LANDESKRIMINALAMT
NIEDERSACHSEN

Lagebild Cybercrime und Kinderpornografie

in Niedersachsen

2022

Impressum

Landeskriminalamt Niedersachsen

Dezernat 62
Zentralstelle Cybercrime/Kinderpornografie

Am Waterlooplatz 11
30169 Hannover

Erreichbarkeiten:

Tel.: 0511/9873-6203
d62@lka.polizei.niedersachsen.de

Stand: 25.05.2023

Inhaltsverzeichnis

1 Was Sie erwartet

Das Medium „Internet“ ist aus kaum einem Lebensbereich wegzudenken. Die Verlagerung der Daten-, Informations- und Kommunikationsstrukturen in Rechenzentren und die weitgehende Nutzung kommerzieller digitaler Dienstleistungen auf Plattformen und sozialen Medien haben zur Konsequenz, dass Cyberkriminelle die Möglichkeiten des digitalen Raums für ihre Zwecke missbrauchen, u.a. für Identitätsdiebstähle, Angriffe gegen das Onlinebanking oder Ransomware.[1]
Während der COVID-19-Pandemie vergrößerten das sog. Social Distancing und die von Arbeitgebern veranlassten Homeoffice-Angebote die Angriffsmöglichkeiten.

Für Cyber-Straftaten sowie im Bereich der Straftaten im Zusammenhang mit Kinder- und Jugendpornografie ist von einem überdurchschnittlich hohen Dunkelfeld auszugehen. Als Zentralstelle für die Kriminalitätsbekämpfung in der Polizei Niedersachsens bietet das Landeskriminalamt Niedersachsen mit dem „Lagebild Cybercrime und Kinderpornografie“ u.a. einen Überblick über die für das Jahr 2022 in Niedersachsen polizeilich registrierten Fälle. Darüber hinaus finden Sie in den folgenden Kapiteln Informationen über

- die im Jahr 2022 am häufigsten aufgefallenen Phänomene im Bereich Cybercrime und Kinderpornografie,
- herausragende Fälle der Cyberkriminalität mit ihren Herausforderungen für die polizeilichen Ermittlungen und erreichten Ermittlungszielen,
- bedeutsame Sachverhalte der Kinderpornografie, die das Ausmaß polizeilich sichergestellter Datenmengen von Missbrauchsabbildungen und deren Verbreitungspraxis verdeutlichen, sowie
- die Entwicklung der entsprechenden Fallzahlen.

Weiterhin finden Sie einen Ausblick auf Herausforderungen der vorgestellten Phänomenbereiche, welche die Polizei im Folgejahr noch erwarten könnten.

An verschiedenen Stellen dieses Lagebildes finden Sie QR-Codes, welche Sie auf Wunsch zu Quellen und weiteren Informationen führen. Dieser QR-Code führt sie zum Dokument selbst auf der Homepage des Landeskriminalamtes Niedersachsen:

- Für die Straftaten der Cyberkriminalität ist von einem überdurchschnittlich hohen Dunkelfeld auszugehen.
- Die Täter und Täterinnen der Cyberkriminalität sind global vernetzt, agieren international, arbeitsteilig und höchst organisiert.
- Ransomware ist aktuell die größte Bedrohung für Wirtschaftsunternehmen.
- Phishing ist das größte Einfallstor für Angriffe gegen Privatpersonen wie auch Unternehmen
- Bei Angriffen gegen das Onlinebanking steigen sowohl Fallzahlen als auch Schadenshöhen enorm an.
- Die Fälle von Kinderpornografie haben sich in den letzten zwei Jahren mehr als verdoppelt und sind weiterhin ansteigend.
- Die Menge auszuwertender kinderpornografischer Daten erreicht mit weit über 3 Petabyte einen neuen Höchststand.
- Zur Bewältigung dieser Herausforderungen passt die Polizei Niedersachsen fortlaufend ihre Bearbeitungsstrukturen an.

[1] vgl. https://www.bitkom.org/Presse/Presseinformation/Drei-Viertel-Cyberkriminalitaet-betroffen

2 Cybercrime in Niedersachsen

2.1 Was ist Cybercrime?

Im Deliktsbereich Cybercrime unterscheidet die Polizei die Begriffe Cybercrime *im weiteren Sinne* und Cybercrime *im engeren Sinne*.

Cybercrime *im weiteren Sinne* umfasst Straftaten, bei denen Täter und Täterinnen sich das Internet, weitere Datennetze, informationstechnische Systeme bzw. deren Daten zur Planung, Vorbereitung und Ausführung zunutze machen. Die Technik ist dabei nur Mittel zum Zweck, um das kriminelle Ziel zu erreichen (beispielsweise Bedrohungen und Beleidigungen in sozialen Netzwerken oder Betrügereien auf Verkaufsportalen). Straftaten, welche sich das Internet lediglich als Tatmittel zu Nutze machen, werden durch die für das jeweilige Deliktsfeld zuständige Polizeidienststelle bearbeitet (beispielsweise Gewalt-, Freiheits- oder Eigentumsdelikte).

Unter Cybercrime *im engeren Sinne* werden Straftaten erfasst, die sich gegen o.g. IT-Systeme oder Daten richten (beispielsweise Ransomware-Attacken). Die Täter und Täterinnen nutzen dabei ihr Fachwissen, um in teils hochkomplexe IT-Systeme eindringen zu können. Diese Delikte werden innerhalb der Polizei von Spezialdienststellen der Cybercrimebekämpfung bearbeitet, deren Personal über entsprechende Fachkenntnisse sowie über besondere technische Ausstattung verfügt.

Dieses Lagebild beschreibt überwiegend die Ausprägungen des Bereichs Cybercrime *im engeren Sinne*. Wie jedoch später unter Punkt „2.5 – Herausragende Sachverhalte“ dargestellt wird, kann es auch bei Delikten der Cybercrime *im weiteren Sinne* erforderlich sein, dass z.B. aufgrund der besonderen Komplexität von Täterstrukturen die Ermittlungen durch die Spezialdienststellen zu führen sind, auch wenn die Delikte eher der Cybercrime *im weiteren Sinne* zuzuordnen sind.

