfolgungsbehörden bis zur Unwirtschaftlichkeit erschwert, sodass kriminalpolizeilich betrachtet insbesondere präventive Maßnahmen für die Bevölkerung und Unternehmenslandschaften im Fokus stehen.

Das Jahr 2021 war geprägt von den Auswirkungen der Covid-19-Pandemie und auch der Internetbetrug übers Jahr gesehen zeigte weiter starke Anstiege. Bereits bekannte Vorgehensweisen wurden von Tätern auf die Pandemie und ihre Auswirkungen adaptiert.

Auch im Bereich der Anrufriminalität kam es zu einer Revitalisierung von bekannten Betrugshandlungen.

Der Internetbetrug laut polizeilicher Kriminalstatistik hat im Jahr 2021 mit 22.440 Anzeigen einen neuen Höchststand erreicht. Auf Basis der Vorjahreszahlen ergibt das eine Steigerung um 19,5 Prozent zum Jahr 2020. Auf den gesamten Bereich Cybercrime gerechnet, stellt somit der Internetbetrug den größten Teil der Anzeigen im Deliktsbereich dar. Bei der Aufklärungsquote ist im Jahr 2021 mit 37,2 Prozent ein durchschnittliches Ergebnis erzielt worden, wenngleich sich zum Vorjahr eine Steigerung von 1,9 Prozentpunkten abzeichnet. Wie auch in den vergangenen Jahren kann dies auf die Verschleiernungsmöglichkeiten der Täter im Internet und der zunehmenden Professionalisierung der Tätergruppierungen zurückgeführt werden.

Zusätzlich ist gerade im Bereich des Internetbetrugs zumeist von Massendelikten auszugehen. Die spezialisierten Tätergruppierungen gehen arbeitsteilig, technisch versiert und dementsprechend überlegt vor. In diesem Deliktsfeld wird durch den zuständigen Fachbereich der Abteilung 7 des Bundeskriminalamtes besonders im Bereich Bestellbetrug ein Schwerpunkt gesetzt. Dabei stehen betrügerische Bestellungen über das Internet bei österreichischen Onlinehändlerinnen und Onlinehändlern im Fokus.

## Crime as a Service

Die angebotenen Leistungen von „Crime as a Service“ Diensten (Caas) 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 „Opfer-Support“. Auch die Nutzung von Bot-Netzwerken, die DDoS Angriffen oder zum Versand von Spam-E-Mails dienen, kann vermehrt wahrgenommen werden. Ebenso wurde ein Anstieg beim in Verkehr bringen von Falschgeld, Kinderpornographie, Kreditkartendaten und gefälschten Urkunden bemerkt.

Durch die im Darknet angebotenen Dienste steigen vor allem Massenerpressungs-E-Mails 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 Leistungen 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.

## Blockchain, Kryptos und NFTs

Kryptowährungen, insbesondere der Bitcoin, existieren seit mittlerweile 13 Jahren. Anfangs noch von der breiten Masse der Bevölkerung als Witz und Spielerei abgetan, bestimmen sie heute zu einem bedeutenden Teil den polizeilichen Alltag. Egal ob Raub, Erpressung oder Betrug: In vielen Deliktsbereichen ist es bereits üblich geworden, dass Kryptowährungen von der Täterschaft genutzt werden. Eine Vielzahl von Kolleginnen und Kollegen in den Polizeiinspektionen und den Fachbereichen im Bundeskriminalamt sind täglich damit konfrontiert. Ein Vorbeikommen an der Thematik ist daher unausweichlich geworden. Die Ermittlungen gestalten sich aufgrund der enormen Anzahl von Blockchains sowie ständigen Weiterentwicklungen (beispielsweise Binance Smart Chain und ERC-20, ERC-721 und ERC-721 Tokens) 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 mit einer Vielzahl an Eigenschaften geschaffen. 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 Kolleginnen und Kollegen von enormer Bedeutung.

Eines der neuesten Phänomene in der Blockchain-Welt stellen NFTs (Non-fungible-tokens) dar. Diese werden aller Wahrscheinlichkeit nach in naher Zukunft auch in polizeilichen Ermittlungen an Bedeutung gewinnen.

### NFT (Non-fungible-tokens)

Wer hätte jemals gedacht, dass ein digitales Kunstwerk, wie das Bild eines Comic-Affen einen Wert von 400.000 Euro erreichen könnte? Dies ist bereits Realität geworden. In diesem Zusammenhang können Anstiege krimineller Handlungen mit dieser neuen Form von Vermögenswerten erwartet werden. Als Beispiel werden zunehmend illegale Transfers und Geldwäsche vermutet.

Es handelt sich hierbei um einen sogenannten ERC-721 Non-fungible-Token. Dieser Token ist einzigartig und nicht austauschbar. In diesem Fall ein gezeichnetes Bild eines Künstlers in der digitalen Welt, basierend auf Blockchain-Technologien mit einem Wert von Hunderttausenden Euros.

NFTs existieren bereits seit einigen Jahren, aber man hat ihnen bis vor kurzer Zeit fast kein Augenmerk geschenkt. Seit 2021 sind NFTs der letzte Schrei in der digitalen Kunstbranche und Blockchain-Welt. Die meisten NFTs basieren auf der Ethereum Blockchain. Sie können spezielle Funktionen enthalten und zum Beispiel auch als Spielfigur in einem Online-Shooter oder wie der Comic-Affe als Kunstwerk in Erscheinung treten. Der Wert des jeweiligen NFTs bestimmen Käuferin oder Käufer, die dem Objekt einen Wert beimessen. Wer Interesse daran hat, kann auf dem größten offiziellen Marktplatz [www.opensea.io](https://www.opensea.io) stöbern und sich selbst einen Eindruck darüber verschaffen.

In England wurden bereits NFTs von der Polizei sichergestellt und es ist nur mehr eine Frage der Zeit bis dieses Phänomen auch bei uns polizeilich im Zuge einer Anzeige aufgeschlagen wird. Auf internationaler kriminalpolizeilicher Ebene wird das Thema bereits intensiv besprochen. Diverse Vorgehensweisen werden diskutiert, eine justizielle Einordnung in Österreich steht allerdings noch aus.

## FluBot

FluBot ist eine technisch hoch entwickelte Malware auf Smartphones mit Android-Betriebssystem, welche 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 Bundeskriminalamts zahlreiche mediale Kampagnen gestartet, um die Bevölkerung zu warnen und präventiv aufzuklären.

Die FluBot-Malware verbreitet sich massenhaft über SMS (Smishing), deren Nachrichtinhalt sich beispielsweise auf eine vermeintliche Paketsendung bezieht. Mit der SMS wird ein Link übermittelt, der beim Anklicken den Download der schädlichen Applikation einleitet. Im Spätsommer wurden diese SMS-Nachrichten zu dieser Form des Daten-Phishings verwendet: Es kursierten mehrere Spam-Kampagnen, die einen Hinweis auf eine angebliche „Zustellbenachrichtigung“ und weiterführende Links enthielten. Hierbei wurde zu Portonachzahlungen von 1,50 Euro aufgefordert, wobei das eigentliche Ziel der Täterschaft das Phishing von Kreditkartendaten war.

Aber nicht nur vorgegaukelte Paketsendungen (Beispielhaft DHL, UPS, FedEx) werden massenhaft verbreitet, sondern auch SMS mit Inhalten zu Videos, die erst durch ein vorgetäushtes Update des Betriebssystems beziehungsweise die Installation des Flashplayers anzusehen sind. Tatsächlich wird das Mobiltelefon aber mit FluBot infiziert.

Es gibt bereits mehrere Varianten von FluBot, die weiterentwickelt wurden und meist sehr ähnlich in ihrer Funktionsweise sind. Ziel ist es dabei, Informationen zu Online-Banking, SMS, Kontakt- und weitere persönliche Daten vom infizierten Mobiltelefon auszulesen.

Die Malware nutzt Overlay-Angriffe, um Anwendungs-Phishing durchzuführen und verbreitet sich selbst über das Mobiltelefon der Opfer.

Ein Overlay-Angriff bedeutet, dass sich eine für die Nutzerin oder den Nutzer nicht erkennbare Applikationsschicht über die legitime, von der Nutzerin oder dem Nutzer gestartete Anwendung legt und dabei die Eingaben abfängt. Genauer: Beim Start der originalen Banking-App durch die Nutzerin oder den Nutzer legt sich über diese ein sogenanntes Overlay (Phishing-Seite, die der Banking-App zum Verwechseln gleicht) und fungiert als Keylogger. Sämtliche Eingaben, wie zum Beispiel Zugangsdaten werden abgefangen und an einen von der Täterschaft kontrollierten Server (C&C Server) übermittelt – unbemerkt und nicht erkennbar durch das Opfer.

Die Schadsoftware hat weiters die Funktionalität unbemerkt SMS zu senden und zu empfangen. FluBot richtet sich selbst als Standard-SMS-Anwendung ein. So wird FluBot in die Lage versetzt durch die Bank versendete TAN SMS abzufangen und an den C&C Server zu übertragen.

Während des Installationsvorganges müssen durch die Nutzerin oder den Nutzer des Smartphones diverse Berechtigungen beziehungsweise Zugriffsrecht freigegeben werden. Nach der Installation analysiert die Malware die installierten Anwendungen (Apps) auf dem Gerät und sobald sie eine Banking-App oder eine Krypto-Anwendung erkennt, wird der Angriff gestartet.

Das Opfer ahnt nicht, dass es Zugangsdaten in eine der Banking-App überlagerte Phishing-Seite eingibt und diese dann an den C&C Server der Täterschaft übermittelt werden.

Nach der Installation der Malware hat die Täterschaft zumeist jederzeit Zugriff auf das Smartphone und ist Teil eines von der Täterschaft kontrollierten Bot-Netzes. Es befindet sich im Verbund mit anderen infizierten Geräten.

Der Zugriff auf das Mobiletelefon ermöglicht es der Täterschaft die Kontaktliste abzu- ziehen. Gleichzeitig empfängt das korruptierte Gerät tausende Rufnummern vom C&C Server und sendet unbemerkt massenhaft SMS (Smishing) mit inkriminierten Links aus und fungiert so als direkter Verteiler der Links zur Schadsoftware.

Im Fall, dass keine Banking-App oder Crypto-Wallet-App auf dem Mobiltelefon installiert ist, fungiert das Gerät trotzdem als Verteiler der URL in Richtung weiterer, potenzieller

Opfer. In der Zwischenzeit schlummt FluBot und wird erst aktiv, sobald das Opfer eine Zielanwendung, zum Beispiel eine Banking-App installiert und ein Overlay-Angriff gestartet werden kann.

Eine Bereinigung des korrumpierten Gerätes lässt sich nicht einfach durch Deinstallation der “FluBot-App” beziehungsweise Zurücksetzen auf Werkseinstellungen durchführen.

Abbildung 1:  
Beispiel einer Textnachricht  
mit URL zur Schadsoftware

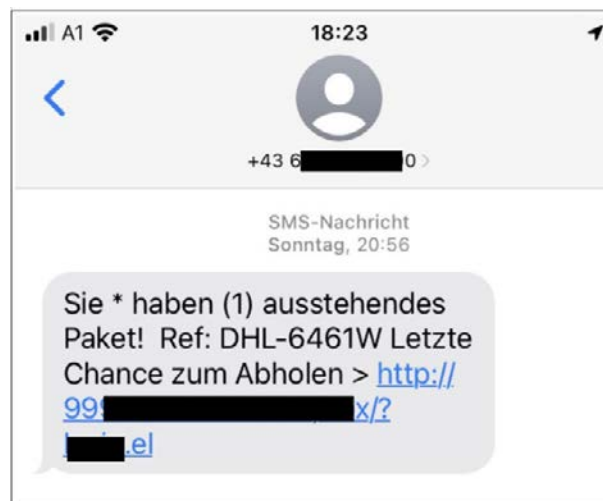
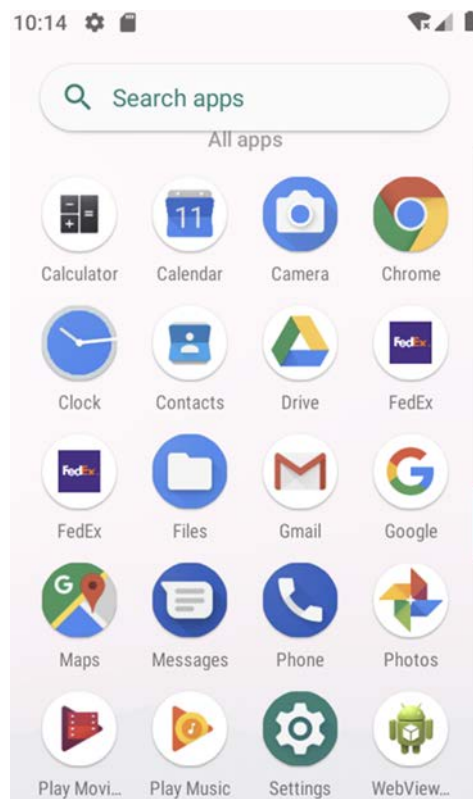


Abbildung 2:  
Beispiel für ein infiziertes  
Gerät, das FedEx Anwen-  
dung vorgaukelt



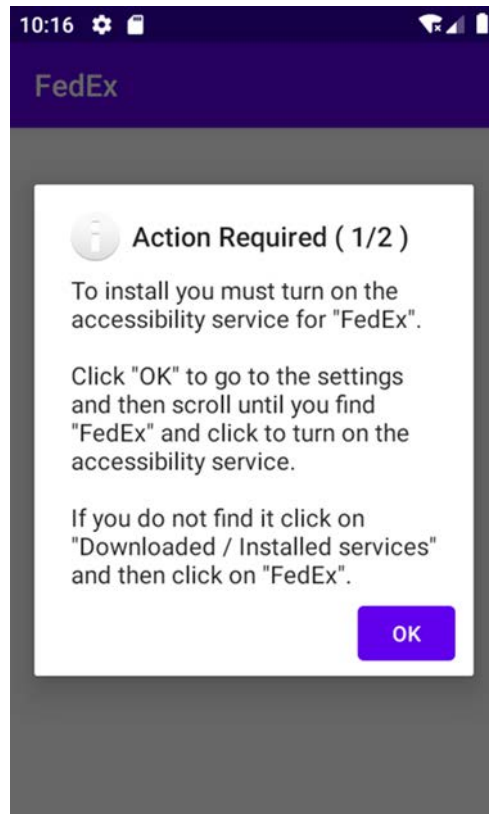


Abbildung 3:  
Beispiel für einen Installationsvorgang mit der Aufforderung zur Genehmigung von Berechtigungen

## Fraud Calls und Call-Bots

Neben dem bereits im Vorjahr aufgetretenen Tech-Support-Scam und Fraud Calls konnten im letzten Jahr neue und für Täter kostenoptimierte Vorgehensweisen wahrgenommen werden. Bei Call-Bot-Anrufen bedienen sich die Täter bestimmter Computerprogramme, welche „Call-Bots“ genannt werden. Damit werden potenzielle Opfer angerufen und mit Tonbandaufnahmen in englischer Sprache konfrontiert. Die Nummer auf dem Display der Angerufenen wird mit technischen Mitteln, dem sogen. „Call-ID-Spoofing“ verfälscht und ist daher nicht rückverfolgbar. Die Opfer werden dabei aufgefordert Tastenkombinationen zu drücken, damit werden mögliche englischsprachige Opfer bereits vorselektiert. Danach melden sich beispielsweise Täter, die sich als (Interpol-) Polizistinnen oder -Polizisten oder Parlamentsangehörige ausgeben. Dem Opfer werden dabei die Mitwirkung an strafbaren Handlungen, wie Geldwäsche, Betrugs-, Suchtmittel- oder Gewaltdelikte vorgeworfen. Danach werden vom Opfer zu seiner Entlastung oder für einen neuen Identität hohe Geldsummen gefordert. Bei Nachfrage zur englischsprachigen Kommunikation verweist man auf die angebliche Internationalität und das Mithören von Europol-Bediensteten.

Die Täter versetzen das Opfer mitfühlend oder aggressiv in eine große Stresssituation, erzeugen Zeitdruck und Angst. Dabei stellen sie sich mit Gegenargumenten auf das Opfer ein.



Durch die zeitnahe Auswertung der Call-Bot-Anrufe erzielte das Auswerteteam der Abteilung Wirtschaftskriminalität im Bundeskriminalamt bereits im Jänner 2022 einige Erfolge: In enger Zusammenarbeit mit der Geldwäschemeldestelle des Bundeskriminalamtes konnte für österreichische Geschädigte rund 110.000 Euro zurückgeholt werden, die sich vermutlich auf Money-Mule-Bankkonten befanden.

## Tochter-Sohn Trick über WhatsApp-Nachrichten

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

## Bezahldienst Trick

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

## Transportdienst Trick

Ebenfalls auf diesen Kleinanzeigenplattformen kursiert derzeit 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 Käufers, der zumeist angeblich im Ausland weilt, kann die Ware jedoch nicht persönlich abgeholt werden. Die angebliche Käuferin oder 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 auszuliegen. Bei der Abholung der Ware würden dann auch die Kosten für diese Versicherung

von der Käuferin oder dem Käufer übernommen und somit bezahlt werden. Bei dieser Betrugsform bestätigen gutgläubige Opfer tatsächlich Zahlungen an den Täter, ohne dass dieser je die Ware abholen lässt.

## Präventionstipps

Bleiben Sie unbekannten Personen gegenüber misstrauisch:

- Wenn Sie etwas verkaufen, müssen Sie keine Bezahl-details 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 Bankanbieters, wenn Sie etwas verkaufen!
- Nutzen und überprüfen Sie die von den Kleinanzeigenplattformen empfohlenen Bezahl-dienste und keine unbekannten Links, deren Herkunft nicht zweifelsfrei feststeht!
- Machen Sie sich mit den auf Kleinanzeigenplattformen angebotenen Bezahl-diensten vertraut!
- Ist ein Schaden entstanden, verständigen Sie sofort ihr Banküberweisungsinstitut oder ihren Kreditkartenanbieter und ersuchen Sie um Rückbuchung. Erstellen 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](https://www.bundeskriminalamt.at/202/Betrug_verhindern/start.aspx)

## 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-E-Mail-Adresse finanzOnline@bmf.gv.at versprachen Steuerrückerstattungen von über tausend Euro. Folgte man dem Link, gelangte man auf eine Phishing-Webseite, welche 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 Onlinebanking 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“.

## Ransomware

Ransomware wurde in den letzten Jahren zu einer großen Bedrohung für die Gesellschaft, die Privatpersonen, aber vor allem Unternehmen mit hohen Schadenshöhen bedroht.

Ransomware wurde zum vielfach genutzten Werkzeug von Cyberkriminellen. Jährlich landen zahlreiche Fälle zur möglichen Weiterbearbeitung im Cybercrime Competence Center (C4) des Bundeskriminalamts.

Dabei sind die korrekte Anzeigenaufnahme und eine entsprechende Datensicherung in der Fläche herausfordernd und essenziell.

Die Schadsoftware verschlüsselt Nutzerdaten, um für deren Wiederherstellung die Bezahlung von Lösegeldern, meist in Form von Bitcoins, zu fordern. Es existieren mittlerweile zahlreiche Varianten mit unterschiedlichen Verbreitungswegen und Verschlüsselungsalgorithmen. Die Gefahr eigene Daten durch eine Schadsoftware zu verlieren, indem diese verschlüsselt und zum Zeitpunkt der Verschlüsselung vorhandene Sicherungen unbrauchbar gemacht werden, ist nach wie vor noch sehr hoch. Wie in den letzten Jahren beobachtet werden konnte, gehen die Täter tendenziell weg von Massenaussendungen. Einzelne, ganz bestimmte Sicherheitslücken werden extra gesucht und dann auch ausgenutzt. Der erpresste Betrag richtet sich nach der Finanzkraft des Unternehmens. Um der Zahlung Nachdruck zu verleihen, wird sehr oft mit der Veröffentlichung von Daten aus dem Unternehmen gedroht.

Die Angriffe richten sich vorwiegend gegen kleine und mittlere Unternehmen (KMU) und weniger gegen Einzelpersonen, wodurch das Risikopotenzial für die österreichische Unternehmenslandschaft hoch bleibt. Aber auch internationale Großunternehmen und Betreiber kritischer Infrastrukturen waren mit internationalen Auswirkungen und sehr hohen Schadenssummen konfrontiert. Auffallend waren in Österreich die branchenübergreifenden Tathergänge mit Betroffenen aus der Lebensmittelproduktion, IT-Dienstleister und deren Kundinnen und Kunden, internationale Anlagefonds, Maschinenbau, Kranbau-

unternehmen, Kfz-Auslieferer, Sportbekleidungsherstellerinnen und Sportbekleidungshersteller sowie Ärztinnen und Ärzte. Die Täter suchen dabei gezielt nach Sicherheitslücken. Das genaue „Profiling“ des Opfers erfolgte dann in einem nächsten Schritt.

Als primäre Infektionsvektoren gelten:

- Fernzugriffe, die für Firmen für die Fernwartung und Datenzulieferung häufig notwendig sind
- E-Mails mit schädlichem Dateianhang oder mit Links, über die Schadsoftware nachgeladen wird
- Schadsoftware, über die die Verschlüsselungssoftware nachgeladen wird, wie zum Beispiel Emotet
- Zahlreiche andere Wege sich mit einem Verschlüsselungstrojaner infizieren zu können, wie beispielsweise Drive-by-Downloads, Supply Chain Attacks oder Malvertising

Die Täter gingen zielgerichtet gegen ihre Opfer vor und mit einer technischen Kompromittierung des Computersystems von durchschnittlich 14 Tagen waren die eingesetzten Methoden oft sehr aufwendig und ausgeklügelt. So wurden die Höhen von Erpressungssummen häufig an den Umsatz und sogar die Verschlüsselungsprozesse an die Backup-Strategien ihrer Opfer angepasst.

Früher wurden solche Schadprogramme noch eher großflächig und wahllos per E-Mail versandt, jedoch sollten vorab getroffene zentrale Sicherheitsmaßnahmen, wie beispielsweise Spamfilter oder allgemeine Virens Scanner diese zeitgerecht herausfiltern können. Trotzdem besteht weiterhin die hohe Gefahr, dass Empfängerinnen und Empfänger die E-Mails und auch die zugehörigen schadhaften Anhänge öffnen.

### **Reputationsverlust und Anzeigeverhalten**

Eine Datenverschlüsselung ohne präventive Sicherung und vordefinierte Prozesse im Anlassfall behindert die Verfügbarkeit von Dienstleistungen und Produktionskapazitäten tagelang und manchmal sind die Daten irreversibel vernichtet.

Neben der existenziellen Bedrohung leidet auch die Reputation des Unternehmens stark durch mediale Negativ-Schlagzeilen. In der Vergangenheit forderten die Erpresserinnen und Erpresser als Lösegeld nur wenige Bitcoins. Auf die Erpressung sind betroffene Unternehmen meist nicht eingegangen, auch weil der Betrieb über die Wiederherstellung von Backups fortgeführt werden konnte. Dies war der Grund warum Anzeigen auch oft nicht bei der Polizei gemeldet wurden.

## Wie kann man sich schützen?

Klären Sie alle Mitarbeiterinnen und Mitarbeiter über die Bedrohung auf! Das Bewusstsein ist auch bei Geschäftspartnerinnen und Geschäftspartnern sowie Lieferantinnen und Lieferanten zu steigern. Als Basismaßnahme wäre mittlerweile in jedem Unternehmen notwendig, dass Schutzprogramme für Systembeschränkungen und Virens Scanner installiert werden, die die anschließende Verbreitung im ganzen internen Unternehmensnetzwerk und die Ausführung der Schadsoftware mit ihrer automatischen Datenverschlüsselung verhindern können. Mittlerweile berücksichtigen komplexere Formen von Schadsoftware das gesamte Netzwerk mit etwaigen Datensicherungen.

- Seien Sie beim Öffnen von Dateianhängen und Links stets vorsichtig, selbst dann, wenn sie von einer bekannten Absenderin oder einem bekannten Absender kommt.
- Aktivieren Sie Makros in Office Dokumenten nur, wenn es erforderlich ist.
- Lassen Sie sich immer Datei-Erweiterungen anzeigen.
- Verwenden Sie zum Beispiel technische Spam- und Malware-Filter beim zentralen E-Mail-Eingang, gegebenenfalls auch am Web-Proxy und an anderen externen Schnittstellen sowie auch auf dem Desktop der Endnutzerin oder des Endnutzers, auf Servern, File Shares und dergleichen.
- Erstellen Sie ein vernünftiges Backup-Konzept und testen Sie regelmäßig Ihre Recovery-Maßnahmen. Hierbei wird geprüft, ob aus den erstellten Backups ein fehlerfreies Produktivsystem wiederhergestellt werden kann.
- Spielen Sie regelmäßig Ihre Security-Patches von allen verwendeten Applikationen in Ihrem Unternehmen ein!
- Überprüfen Sie alle Verbindungen zu IT-Dienstleistern, Fremdfirmen, Geschäftspartnerinnen und Geschäftspartnern sowie zu Ihren Cloud-Lösungen auf deren sichere Funktion!
- Verwenden Sie eine sehr geringe Zahl an Administratoren-Zugängen und überlegen Sie sich sichere Passwörter!
- Verwenden Sie im Unternehmen Whitelists zum Schutz vor unerlaubten Anwendungen!
- Erstellen Sie Notfallpläne mit Telefonlisten und legen Sie Kompetenzen vorab fest! Erstellen Sie dazu genaue Handlungsanweisungen!
- Gehen Sie Vorfälle durch Ransomware in Szenarien durch und richten Sie auch einen Fokus auf Ihre Liquidität!
- Schulen Sie Führungskräfte und Ihre Mitarbeiterinnen und Mitarbeiter!

Die Wirtschaftskammer Österreich (WKO) kann Ihnen zur Umsetzung der genannten Punkte im Bedarfsfall eine Liste von zertifizierten IT-Sicherheitsdienstleistern übermitteln!

Holen Sie sich besser eine externe Expertise von Expertinnen und Experten ein! Zudem kann eine externe Überprüfung durch ein anerkanntes und qualifiziertes IT-Security-Unternehmen eine gute Investition in die Zukunft darstellen und bietet einen wertvollen Direktkontakt für den späteren Ernstfall.

**Wenn Sie Opfer von Cyber-Kriminalität geworden sind, möchten wir Sie dazu ermutigen, strafrechtlich relevante Vorfälle bei der Polizei anzuzeigen.**

Die strafrechtliche Verfolgung der Täter und das Geltend machen der Schäden in einem späteren Zivilverfahren ist wichtig. Ebenso helfen die „Puzzlesteine“ jedes angezeigten Vorgangs bei den Ermittlungen durch die Spezialistinnen und Spezialisten im Bundeskriminalamt und in den Landeskriminalämtern.

## **Zusammenfassung aktueller Informationen zum Themenbereich**

### **Ransomware:**

Ransomware bleibt eine der größten Gefahren im Internet, um persönliche Daten zu verlieren. Bestehende Varianten von Ransomware werden technisch ständig weiterentwickelt und der Modus Operandi vom Weg der Infektion bis zur Lösegeldforderung den Umständen und Opfern flexibler angepasst. Setzen Sie präventive Maßnahmen dagegen!

Angriffe mit Ransomware erfuhren auch im letzten Jahr eine zielgerichtete Spezialisierung auf Unternehmen, bei denen die Geldforderungen der Täter an die wirtschaftliche Leistungsfähigkeit beziehungsweise an die vorhandene IT-Infrastruktur mit ihren Backup-Lösungen angepasst werden.

Die Infektion in Unternehmen hat immer häufiger den Ursprung in einer anderen Schadsoftware (Trojaner), die wochen- oder monatelang vor der eigentlichen Datenverschlüsselung das komplette Netzwerk oder Computersystem ausgespäht hat.

Die Angriffe lassen immer öfter auf eine hohe Befähigung und Kenntnisse organisierter Tätergruppen beziehungsweise Anbieterinnen und Anbietern von RaaS schließen.

Gewinnen Sie für das Risikomanagement einen Überblick über die wichtigsten Phänomene und Deliktsfelder!

Bereiten Sie sich dazu in Ihrem Unternehmen rechtzeitig auf mögliche und wahrscheinliche Straftaten im Bereich Ransomware und generell auf Angriffe durch Cyberkriminelle vor. Der Cybercrime-Report des Bundeskriminalamtes kann Ihnen dazu eine Hilfestellung geben!

Sichern Sie die unternehmenseigene IT-Infrastrukturen rechtzeitig ab!

Entwickeln Sie ein umfassendes internes und externes Informationsmanagement und vernetzen Sie sich mit Expertinnen und Experten sowie branchengleichen Firmen!

**Ergreifen Sie bei Ransomware zuerst die Initiative!**

**Beugen Sie zeitgerecht durch Maßnahmen vor!**

## RDDoS-Angriffe

Eine Sonderform von DDoS-Attacken stellten im vergangenen Jahr vor allem 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 ist die Angreiferin oder der Angreifer möglicherweise technisch gar nicht in der Lage den Angriff durchführen. 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.

Aufgrund der verwendeten Technik, der Angriffsmuster und der Methodik liegt es nahe, dass es sich bei etlichen Gruppierungen, wie beispielsweise den „Guardians of Peace“ um staatlich kontrollierte Akteure handelt.

## Suchtgifthandel im Darknet

Der Onlinehandel mit verbotenen Substanzen hat sich mittlerweile zu einer gängigen Begehungsform der Suchtmittelkriminalität entwickelt. Sowohl Einzeltäter als auch kriminelle Organisationen bedienen sich des Darknets 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 zeigen bislang, dass der Online-Drogenhandel den Straßenhandel nicht verdrängt. Vielmehr wird der Handel auf Online-Plattformen dazu genutzt, illegale Suchtmittel höherer Qualität zu erwerben, um diese im Straßenverkauf gewinnbringend weiterzuverkaufen. Der klassische Straßenhandel wird somit durch den Internethandel erweitert und ergänzt. 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 Briefsendungen durch das Zollfahndungsamt sichergestellt, die Suchtmittel zum Inhalt hatten. 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. Die rund 2.300 für Österreich bestimmten Postsendungen enthielten insgesamt über 268,5 Kilogramm Suchtgift, hauptsächlich Amphetamin und MDMA, einschließlich 41.115 Stück Ecstasy-Tabletten und 1.230 LSD-Trips. Auch in Österreich werden im Zuge von Kontrollen regelmäßig Postsendungen mit illegalen Suchtmitteln sichergestellt. Die Folgeermittlungen zu den bisherigen Sicherstellungen ergaben, dass das Suchtgift der aufgegriffenen Briefsendungen ausschließlich über Darknet-Marktplätze bestellt wurde. Etwa 80 Prozent der in Österreich sichergestellten Postsendungen wurde aus den Niederlanden versandt.

Um dieser Begehungsform der Suchtmittelkriminalität entgegenzutreten, wurde zu deren Bekämpfung bereits 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 sowie -händler und koordiniert die polizeilichen Maßnahmen gegen die Käuferinnen und Käufer. Neben den operativen Ermittlungsmaßnahmen werden durch das Fachreferat, teils im Wege des internationalen polizeilichen Informationsaustausches, fortwährend neue Strategien entwickelt und aktuelle Entwicklungen analysiert. Dadurch konnte festgestellt werden, dass zur Bekämpfung dieser Kriminalitätsform, die Zerschlagung der Vertriebswege eines der effektivsten Mittel darstellt. Die auf Darknet-Marktplätzen veräußerten 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 werden in enger Kooperation mit der österreichischen Zollverwaltung durchgeführt.

## Auswirkungen der COVID-19 Pandemie auf den Online-Suchtmittelhandel

Im Bereich des Suchtmittelhandels über Darknet-Marktplätze konnte hinsichtlich der Covid-19-Situation im Jahr 2021 betreffend Österreich Folgendes festgestellt werden:

Die Online-Suchtmittelhändlerinnen und -händler (Vendoren genannt) befürchteten zu Beginn der Pandemie 2020 eine mögliche Verstärkung der Kontrollen von Paketsendungen und Verzögerungen bei der Zustellung von Postsendungen.



Einige Vendors versendeten seitdem daher nur mehr im eigenen nationalen Bereich.

Es gab Beschwerden von Abnehmerinnen und Abnehmern über nicht erhaltene Bestellungen beziehungsweise, dass bei Verlust kein Ersatz versandt wurde. Es war eine vermehrte Unzufriedenheit unter den Käuferinnen und Käufern zu bemerken. Es stand der Vorwurf im Raum, die Händlerinnen und Händler würden die Covid-19-Situation als Ausrede für nicht erhaltene Bestellungen nutzen.

Es kann davon ausgegangen werden, dass es durch die beschränkten Liefermöglichkeiten vorerst zu einem Engpass bei der Zulieferung von Drogenausgangsstoffe für die Herstellung synthetischer Suchtmittel kam. Dies wirkte sich deshalb vor allem auch auf den Online-Suchtmittelhandel aus, da über die Darknet-Marktplätze in erster Linie synthetische Suchtgifte vertrieben werden.

Nach einem leichten Rückgang des Online-Suchtmittelhandels im Jahr 2020, normalisierte sich die Lage auf den Darknet-Marktplätzen wieder. Zusammengefasst nahm der Onlinehandel im Laufe des Jahres 2021 wieder jene Form an wie vor Beginn der Pandemie.

Insbesondere kann bei den österreichischen Verkäuferinnen und Verkäufern wieder ein Anstieg festgestellt werden.

## Pornographische Darstellungen Minderjähriger

Im Bereich dieses Tatbestandes stellte sich 2021 die Gesamtsituation ähnlich wie in den Jahren zuvor dar. Das ist auf den Umstand eines verstärkten Kampfes gegen die Verbreitung von Online-Kindesmissbrauch durch soziale Medien zurückzuführen. Die Inhalte der Benutzerinnen und Benutzer werden vor allem in den USA verstärkt auf pornografische Inhalte überprüft. Inhalte mit Online-Kindesmissbrauch 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 oder die Verursacherin zugeordnet werden kann.

Im Jahr 2021 kam es zur Übermittlung von 5.869 derartiger Verdachtsmeldungen durch Internet Service Provider an das Bundeskriminalamt beziehungsweise gingen darüber hinaus 372 Hinweise mit 6.115 verdächtigen Links in die Meldestelle für Sexualstraftaten und Kinderpornografie zur weiteren Bearbeitung ein.

Positiv hervorzuheben ist jedenfalls die Tatsache, dass es dem zuständigen Referat Sexualstraftaten und Kinderpornografie des Bundeskriminalamtes und den nachgeordneten Dienststellen gelungen ist, die Aufklärungsquote im Bereich des § 207a Strafgesetzbuch (StGB - Pornographische Darstellungen Minderjähriger) gegenüber dem Vorjahr um 2,6 Prozentpunkte zu heben.

§ 207a StGB (Pornographische Darstellungen Minderjähriger)	Straftatenanzahl	Anzahl geklärt	Aufklärungsquote
Jahr 2012	572	535	93,5 %
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 %
Veränderung z VJ	12,9 %	16,2 %	2,6 %-Punkte

Tabelle 1:  
10 Jahres-Vergleich des  
§ 207a StGB

# 3 Jahresrück- blick



## Zahlen und Fakten im Überblick

Die nachfolgenden Zahlen und Daten stammen in bewährter Weise aus der öffentlich verfügbaren und offiziell verlautbarten PKS. Bereits im Vorjahr erwähnte Faktoren, wie die Covid-19-Pandemie im besonderen Ausmaß und beispielsweise rechtliche Herausforderungen, spiegeln sich deutlich in der Kriminalitätsentwicklung. Eine starke Zunahme der begangenen Straftaten im Cybercrime-Bereich kann auch im Jahr 2021 beobachtet werden. Dieser Trend wurde durch die Pandemie und die anhaltende Verlagerung vieler Lebensaspekte in die digitale Welt zusätzlich verstärkt.

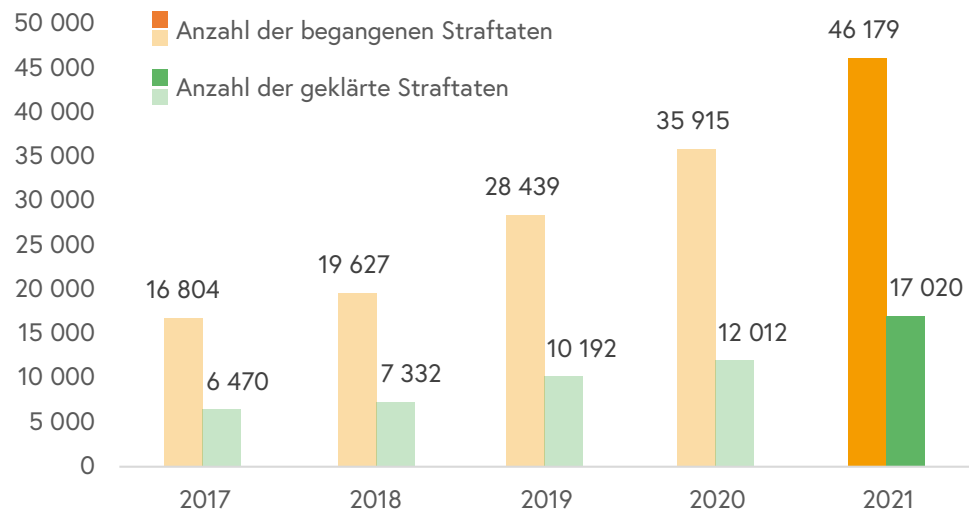
Cybercrime im 5-Jahresvergleich			
Jahr	Anzahl der angezeigten Straftaten	Anzahl der geklärten Straftaten	Aufklärungsquote (gerundet)
2017	16.804	6.470	38,5 %
2018	19.627	7.332	37,4 %
2019	28.439	10.192	35,8 %
2020	35.915	12.012	33,4 %
2021	46.179	17.020	36,9 %

Tabelle 2:  
Entwicklung der Anzeigen, geklärten Fälle und der Aufklärungsquote von Cybercrime 2017 bis 2021 (Fünf-Jahres-Vergleich)

Veränderung der Aufklärungsquote in %-Punkten im Vergleich zum Vorjahr			
	Jahr 2020 33,4 %	Jahr 2021 36,9%	+3,4 %-Punkte

Die Entwicklung der Internetkriminalität in den letzten fünf Jahren zeigt, dass mit 46.179 Anzeigen und einer Zunahme von 28,6 Prozent gegenüber dem Vorjahr ein neuer Spitzenwert erreicht wurde. Der Aufwärtstrend setzt sich somit kontinuierlich fort, denn im Vergleich zum Jahr 2018 wurden mehr als doppelt so viele Straftaten angezeigt. Trotz des erneut beachtlichen Zuwachses konnte 2021 die prozentuelle Aufklärungsquote um 3,4 Prozentpunkten im Vergleich zum Vorjahr deutlich gesteigert werden. In absoluten Zahlen konnten rund 5.000 zusätzliche Straftaten erfolgreich aufgeklärt werden, was einer bedeutenden Steigerung entspricht.

Abbildung 4:  
Entwicklung der Anzeigen  
und aufgeklärten Fälle von  
Internetkriminalität 2017 bis  
2021



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

## 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 Kommunikationstechnik (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 DDoS-Angriffen.

Im Jahr 2021 musste bei Tatbeständen zu Cybercrime im engeren Sinn ein kräftiger Gesamtanstieg der Anzeigen in der Höhe von 19,9 Prozent gegenüber dem Vorjahr verzeichnet werden.

Massive Steigerungen wurden erneut beim betrügerische Datenverarbeitungsmissbrauch § 148a StGB erreicht. Mit über 12.000 angezeigten Fällen entspricht das einer Steigerung von 130 Prozent im Vergleich zu 2019. Eine beträchtliche Steigerungsrate wurde auch bei § 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten) verzeichnet, bei dem die Erhöhung mit 52,5 Prozent im Jahresvergleich zu Buche schlägt. Trotz der massiven Zunahme angezeigter Fälle konnten 2.895 Straftaten aufgeklärt werden und das Vorjahresniveau in absoluten Zahlen um 436 in diesem Bereich übertroffen werden. Die relative Aufklärungsquote sank jedoch leicht aufgrund der verzeichneten Anzeigenzuwächse auf 18,7 Prozent.

Delikt	Angezeigte Fälle 2020	Angezeigte Fälle 2021	Geklärte Straftaten 2020	Geklärte Straftaten 2021
§ 107c StGB	329	395	253	299
§ 118a StGB	816	952	113	165
§ 119 StGB	12	14	5	11
§ 119a StGB	67	58	12	4
§ 126a StGB	361	354	78	64
§ 126b StGB	71	95	10	12
§ 126c StGB	354	540	66	46
§ 148a StGB	10603	12 701	1723	2182
§ 225a StGB	301	375	199	112
<b>Gesamt</b>	<b>12914</b>	<b>15484</b>	<b>2459</b>	<b>2895</b>

Tabelle 3:  
Angezeigte Fälle und geklärte Straftaten von Cybercrime im engeren Sinn nach Paragrafen des StGB 2021 im Vergleich zu 2020.

§ 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)

## Cybercrime im weiteren Sinn (IKT als Tatmittel)

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

Der Internetbetrug erreichte 2021 mit 22.440 angezeigten Fällen erneut einen neuen Höchststand. Die Anzahl der angezeigten Fälle von Betrugsformen im Internet §§ 146 bis 148 StGB folgten mit einem Anstieg von 19,5 Prozent dem stetig steigenden Trend der vergangenen Jahre. Auf den gesamten Bereich Cybercrime gerechnet stellt der Internetbetrug nahezu die Hälfte aller Anzeigen dar. Auch die sonstige Kriminalität im Internet stieg deutlich an (2021: 8.255 angezeigte Fälle, 2020: 4.221). Nichtsdestotrotz

konnte in nahezu allen Bereichen die Zahl der geklärten Straftaten deutlich erhöht werden. Bei prozentueller Betrachtung ging die Aufklärungsquote beim Internetbetrug leicht zurück (minus 1,9 Prozentpunkte gegenüber dem Vorjahr).

Zuwächse im Bereich der sonstigen Kriminalität im Internet sind auf gestiegene Zahlen beispielsweise bei § 107 StGB (gefährliche Drohung), § 107a StGB (beharrliche Verfolgung), § 207a StGB (pornographische Darstellungen Minderjähriger), aber auch aufgrund von Anzeigen nach dem Suchtmittel- (§ 27 SMG) sowie dem Verbotsgesetz (§ 3g Verbotsg) zurückzuführen.

Auch Delikte im Zusammenhang mit §144 StGB (Erpressung), die im Internet in den vergangenen Jahren vor allem durch die Versendung von Massenerpressungs-E-Mails und die Infizierung mit Ransomware begangen wurden, nahmen wieder deutlich zu.

Tabelle 4:  
Jahresvergleich 2020 und  
2021: Angezeigte Fälle von  
Cybercrime im weiteren Sinn  
nach Paragraphen

Delikt	Angezeigte Fälle 2020	Angezeigte Fälle 2021	Geklärte Straftaten 2020	Geklärte Straftaten 2021
<b>Internetbetrug</b>				
§ 146 StGB	16.279	19.224	5.639	7.138
§ 147 StGB	1.761	2.246	580	701
§ 148 StGB	740	970	407	509
<b>Internetbetrug- Gesamt</b>	<b>18.780</b>	<b>22.440</b>	<b>6.626</b>	<b>8.348</b>
<b>Sonstige Kriminalität im Internet</b>				
§ 105 StGB	0	47	0	30
§ 106 StGB	0	23	0	17
§ 107 StGB	0	1.303	0	1.124
§ 107a StGB	1	459	1	423
§ 115 StGB	0	88	0	80
§ 144 StGB	778	1.639	83	111
§ 145 StGB	72	165	13	20
§ 207a StGB	1.702	1.921	1.528	1.775
§ 207b StGB	22	9	21	9
§ 208a StGB	142	121	102	87
§ 218 StGB	7	18	4	12
§ 223 StGB	45	87	30	60
§ 224 StGB	23	25	16	19
§ 228 StGB	1	0	1	0

§ 229 StGB	1	0	0	0
§ 231 StGB	38	37	15	19
§ 232 StGB	13	16	10	10
§ 241a StGB	1	1	1	0
§ 283 StGB	2	262	2	246
§ 27 SMG	1.154	1.201	905	941
§ 28 SMG	9	15	8	15
§ 28a SMG	63	45	58	40
§ 30 SMG	29	31	26	29
§ 31 SMG	0	1	0	1
§ 31a SMG	0	1	0	1
§ 3a VerbotsG	0	3	0	2
§ 3d VerbotsG	0	2	0	2
§ 3g VerbotsG	118	651	103	624
§ 3h VerbotsG	0	84	0	80
<b>Sonstige Kriminalität im Internet gesamt</b>	<b>4.221</b>	<b>8.255</b>	<b>2.927</b>	<b>5.777</b>
<b>Internetkrimi- nalität gesamt</b>	<b>35.915</b>	<b>46.179</b>	<b>12.012</b>	<b>17.020</b>

## Dunkelziffer und Anzeigeverhalten

Die Dunkelziffer im Bereich der Internetkriminalität ist unter Berücksichtigung internationaler Studien 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 könne.

Jedoch kann mit jedem angezeigten Vorfall die Beweismittellage zu verdächtigen Tätergruppen weiter verdichtet werden. Außerdem verbessert die Anzahl der Anzeigen die frühere Erkennung von neuen Massenphänomenen für die ermittelnden Strafverfolgungsbehörden. Ebenso können Präventionsmaßnahmen zeitnaher gesetzt werden und mit zielgerichteten Warnhinweisen an die Bevölkerung die Anzahl der Geschädigten reduziert werden. Eine Wiedererlangung abhanden gekommener Vermögenswerte gelingt jedoch selbst nach internationaler Ausforschung der Täter nur in den seltensten Fällen. Deshalb gebührt im Bereich des Internetbetrugs der Verhinderung von Straftaten durch verstärkte Bewusstseinsbildung und Aufklärung erhöhte Aufmerksamkeit. Die



Täter nutzen menschliche Schwächen, wie Gier und Sehnsüchte nach Anerkennung oder Beziehungen aus, um sich zu bereichern. Auch im Jahr 2021 blieb Social Engineering ein maßgeblicher Angriffsvektor.

4

# Aufbau- organisation und Abläufe



## Nationale und internationale Koordinierungs-, Ermittlungs- und Meldestelle

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

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

## Meldestelle

Die Meldestelle zur Bekämpfung der Internetkriminalität ist seit knapp zehn Jahren im C4 etabliert und ist in einem 24/7 Betrieb rund um die Uhr erreichbar. Durch diese können umgehend die erforderlichen Maßnahmen zur Gefahrenabwehr eingeleitet werden. 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 2021 erreichten die Meldestelle 15.202 schriftliche und telefonische Anfragen, wobei 13.183 davon einen Bezug zu Cybercrime hatten. Damit konnte erneut eine Zunahme im Vergleich zum Vorjahr festgestellt werden (2020: 14.988 Gesamt beziehungsweise 11.576 relevant). Die allgemeinen Steigerungsraten im Cybercrime-Bereich während des Vergleichszeitraumes spiegeln sich somit auch in der Meldestelle wider.

In ihrer zentralen Funktion als Cybercrime-Schnittstelle innerhalb polizeiinterner Strukturen sowie als Meldestelle für Bevölkerung und Wirtschaft, agiert die Meldestelle als Koordinierungs- und Informationszentrum für diesen Themenkreis. Zusätzlich umfasst diese Tätigkeit auch proaktive und präventive Maßnahmen, wobei auftretende Phänomene, insbesondere im Bereich von Phishing-Attacken, auch ministeriumsübergreifend koordiniert und die notwendigen Maßnahmen eingeleitet werden. Die deutlich erkennbare Sensibilisierung und Bewusstseinsbildung zum Thema Cybercrime erfolgte einerseits durch die fortlaufende Kooperation mit unterschiedlichen Institutionen aus dem Bereich der Wirtschaft und Vereinen, wie beispielsweise der WKO oder der Initiative „Watchlist

Internet“, die unter [www.watchlist-internet.at](http://www.watchlist-internet.at) erreichbar ist. Ebenso führen Erstanalysen der eingehenden Meldungen zu schnellen Informationsweitergaben aktueller Phänomene, damit akute, negative Auswirkungen minimiert werden können. Für diese Aufgaben ist ein technischer Journaaldienstbetrieb eingerichtet, der in dringenden Fällen organisationsübergreifende Informations- und Sofortmaßnahmen einleiten kann.

Da die Meldestelle zudem als Drehscheibe zu anderen internationalen Dienststellen und Polizeieinheiten, wie dem INTERPOL Digital Crime Centre (IDCC), dem European Cybercrime Centre (EC3), und den jeweiligen High-Tech Crime Units anderer Staaten (NCPs) fungiert, konnte auch im Bereich der internationalen Anfragen und Unterstützungsmaßnahmen, insbesondere im Hinblick auf Vorabsicherungen von Daten und diesbezüglichen Ermittlungen im Sinne der Budapest Cybercrime Convention, ein entsprechender Anstieg der Anfragen und damit verbundene Ermittlungsaufgaben vermerkt werden.

#### Kontakt:

Bundeskriminalamt - Meldestelle Cybercrime

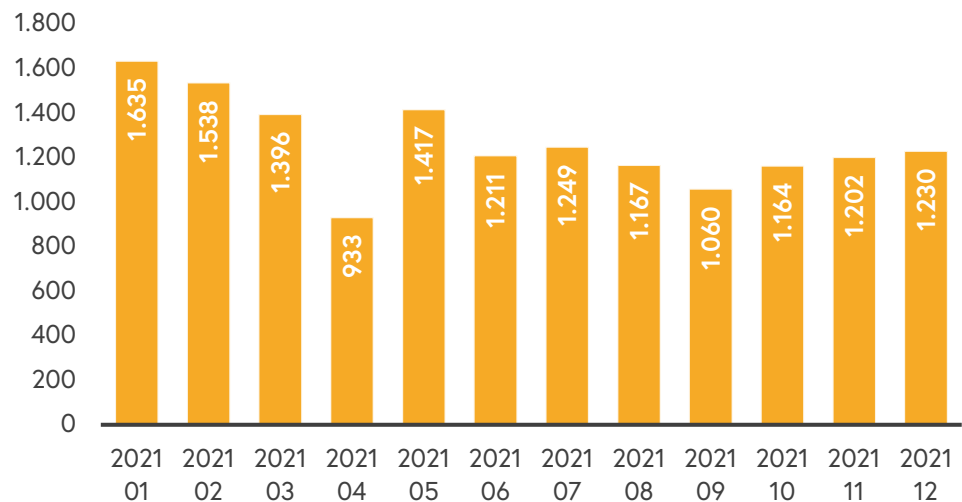
Josef-Holaubek-Platz 1, 1090 Wien

E-Mail: [against-cybercrime@bmi.gv.at](mailto:against-cybercrime@bmi.gv.at)

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
Januar	1.109	420	106	1.215	1.635
Februar	1.262	177	99	1.361	1.538
März	1.139	169	88	1.227	1.396
April	797	52	84	881	933
Mai	1.207	115	95	1.302	1.417
Juni	1.033	125	53	1.086	1.211
Juli	853	301	95	948	1.249
August	968	121	78	1.046	1.167
September	833	160	67	900	1.060
Oktober	955	127	82	1.037	1.164
November	983	139	80	1.063	1.202
Dezember	1.063	113	54	1.117	1.230

Tabelle 5:  
Monatliche Übersicht aller Meldungen an die C4-Meldestelle

Abbildung 5:  
Gesamtanzahl der Meldungen an die C4-Meldestelle nach Monaten 2021



## Digitales Beweismittelmanagement (DBM)

Der Bereich „Digitales Beweismittelmanagement“ (DBM) im C4 fasst die Kompetenzen zusammen, die für eine zeitgemäße kriminalpolizeiliche Bearbeitung komplexer Fälle mit großen Datenmengen notwendig sind. Das umfasst die technische Aufbereitung sichergestellter digitaler Beweismittel für eine systematische Indizierung und nachfolgende Bereitstellung für die Ermittlungsbereiche im Bundeskriminalamt und bei Bedarf der Landeskriminalämter sowie das Fallmanagement als Schnittstelle zwischen Forensikerinnen und Forensikern, Ermittlerinnen und Ermittlern sowie Technikerinnen und Technikern und der Justiz.

Die Auswahl, Inbetriebnahme und laufende Betreuung moderner Auswertesoftware gehört dabei ebenfalls 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 Forensiker

Etablierung einer Schnittstelle zwischen beteiligten kriminalpolizeilichen Fachbereichen zur optimierten, reibungsfreien Fallbearbeitung

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

Mithilfe spezieller Programme zur Sichtung großer Datenmengen wurden 2021 insgesamt 29 neue Fälle mit einem Analyseausgangsdatenvolumen von über 110 TByte erstellt. Zusätzlich wurden 49 separate virtuelle Maschinen zur Beweismittelsichtung und fall-bezogenen Recherche in Betrieb genommen, womit insgesamt knapp 500 Ermittlerinnen und Ermittler im Bundeskriminalamt und den LKAs Zugriff auf eine moderne Arbeits-umgebung zur Strafverfolgung erhalten haben.

Eine der wesentlichen Herausforderungen im Jahr 2021 stellte überdies die Übersiedlung des C4 innerhalb Wiens dar. Dabei wurden vorbereitend am neuen Standort über 100km Strom- und Netzwerkleitungen verlegt und ein zeitgemäßer Serverraum ausgestattet, um das notwendige Equipment (Server, Speicher und Netzwerkkomponenten) mit einer Masse von mehr als vier Tonnen gut gekühlt unterzubringen. Der Transport der sensiblen Ausrüstung und der darauf gespeicherten Daten erfolgte mit zivilem Begleitschutz auf vorab nicht bekanntgegebener Route, um das Risiko einer absichtlichen Datenbeschä-digung zu reduzieren.

## IT-Forensik

Die Auswertung von IT und Speichermedien stellten die Mitarbeiterinnen und Mitarbeiter erneut vor große Herausforderungen. Nach wie vor sind unzählige Geräte mit beträcht-lichen Datenmengen aufzubereiten, um die ressourcenintensive Unterstützung der Er-mittlerinnen und Ermittler zu gewährleisten. Eine Tatsache, die an den untenstehenden Statistiken deutlich abgelesen werden kann. So lässt sich im Bereich der IT-Forensik nahezu eine Verdoppelung der Datenmenge im Jahresvergleich feststellen. Die Mobile Forensik ist ebenfalls mit einer starken Zunahme konfrontiert.

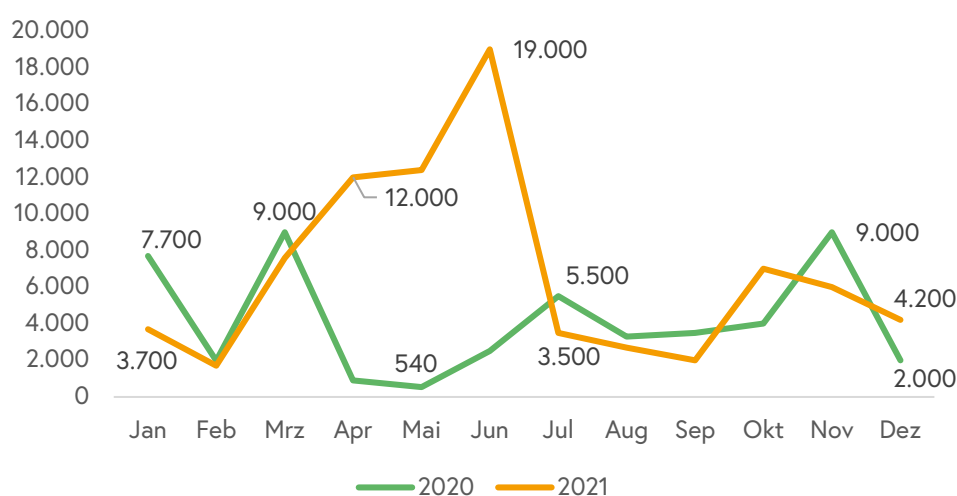
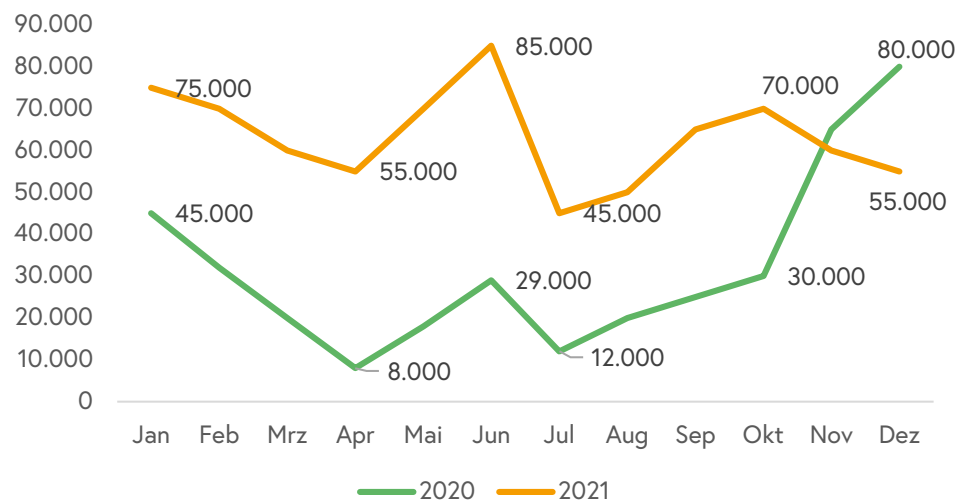


Abbildung 6:  
Mobile Forensik, Jahresver-  
gleich der ausgewerteten  
Datenmengen in Gigabyte  
(GB)

Auch 2021 war der Support der C4 Forensik ein unverzichtbarer, wesentlicher Bestandteil strafrechtlicher Ermittlungen. Die gesamte Datenmenge forensischer Auswertungen war im Vergleich zum Vorjahr stark steigend. Es fanden deutlich mehr Hausdurchsuchungen als im Jahr zuvor statt. Der elektronischen Beweismittelsicherung im C4 und den Landeskriminalämtern kommt weiterhin essentielle Bedeutung in der Ermittlungsarbeit zu.

Aufgrund der rasanten technischen Entwicklung wird die Auswertung diverser Medien allerdings immer schwieriger. Herstellerspezifische Systeme mit ausgeprägten Verschlüsselungsverfahren stellen die elektronische Beweissicherung fortwährend vor große Herausforderungen. Insbesondere im Bereich der mobilen Forensik werden Datensicherungen und Auswertungen immer komplexer. Die steigenden Zahlen zu forensischen Tätigkeiten erklären sich ebenso mit den zunehmend umfassenden Auswertungen von Smartphones und Clouds, die zum Teil von den Landeskriminalämtern nicht mehr bewältigt werden können. Die auszuwertenden Datenmengen (Festplatten, Netzwerkdaten, auch bei Mobiltelefonen) nehmen stetig zu.

Abbildung 7:  
IT-Forensik, Jahresvergleich  
der ausgewerteten Daten-  
mengen in GB



Das zeit- und ressourcenaufwendige Chip Off-Verfahren, bei dem Memory-Chips von ihrer Hardware physisch entfernt werden sowie der Bereich Kfz-Forensik, können nur zentral im C4 durchgeführt werden. Die Anzahl der Chip Off-Verfahren war 2021 deutlich im Steigen begriffen.

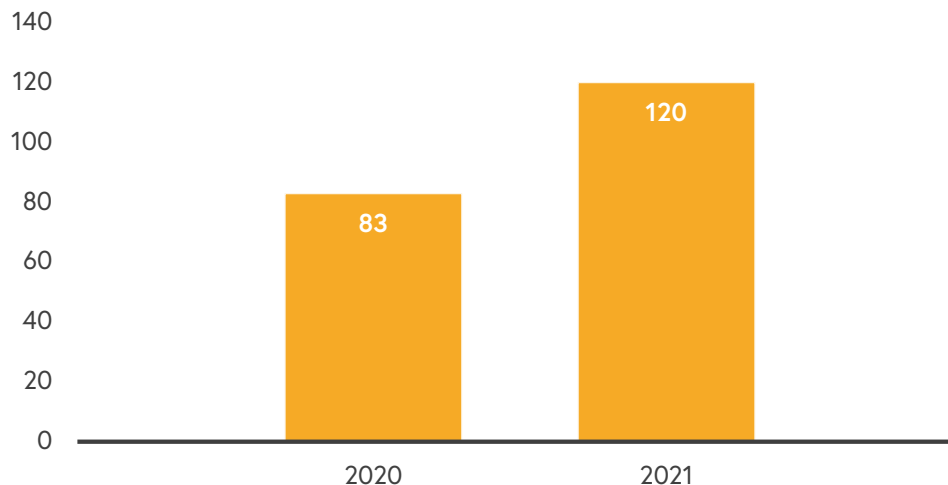


Abbildung 8:  
Durchgeführte Chip Off Ver-  
fahren im Jahresvergleich

## Fahrzeugforensik und Automotive-IT

Im Bereich der Fahrzeugforensik und der Automotive-IT, welche 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 vermehrt zu Auswertungen in Zusammenhang mit schweren Straftaten.

Key-Learning as a Service (KlaaS): Moderne Autos haben immer mehr elektronische Komponente, die nicht nur mit der Lenkerin oder dem Lenker, sondern auch mit der Außenwelt durch eine WLAN-, Internet- oder Bluetooth-Verbindung kommunizieren können. Die fortschreitende Technisierung befähigt weiterhin in zunehmenden Maßen kriminelle Organisationen, das Signal eines Transponderschlüssels abzufangen, um sich so Zugang zum Fahrzeug zu verschaffen („Extender“ beziehungsweise „Keyless-Relais-Attack“), beim Fahrzeug einen neuen Schlüssel zu programmieren beziehungsweise „Remote“ programmieren zu lassen (Key Learning as a Service) oder die elektronische Wegfahrsperre zu deaktivieren, um das Fahrzeug unberechtigt in Betrieb nehmen zu können. Die Experten der Kfz-Forensik des Bundeskriminalamtes haben diese neue Diebstahlsmethode (Key Learning as a Service) erfolgreich identifizieren können.

Ein weiterer Anstieg von Anfragen konnte in Zusammenhang mit schweren und tödlichen Verkehrsunfällen festgestellt werden, wobei der Schwerpunkt auf die Sicherung von Crashdaten (EDR-Event Data Recorder) gerichtet war. Diese Crashdaten können in Zusammenhang mit herkömmlichen Untersuchungsschritten maßgeblich zur Rekonstruktion des Unfallhergangs beitragen, da wichtige digitale Informationen über Fahr-



manöver in engem zeitlichem Zusammenhang mit dem Unfallereignis analysiert werden können. Dieser Umstand wurde auch seitens der EU-Kommission thematisiert, wodurch konventionelle Personenkraftfahrzeuge ab 2022 verpflichtend mit einem EDR-System ausgestattet werden sollen. Der aktuelle Entwurf sieht allerdings vor, dass diese Crash-daten zukünftig keine Orts-, Datums- und Zeitangaben mehr enthalten sollen, wodurch diesen Informationen keine faktische Beweiskraft mehr zukommen würde. Derartige Entwicklungen werden genauestens durch den Fachbereich beobachtet und in internationalen Gremien behandelt. Die Mitarbeiter der Kfz-Forensik sind beispielsweise Teil der Fachgruppe Automotive-IT bei Europol, stehen laufend in Kontakt mit Interpol, aber auch mit der Automobilindustrie und deren Vertreterinnen und Vertretern. Hierbei gilt es zukünftige Entwicklungen zu erkennen, welche nicht vernachlässigbare Auswirkungen auf die polizeiliche Ermittlungsarbeit und digitale Beweissicherung haben. Dazu zählt beispielsweise der stetig steigende Anteil an Elektrofahrzeugen, die Vernetzung von „intelligenten“ Kraftfahrzeugen untereinander sowie mit Verkehrsinfrastruktur und die fortschreitende Technik in Bezug auf teilautonomes beziehungsweise autonomes Fahren.

## Entwicklung und Innovation

Sowohl im Bereich der Cybercrime Ermittlungen als auch der digitalen Forensik gibt es immer wieder den Bedarf, die Kolleginnen und Kollegen mit Tools und Skripten zu unterstützen. Diese werden maßgeschneidert gemeinsam mit den Bedarfsträgerinnen und Bedarfsträgern entwickelt. Schwerpunkte dazu waren im Jahr 2021 wieder die Bereiche Kryptowährungen, digitale Ermittlungen und Forensik, aber auch Analyse von Malware. Sofern festgestellt wird, dass diese Werkzeuge auch bei anderen Fällen nützlich sein können, werden sie nicht nur national, sondern auch international, über das Europol Projekt SIRIUS, für Strafverfolgungsbehörden zur Verfügung gestellt. Gerade im Bereich der digitalen Ermittlungen ist es erforderlich, große Datenmengen flexibel und effizient abzuarbeiten, das Wesentliche daraus zu erkennen und optimal für die weitere Tätigkeit der Kriminalpolizei zu verwerten. Dabei ist es notwendig, nicht ständig „das Rad neu zu erfinden“, sondern auch Synergien zwischen den Entwicklungsbereichen verschiedener Strafverfolgungsbehörden optimal zu nutzen.

Sicherheitsforschung im Cybercrime-Bereich war einer der zentralen Punkte des vergangenen Jahres, um die organisatorischen und technischen Strukturen von Täterschaften besser abschätzen zu können. Die Praxisorientierung ist notwendig, um operativen Ermittlerinnen und Ermittlern die erworbenen Kenntnisse und Informationen für zielführende Ermittlungen weiterzugeben. Durch den raschen und flexiblen Informationsaustausch, den weiter anwachsenden „Cybercrime Communities“ sowie den zahlreichen CaaS-Angeboten wird es deutlich schwerer, verschiedene Vorgehensweisen der Täterschaften und kriminelle Strukturen zu verstehen. Daher ergeben sich ähnlich gelagerte Ziele

mit dem Bereich der Cybersicherheit, die jedoch für den Kriminalitätsbereich andere Fragestellungen erfordern.

## Wissensvermittlung durch Ausbildung und internationalen Austausch

Bereits seit dem Jahr 2012 findet eine grundlegende Ausbildung von Bezirks-IT-Ermittlerinnen und -Ermittlern statt. Mittlerweile unterstützen mehr als 300 speziell ausgebildete Kolleginnen und Kollegen durch fachgemäße Erstmaßnahmen und Ermittlungen auf lokaler Ebene. Die Vortragenden werden aus den besten Expertinnen und Experten der Landeskriminalämter und dem Bundeskriminalamt rekrutiert. Einem größeren polizeilichen Bereich wird das Thema Cybercrime insbesondere im Rahmen der Kriminaldienstfortbildungsrichtlinie (KDFR) sowie in den Grundausbildungslehrgängen zugänglich gemacht.

Auch im Jahr 2021 wurde der Ausbildungsbereich durch Covid-19 und den damit verbundenen Schutzmaßnahmen vor große Herausforderungen gestellt. Präsenzkurse konnten nur teilweise und mit Einschränkungen durchgeführt werden. Das C4 hat unter Nutzung der eigenen Webinar-Plattform die geeigneten Module der Bezirks-IT-Ermitterschulung 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-relevanten Themen allen interessierten Ermittlerinnen und Ermittlern sowie Vertreterinnen und Vertretern der Staatsanwaltschaften präsentiert.

Aufgrund von Covid-19 mussten besonders geschulte Präventionsbeamtinnen und -beamte, die insbesondere für Klein- und Mittelbetriebe, aber auch für die interessierte Allgemeinheit im Einsatz waren, die meisten Präsenzveranstaltungen absagen.

Das C4 vertritt Österreich zudem auf internationaler Ebene im Themenbereich Aus- und Fortbildung bei Cybercrime in der European Cybercrime Training and Education Group (ECTEG).

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

Bei manchen 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 auch 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 für einzelne Ermittlungen aus.

Durch die gewonnenen Informationen der Providieranfragen können im Anlassfall 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 ist einheitliche, klare und einfach geregelte Ablaufprozesse künftig zentral abzuwickeln und das dort gewonnene Knowhow den Kolleginnen und Kollegen zur Verfügung zu stellen.

Damit entsteht eine verstärkte Unterstützung für die einzelnen Ermittlungsbereiche und es konnte ein höherer Output generiert werden. Ebenso plädieren zahlreiche Diensteanbieter ihrerseits bereits 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 den Vertreterinnen und Vertretern der Social Media Anbieter, sondern ist auch Ansprechstelle für Anfragen aller Polizeidienststellen Österreichs und der Justiz.

Mit 01. September 2020 wurde im C4 ein Probetrieb 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 diese Quote auf rund 80 Prozent positiver Beantwortungen gesteigert werden, eine Tatsache die internationalen Standards in diesem Bereich entspricht.

Aufgrund positiver Evaluierung wurde der Probetrieb mit 15. Februar 2022 in einen Vollbetrieb für das gesamte Bundesgebiet übergeleitet. Mit Stand 15. März 2022 wurden über die ZASP rund 440 Fälle abgehandelt und dabei etwa 650 Accountanfragen gestellt, darunter auch Auskünfte zu den Tatbeständen „Gefährliche Drohung“, „Kinderpornografie“ und „Erpressung“.

Der Konzern Meta war der erste Partner in der Zusammenarbeit mit der ZASP, wodurch die Kooperation gerade bei Fällen schwerer Kriminalität auf ein höheres Level angehoben werden konnte. Die neue kriminalpolizeiliche Einheit kann als erfolgreiches Beispiel für zukunftsgerichtete Kooperationen zwischen Behörden und Plattformen angesehen werden.

Zukünftig kann davon ausgegangen werden, dass ebenso Anfragen an weitere Social Media Plattformen und Service Provider über die ZASP zentral für ganz Österreich abgewickelt werden. Hierdurch soll Cyberkriminalität noch effizienter und schneller bekämpft werden können.

## Erstattung einer Anzeige

Sind Sie Opfer eines Cybercrime-Delikts 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/Leben), dann rufen Sie den Polizeinotruf 133 an.

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

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

Häufig haben Sie auch selbst die Möglichkeit, bei den von Ihnen betroffenen Accounts, Informationen zu erfragen, die für eine Tätersausforschung notwendig sind. Exemplarisch sind das IP-Adressen über widerrechtliche Zugriffe inklusive Zeitstempel, Logdaten, und dergleichen. Überprüfen Sie dazu am besten selbst, welche der für die Tathandlung relevanten Daten beim jeweiligen Account-Anbieter beziehungsweise Online Service Provider gespeichert werden und für Sie zugänglich sind oder deren Bekanntgabe über diesen angefordert werden kann.

Wenn es sich um komplexere Tathandlungen handelt, dokumentieren Sie den Tathergang in chronologischer Weise und stellen Sie sicher, dass die Geschehnisse zeitlich richtig eingeordnet sind.

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

Stellen Sie die gesicherten Daten der aufnehmenden Beamtin oder dem Beamten nach Absprache mit dieser oder diesem 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.

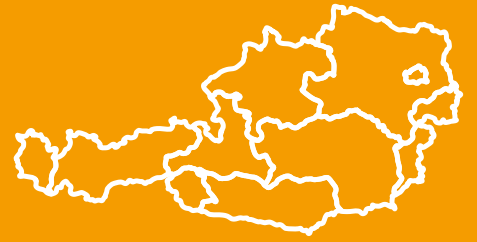
Bitte haben Sie Verständnis dafür, dass Sie bei einem ersten Gespräch mit der Polizei nicht unmittelbar auf spezialisierte Cybercrime-Expertinnen und -Experten treffen und deshalb in den meisten Fällen erst in einem zweiten Schritt an eine spezialisierte Fachdienststelle weitergeleitet werden oder von 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 aufzusuchen. Derzeit ist eine formelle Anzeigeerstattung über die Meldestelle nicht vorgesehen.

Kontakt zur Meldestelle: [against-cybercrime@bmi.gv.at](mailto:against-cybercrime@bmi.gv.at)

5

# Cybercrime- Bekämpfung in den Bundesländern



## Best practices

Zu den großen polizeilichen Herausforderungen hinsichtlich der Bekämpfung von Cybercrime- auf Landesebene gehören in technischer Hinsicht die enorm gestiegenen Datenmengen im Bereich der Mobilforensik, die sich jedes Jahr nahezu verdoppelt haben.

Große Herausforderungen liegen in den von Tätern verwendeten Anonymisierungsdiensten (VPN, VPS), die eine Verfolgung der digitalen Spuren erheblich erschweren und oft sogar unmöglich machen. Hier gilt es, die technische Infrastruktur der Kriminalpolizei auch auf Länderebene entsprechend zu modernisieren und Ermittlungsbediensteten Fortbildungen am aktuellsten Stand zu ermöglichen. Im Bereich der zunehmend komplexen Cybercrime-Ermittlungen 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. Der Anspruch an die fachliche Qualifikation ist gestiegen, weshalb der Bereich der Aus- und Fortbildungen laufend erweitert und bundesweit entsprechende Anreize für Interessentinnen und Interessenten geschaffen werden sollten.

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 Landeskriminalamt.

## Kärnten

Aufgrund der enorm gestiegenen Datenmenge im Bereich der Mobilforensik, wird vor allem in Kärnten eine laufende und skalierbare Speicherlösung benötigt, bei der aus Sicherheitsgründen auch auf eine entsprechende Redundanz geachtet werden sollte.

Als einer der größten Wachstumsbereiche innerhalb der Cybercrime-Delikte sind die verschiedensten Varianten von Anlagebetrug mit virtuellen Währungen zu sehen. Bekannte Phänomene, wie Ransomware, Sextortion (Erpressungen mit bildlichen Darstellungen sexueller Inhalte von meist männlichen Opfern) und Love Scam fallen auch weiterhin in regelmäßigen Abständen auf allen Dienststellen in Kärnten an. Als Fortschritt in diesen Bereichen können analog den gestiegenen Anlagedelikten auch die immer besser werdenden Ermittlungsmöglichkeiten durch Blockchain-Analysesoftware gesehen werden. Erhebungen können hierdurch effizienter und zielorientierter geführt werden. Auch im

Bereich der Fahrzeugforensik führen immer umfangreichere Informationen zur besseren Aufklärung von Sachverhalten.

### **Erfolge und besondere Leistungen**

Im Bereich der Kryptowährungen kommt es nicht nur zu einem erhöhten Anfall, sondern auch zu einer zunehmenden Menge an Sicherstellungen an Bitcoins und anderen Währungen. Allein im Landeskriminalamt Kärnten ist der Aktenanfall von 2020 auf 2021 um über 400 Prozent gestiegen. Dabei konnten insgesamt 72 beteiligte Personen als Geldempfängerinnen und Geldempfänger illegaler Geldflüsse im Bereich digitaler Währungen überführt werden.

### **Strategische Entwicklungen und Ausblick in Kärnten**

Die Tendenz im Bereich Cybercrime entspricht dem österreichweiten Trend und führt zu einer zusätzlichen Bindung von Polizeikräften, die als Aktenführer auch für die Sichtung anderweitiger Akte zuständig bleiben werden. Um den Entwicklungen entgegenzuwirken und für die Zukunft gerüstet zu sein, wurde im Landeskriminalamt Kärnten der Probetrieb Cybercrime-Ermittlungen gestartet. Hierbei wird Cybercrime deliktsübergreifend bearbeitet. Beamtinnen und Beamte werden aus allen Bezirken in Form von Schulungszuteilungen ausgebildet.

## **Salzburg**

Der Internetbetrug bildet nahezu die Hälfte aller Fallzahlen im Bereich der Internetkriminalität in Salzburg ab. Im Deliktsfeld „Cybercrime im engeren Sinn“ dominierten in Salzburg in den vergangenen Jahren Straftaten nach § 148a StGB, die auch hauptausschlaggebend für den Anstieg im gesamten Deliktsfeld waren – davon überwiegend NFC-Zahlungen mit entfremdeten Bankomatkarten. Verstärkend kommt hinzu, dass es sich pro entfremdete Bankomatkarte meist um Mehrfachbezahlungen handelt. 2021 wurden vermehrt Fälle von „Paketdienst-Smishing“ (bei aktiviertem Link) beobachtet. Der Auslandschriftverkehr beziehungsweise die Rechtshilfe, insbesondere mit Exchangern, gestaltet sich oft als sehr langwierig und schwierig.

### **Fortschritte in den Bereichen Ermittlungen und Forensik**

Wie bereits festgestellt, war und ist man weiterhin bestrebt, die technische Infrastruktur im Rahmen der budgetären Möglichkeiten bestmöglich zu optimieren, Ermittlungsbedienstete am aktuellsten Stand fortzubilden und das erforderliche Zusammenwirken einzelner Organisationseinheiten zu fördern. Es werden erfolgreich Schulungen in den Grundausbildungslehrgängen der Polizei durchgeführt und an Ausbildungstagen der Bezirkspolizeikommanden teilgenommen. Ein wichtiger Part des vom LKA-Salzburg organisierten KDFR-Seminars für Menschenhandel/Schlepperei wurde 2021 ebenfalls abgedeckt.



## **Erfolge und besondere Leistungen**

Im Jahr 2021 waren im Bundesland Salzburg zumindest zwei bedeutende Großfirmen (hoher Jahresumsatz, viele Mitarbeiter, systemkritische Infrastruktur) von gezielten Ransomware-Angriffen betroffen.

Das Landeskriminalamt Salzburg ermittelte und unterstützte auch bei schweren Erpressungsfällen im Cybercrimebereich, wie zum Beispiel bei Sextorsion. Ein besonders prekärer Fall mit einem Opfer aus dem Bundesland Salzburg beschäftigte die Ermittlerinnen und Ermittler fast das gesamte Jahr 2021 hindurch (laufender Schriftverkehr mit der Täterschaft, Betreuung des Opfers, laufende Rechtshilfeersuchen/Auslandschriftverkehr). CCR kann irgendwann gelesen werden. Die Täterschaft zeichnete sich insbesondere durch beharrliche Kontaktaufnahmeversuche und situationsbezogen veränderte Taktiken aus (Geldforderung mit Drohung der Veröffentlichung von Nacktbildern, dann Entschuldigung und Mitleidsmasche, dann erneut Drohung mit der Tötung von Angehörigen unter Vorweisen von Bildern aus sozialen Netzwerken und Beschreibung des persönlichen Umfelds sowie schließlich Kontaktaufnahme als vermeintlicher Polizeiermittler).

## **Strategische Entwicklung und Ausblick im LKA Salzburg**

Die Landespolizeidirektion Salzburg hat sich im Arbeitsprogramm 2022 mit entsprechenden Kennzahlen und Maßnahmen besonders die Förderung IT-affinen Personals sowie die verstärkte Nutzung digitaler Möglichkeiten zum Ziel gesetzt.

Im Zuge der polizeilichen Grundausbildung, wie auch in den weiterführenden Ausbildungen (GAL-E2a und Fachausbildung für den Kriminaldienst) werden Vorträge und Schulungen gehalten, um die Kolleginnen und Kollegen auf das Thema Cybercrime zu sensibilisieren und verschiedene Bereiche wie IT-Forensik und Ermittlungen vorzustellen. Es lässt sich dabei immer wieder erkennen, dass der Neuzugang an Kolleginnen und Kollegen, High-Userinnen und -User entsprechender Medien, Plattformen und Endgeräte sind, die dadurch ein generell höheres Verständnis für diesen technischen Bereich entwickeln, wovon schlussendlich auch die gesamte Organisation profitiert.

Das Landeskriminalamt Salzburg hält jedenfalls, soweit pandemiebedingt möglich, auch an der Forcierung der erlassmäßigen Ausbildung von Bezirks-IT-Ermittlungsbediensteten fest (Schwerpunkt vor allem die Kompensation von Abgängen, Ruhestandsversetzungen). Hinsichtlich der Grundausbildung von Bezirks-IT-Ermittlerinnen und Ermittlern besteht in diesem Zusammenhang laufender Bedarf an Präsenzs Schulungsangeboten des C4.

6

# Kooperation und Prävention



## Unterstützung der klein- und mittelständischen Unternehmenslandschaft

Auch 2021 erfolgten wieder Maßnahmen gemeinsam mit der Experts Group IT Security WKÖ. Die Experts Group IT Security gehört dem Fachverband Unternehmensberatung, Buchhaltung und Informationstechnologie (UBIT) an und ist eine Kooperations- und Marketingplattform zum Schwerpunktthema IT-Security in der Unternehmensberatung, Informationstechnologie und Buchhaltung. Die Mitgliedsbetriebe haben sich dem Themengebiet der Informationssicherheit in all ihren Formen verschrieben und sind präventiv und reaktiv gegen Cybercrime tätig.

So wurde während der Covid-19-Pandemie beispielsweise der E-Day im Onlineformat veranstaltet, bei dem sich Unternehmen aus der Wirtschaft zu Digitalisierungsthemen und neue Technologien austauschen. Durch das C4 wurde über aktuelle Gefahren von Cybercrime aufgeklärt und die Fragen der Online-Teilnehmerinnen und -Teilnehmer beantwortet.

Ebenso ist eine Informationsbroschüre als Leitfaden und rasche Hilfestellung für betroffene Betriebe bei der Anzeige von Cybercrime-Delikten erstellt worden.

In einer EU-weit einzigartigen Zusammenarbeit des Public Private Partnership wurde mit der Cyber-Security-Hotline (0800 888 133) der Wirtschaftskammern ein bundesweiter Service geschaffen, der Mitgliedsbetrieben im Cybercrime-Notfall operative Hilfeleistungen bietet. Durch wechselseitiges Verweisen werden die Serviceleistungen der Cyber-Security-Hotline und der Meldestelle des C4 verschränkt, um von der Anzeige über die erforderliche operative IT-Dienstleistung den Notfall zu begleiten.

## Prävention im Zeichen der Pandemie

Auch im zweiten Jahr der Covid-19-Pandemie wirkt sich diese auf die Existenz vieler Menschen aus. Das tägliche Leben hat sich für viele nachhaltig verändert, auch beruflich. Gearbeitet wird oft von zu Hause aus dem Homeoffice. Infolgedessen lässt sich eine Verschiebung der klassischen Eigentumsdelikte, wie Einbruch und (Taschen-) Diebstahl hin zu einem verstärkten Aufkommen von Betrugsdelikten oder strafbaren Handlungen im digitalen Bereich feststellen. Aufgabe der Polizei ist, neben der klassischen Aufklärung der Tat, immer stärker auch die Präventionsarbeit im Bereich der Computer- und Internetsicherheit.

Seit 1999 steht der Februar unter dem Motto „Safer Internet Month“. Dabei werden alle Schulen in Österreich dazu eingeladen, eigene Vorhaben, die Computer- und Cybersicherheit betreffen, auszuarbeiten und zu präsentieren. Die daraus entstandenen Projekte,

Präsentationen, Videos und Workshops wurden auf der Website [www.saferinternet.at](http://www.saferinternet.at) vorgestellt. Weiterführend zielt der „Safer Internet Day“ auf eine gemeinsame Bewusstseinsbildung und Sensibilisierung rund um den sicheren Umgang mit digitalen Medien ab, denn Internet, Smartphone & Co. sind längst zum festen Bestandteil des täglichen Lebens geworden.

Das Bundeskriminalamt bietet gemeinsam mit dem Digitalisierungsministerium über die Plattform [www.fit4internet.at](http://www.fit4internet.at) eine umfangreiche Informationsquelle für Menschen, insbesondere für Seniorinnen und Senioren, die gerade erste Erfahrungen mit dem „neuen Medium Internet“ machen. Dazu wird beispielsweise ein „Smartphone Führerschein-Kurs“ angeboten. Um die Eintrittsschwelle möglichst niedrig zu halten, kann die Anmeldung zu diesem telefonisch über die kostenlose fit4internet-Hotline (Tel. 0800/400 222) erfolgen.

Ebenfalls lassen sich über die fit4internet-Hotline Exekutivbedienstete (Polizistinnen und Polizisten mit Sonderausbildungen im Bereich Prävention) in ganz Österreich für Beratungen und Vorträge engagieren. Diese Seminare werden dann persönlich oder digital als Webinar abgehalten. In den Vorträgen und Beratungen werden Handlungsanleitungen dargelegt und eine entsprechende Sensibilisierung bei besonders häufigen Delikten mit dem Ziel vorgenommen, das Risiko im Bereich Internetkriminalität zu senken. Aktuell sind für das Aufgabenfeld „Computer und Cybersicherheit“ österreichweit über 200 speziell ausgebildet Kolleginnen und Kollegen im Einsatz.

## CyberKids

Vor einigen Jahren wurde das Präventionsprogramm CyberKids speziell für Kinder im Alter zwischen acht und zehn Jahren ins Leben gerufen. Im Rahmen der Ausbildung zur Kinderpolizisten oder Kinderpolizisten in den Volksschulen wird hier ein gewissenhafter Umgang mit dem Internet, digitalen Medien und dergleichen vermittelt. Das Ziel von CyberKids ist es, Gefahren im Internet für unerfahrene, jüngere Nutzerinnen und Nutzer aufzuzeigen, wie man sich davor schützen kann und wie man sich im Netz verhält. Es soll ein verantwortungsvoller Umgang mit den „neuen Medien“ und dem Internet („digitale Welt“) erreicht werden, aber die Kinder sollen auch über die damit verbundenen Gefahren sensibilisiert werden. Es wurde ein bundesweites einheitliches Niveau für ganz Österreich geschaffen und von speziell geschulten Verkehrserzieherinnen und Verkehrserziehern beziehungsweise Kinderpolizistinnen und Kinderpolizisten werden diese wichtigen Themen in der Volksschule den Kindern, Eltern und Lehrerinnen oder Lehrern vermittelt. Die Programminhalte entsprechen wissenschaftlichen Ansprüchen und wurden mit dem Bildungsministerium koordiniert.

Aufgrund der aktuellen Situation (Covid-19, Lockdowns und so weiter), ist es noch wichtiger geworden, unsere nächsten Generationen so gut als möglich in allen Lebenslagen

zu unterstützen. Durch „distance learning“ wurde dieses Programm noch wichtiger, da Kinder noch mehr Zeit in dieser digitalen Welt verbringen und weiterhin verbringen werden. Somit wird es immer bedeutender, dass Kinder in dieser Hinsicht geschult und damit vertraut gemacht werden. Im Internet lauern viele Gefahren, da Internetsurfen oder Kinderfilme streamen, wie beispielsweise auf Youtube, alltäglich geworden ist. Deshalb wurde und wird vor allem in den nächsten Jahren viel Arbeit und Zeit in die Ausbildung der CyberKids-Betreuerinnen und -Betreuer investiert, damit wir unsere nächste Generation in diesem Bereich auf einen guten Weg bringen können.

Ablauf: Die Volksschule nimmt Kontakt mit der Polizei durch die Schulleitung auf. Danach wird ein Aufklärungsgespräch hinsichtlich Dauer, Umfang und gemeinsamer Zielsetzung festgelegt. Es erfolgt eine Programmvereinbarung mit dem Klassenvorstand und schlussendlich eine Information der Eltern durch den Klassenvorstand mit eventuell Elternabend/ Elternbrief zum Themenbereich gemeinsam mit der Polizei.



#### Tipps von Polizeibär Tommi:

- Gib deine persönlichen Daten, wie deinen Namen, Geburtstag oder deine Wohnadresse im Internet nicht weiter. Sie bleiben dein persönliches Geheimnis.
- Schütze dich mit einem kreativen Passwort: Tommi1234 ist viel zu einfach!
- Hast du in einem Chat ein unangenehmes Gefühl, beende sofort das Gespräch.
- Vermeide Kontakt zu Personen, die du im Internet kennengelernt hast. Unter Umständen wollen sie sich mit dir treffen. Hüte dich vor fremden Personen.
- Nicht alles, was im Internet steht, ist wahr. Hast du im Internet etwas Komisches gelesen, erzähle sofort deinen Eltern, Großeltern oder Geschwistern davon.
- Fotos „online“ sind „out“. Du sollst keine Fotos von dir oder deinen Freunden ohne deren Erlaubnis ins „Netz“ stellen. Merke dir: Das Internet vergisst nichts!
- Vorsicht bei möglichen „Gratis“-Spielen, Apps oder sonstigen Schnäppchen-Angeboten. Im Internet ist leider nichts gratis.

Erzähle deinen Eltern, Großeltern oder Geschwistern, was du im Internet angeschaut und dabei erlebt hast.

7

# Strategie und Ausblick



## Kriminaldienstreform 2.0

Ein strategischer Schwerpunkt umfasst weiterhin die Verstärkung der nationalen und internationalen Zusammenarbeit zwischen staatlichen Behörden, privaten Organisationen und relevanten Unternehmen. Das Ziel bleibt weiterhin die schnelle Erkennung von kriminellen Phänomenen zum Zwecke der Strafverfolgung, aber auch zum Schutz der Bevölkerung. In diesem Zusammenhang muss in den nächsten Jahren die Ausbildung weiter forciert werden und das Knowhow bei allen Strafverfolgungsbehörden bis zur letzten Polizeidienststelle verbessert sowie die Gesellschaft im Umgang mit neuen Technologien zur Wahrung ihrer Sicherheit sensibilisiert werden.

Weiterhin bedarf es einer dringenden Anpassung rechtlicher Rahmenbedingungen gerade im Hinblick auf die Problematiken bei Carrier Grade NAT, Domainnamen und Kryptowährungen, die derzeit die kriminalpolizeiliche Arbeit erschweren beziehungsweise sogar verhindern. Eine Aktualisierung der Strategie und Konzepte zur Bekämpfung von Cybercrime wurde auch im Jahr 2021 vorgenommen und bestehende Empfehlungen des Rechnungshofes eingearbeitet.

Sowohl der Bereich der IT-Ermittlungen wie auch der digitalen Beweismittelsicherung wurden soweit möglich personell verstärkt. Die Personalakquise blieb auch 2021 herausfordernd, eine Tatsache, mit der die Kriminalpolizei in der Bekämpfung von Cybercrime seit Jahren konfrontiert ist.

Gesetzliche Bestimmungen des materiellen und formellen Cyberstrafrechts wurden im Bereich Recht der Kriminaldienstreform 2.0 evaluiert. Konkrete Vorschläge zur Abänderung von Gesetzesbestimmungen, die während des Reformprozesses formuliert wurden, befinden sich aktuell in Abstimmung mit den zuständigen Stakeholdern.

Ein kleiner Fortschritt in diesem Bereich ist beim neuen § 126c StGB zu vernehmen, der am Ende des Jahres in Kraft trat. Der neue Absatz des § 126c Abs 1a StGB im Zusammenhang mit § 148a StGB („Freiheitsstrafe bis zu zwei Jahren zu bestrafen“), sollte jedoch auf den gesamten Absatz 1 ausgeweitet werden.

Der grenzenlose, altersübergreifende, digitale Raum ohne einheitliche Werte- und Normenkonstrukt, in dem statistisch gesehen jeder Mensch mehr Zeit verbringt als im öffentlichen Straßenverkehr, stellt auch die Kriminalpolizei vor enorme Herausforderungen. Daher ist die wesentliche Stoßrichtung der derzeit laufenden Kriminaldienstreform des Bundesministeriums für Inneres die Anpassung der Organisation, der Technik, der Prozesse und des Personaleinsatzes an die dynamischen Umweltveränderungen im Zusammenhang mit der Digitalisierung.

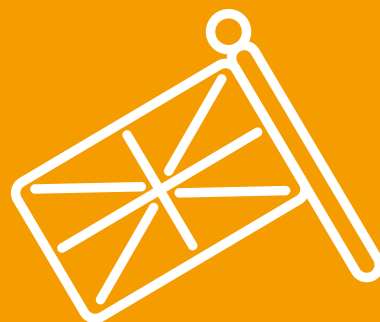
Die eingesetzte Expertengruppe diskutiert einen alle Ebenen betreffenden interdisziplinären Ansatz für die zukünftige kriminalpolizeiliche Cybercrime-Bearbeitung. Auf der einen Seite soll die IT-Forensik neue technische Möglichkeiten bis auf Ebene der Polizeiinspektionen erhalten sowie zur Abfederung der stark steigenden Einsatzzahlen personell verstärkt werden. Auf der anderen Seite ist ein neuer Organisationsteil auf Ebene der Landeskriminalämter in Ausarbeitung. An dieser Stelle wird sich hohe IT-Kompetenz bündeln und eine neue spezialisierte Ermittlungseinheit für Cybercrime-Delikte aller Art entstehen. Dort werden Internet-, Darknet- und Krypto-Ermittlungen auf hohem Niveau bereitgestellt, um mithilfe von neuen Meldeschienen und Arbeitsanalysedatenbanken Massendelikte schneller erkennbar und gebündelt werden. Damit wird eine zentrale Cybercrime-Ansprechstelle in jedem Bundesland ermöglicht. Durch Schulungszuteilungen von den einzelnen Polizeiinspektionen soll eine erhöhte, flächendeckende Cybercrime-Ermittlungskompetenz erreicht werden.

Neben der Modernisierung von Ausbildungsinhalten der Sicherheitsakademie sind auf operativer Ebene im Bereich der Landeskriminalämter Cybercrime-Training-Center in der Konzeptionsphase. Damit sollen einerseits alle Bediensteten von Polizeiinspektionen ein Cybercrime-Grundmodul absolvieren können, andererseits Aufbaumodule sowie Spezialmodule für Kriminalistinnen und Kriminalisten bereitgestellt werden. Dabei handelt es sich um mehr als einen „EDV-Lehrsaal“: Moderne Ausbildungszentren mit einem praxisnahen „Hands-On“-Ausbildungskonzept am Puls der Zeit zur Bewältigung der zukünftigen Herausforderungen werden angestrebt.



8

# Strategy and Outlook



## “Kriminaldienstreform 2.0”

One strategic focus of the “Kriminaldienstreform 2.0” (CID Reform 2.0) will still lie on the increase of national and international cooperation between government authorities, private organisations and relevant companies. The aim continues to be the fast detection of criminal phenomena for the purpose of criminal prosecution, but also for the protection of the public. In this context, training has to be further enhanced in the years to come and know-how has to be improved at all levels of law enforcement, down to every police station. Also, society must be sensitized on secure handling of new technologies.

There is still an urgent need to adapt the legal framework, especially with regard to the problems with Carrier Grade NAT, domain names and cryptocurrencies that complicate or even prevent CID investigations. In 2021, the strategy and the concepts for combating cybercrime were updated, taking into account recommendations by the Austrian Court of Audit.

Staff numbers were raised as far as possible in the area of IT investigations, but also in the field of preservation of digital evidence. However, recruitment remained a challenge also in 2021, a problem criminal police has had for years when combating cybercrime.

Legal provisions of substantive and adjective criminal law on cybercrime were assessed in the legal part of CID Reform 2.0. Specific suggestions to amend certain legal provisions that were formulated in the course of the reform process are currently being discussed with the competent stakeholders.

Some progress in this area has been made with a new provision in the Austrian Penal Code, section 126c, which entered into force in late 2021. However, the new paragraph of section 126c para 1a in connection with section 148a (“shall be liable to a prison term of up to two years”) should be extended to the entire paragraph 1.

The vast, intergenerational digital space without any uniform framework of values and norms, where people, statistically speaking, spend more time than in public traffic also pose enormous challenges for CID work. Therefore, the Federal Ministry of the Interior’s ongoing CID Reform 2.0 focusses on adapting structures, technology, procedures and employment of staff to the dynamic environmental changes linked to digitalisation.

The expert group in charge is discussing an interdisciplinary approach at all levels for future cybercrime investigations by criminal police. On the one hand, IT forensics require new technological solutions, down to the level of police stations. Also, additional staff is required, as case numbers are on the rise. On the other hand, a new organisational unit at the level of provincial CIDs is being developed, which is intended to bundle high-level IT competence and serve as a new specialised investigation unit for cybercrime offences

of all kinds. This unit will provide high-level internet, darknet and cryptocurrencies investigations. New reporting mechanisms and analysis work file systems will ensure that mass crime will be pooled and detected faster. Every province will thus have a central cybercrime contact point. Training secondments for police station staff are intended to lead to higher cybercrime investigation skills all around Austria.

In addition to the modernisation of the Federal Police Academy's training content, at the operational level in the field of provincial CIDs, cybercrime training centres are being designed. This will enable all police station staff to complete a cybercrime basic training module, and there will also be advanced modules and special modules for CID officers. This is more than a "computer lab": Rather, it is intended to have modern training centres with a practical cutting-edge "hands-on" training concept to meet the challenges of the future.

# 9 Glossar



## **Anonymisierungsdienst**

Bei Anonymisierungsdiensten handelt es sich um Services und Techniken im Internet, die dazu dienen, bestimmte Informationen, die auf die Identität einer Internetnutzerin oder eines Internetnutzers hindeuten könnten, zu verschleiern.

## **Antivirenprogramm**

Ein Antivirenprogramm (synonym mit Virens Scanner 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, eine Mitarbeiterin oder einen Mitarbeiter der Firma zu einer Geldtransaktion auf das Bankkonto der Täter zu veranlassen. 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 Unternehmensmitarbeiter durchzuführen und es ist ratsam im Schriftverkehr mit Handelspartnerinnen und Handelspartnern vorsichtig zu sein. Bei unklaren oder eigenartigen Sachlagen sind die Sachverhalte zu überprüfen.

## **Behördenwallets**

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

## **Bitcoin**

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

## **Call-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 Aufwand verbunden. Wenn die Manipulation im eigenen Netz eines Anbieters stattgefunden hat, besteht für diesen kaum eine Möglichkeit zu kontrollieren, ob die signalisierte Telefonnummer stimmt oder nicht. Dazu können existierende – auch aus dem Ausland stammende – Telefonnummern verwendet werden, obwohl die Inhaberin oder der Inhaber der Nummer für den Anruf gar nicht verantwortlich ist. Auch Fantasienummern, also Telefonnummern, die nicht vergeben sind, können eingesetzt werden.

## **Crime as a Service (CaaS)**

Die für die Begehung einer Straftat benötigten Dienste werden gleichsam eines Puzzles 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 mehr, um die Straftat zu begehen, sondern kaufen sich das fehlende Wissen schlichtweg zu.

## **Collège Européen de Police (CEPOL)**

Die European Union Agency for Law Enforcement Training beziehungsweise Europäische Polizeiakademie ist eine durch Beschluss des Rates der europäischen Justiz- und Innenminister 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, den so genannten Uniform Resource Locator (URL), aufgerufen werden. Um in das Darknet beziehungsweise Tor-Netzwerk zu gelangen, benötigt man beispielsweise einen speziellen Browser, wie den Tor-Browser. Daten werden im Darknet anonym und verschlüsselt über verschiedene Server geschickt. Das Darknet war ursprünglich für Personen und Organisationen gedacht, die von Zensur bedroht waren. Heutzutage reicht das Spektrum an illegalen Aktivitäten im Darknet vom Drogen- und Waffenhandel über Dokumentenfälschung, Geldfälschung, Datenhandel bis hin zur Kinderpornografie und weit darüber hinaus.

## **DDoS-Angriffe**

DDoS-Angriffe beziehungsweise „Distributed Denial of Service“-Angriffe sind Attacken auf die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems oder von Netzwerken, meistens mit dem Ziel, diese zu blockieren und somit regulären Benutzerinnen und Benutzern keinen Zugriff mehr zu ermöglichen. Die Angriffe erfolgen häufig von vielen verschiedenen Ressourcen aus dem Internet. Neben politisch oder persönlich motivierten Angriffen versuchen 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](http://www.bmi.gv.at), in eine IP-Adresse (siehe IP-Adresse), um eine Kommunikation zwischen den Computersystemen zu ermöglichen.

## **European Cybercrime Center (EC3)**

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

Bekämpfung von Cybercrime, begangen durch organisierte Gruppierungen, die beispielsweise durch Online-Betrug große Geldmengen erbeuten.

Bekämpfung von Formen von Cybercrime, die die Opfer massiv schädigen, wie beispielsweise sexueller Missbrauch von Kindern.

Bekämpfung von Cybercrime (inklusive Cyberattacken), die gegen kritische Infrastruktur und Informationssysteme der EU-Mitgliedsstaaten gerichtet ist.

## **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.

## **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 oder Romance Scam**

Bei Love Scam handelt es sich um eine Art von Partnervermittlungsbetrug. Der Täter stellt meist den ersten Kontakt per E-Mail oder soziale 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 dem Täter nur als Tarnung. Die Betrügerinnen und Betrüger 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 oder Downloader, jeweils versteckt als JavaScript, eingebettet in komprimierten Dateien oder anderen Datenformaten) oder diese E-Mails beinhalten „nur“ einen Link, der aktiv von der Empfängerin oder vom Empfänger angeklickt werden muss, damit die schädlichen Komponenten auf dem Gerät des Opfers installiert werden.

## **Money Mules**

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

## **Network Address Translation (NAT)**

Bei Carrier Grade NAT teilt der Provider eine IPv4-Adresse aus dem privaten Adressbereich „10.0.0.0/8“ den Endkundenanschlüssen zu – keine „öffentliche IP-Adresse“ (§ 92 Abs 3 Z 16 TKG). Auf diese Weise spart er mittlerweile sehr rare öffentliche IPv4-Adressen. Zwischen dem privaten Provider-Netz und dem öffentlichen IPv4-Netz vermittelt dann die NAT oder Port Address Translation (PAT). Der dafür zuständige vermittelnde Server kümmert sich um die Adressübersetzung zwischen den privaten und öffentlichen IPv4-Adressen und reicht die Pakete zwischen den Netzwerken weiter. NAT wurde ursprünglich für lokale Netzwerke, wie 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 die Kundin oder der Kunde immer noch nur eine IPv4-Adresse für mehrere Clients bekommt.

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 im 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.

## **Remote Access Trojaner (RAT)**

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 die Anwenderin oder der Anwender aufgerufen hat, beispielsweise ein Spiel oder ein E-Mail-Anhang. Sobald das Zielsystem kompromittiert ist, macht sich der Eindringling diesen Umstand zunutze, um RATs auf andere anfällige Computer zu verteilen.

## **Schadsoftware**

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

## **Smart Contracts**

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

## **Social Engineering**

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

## **Spam**

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

## **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 das Opfer braucht, um ihr oder ihm zu helfen, nach Hause zurückzukehren. Gefordert werden Geldbeträge in unterschiedlicher Höhe. Tatsächlich wurde das E-Mail-Konto gehackt und die Nachricht an alle Kontakte im Adressbuch gesendet. Die 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 der Anwenderin oder des Anwenders 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 selbst verbreiten und unterschiedliches Schadpotenzial in sich tragen. Sie treten in Kombination mit einem Wirt auf, das heißt mit einem infizierten Dokument oder einer Applikation.

## **Verschlüsselung**

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

## **Wallet**

Ein Wallet, der englische Begriff für „Geldbeutel“ oder „Portemonnaie“, ist eine virtuelle Geldtasche, in der die Benutzerin und der Benutzer Bitcoins oder auch andere Kryptowährungen aufbewahrt. 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 die Eigentümerin oder den Eigentümer und den Ansprechpartner der Domain (siehe Domain Name System) sowie IP-Adressen über diesen Dienst abzufragen, da alle Daten öffentlich zugänglich gewesen sind.

## **Deliktsbezeichnungen nach Paragraphen 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

## **Verbotsgesetz (VerbotsG)**

- § 3g VerbotsG Wiederbetätigung

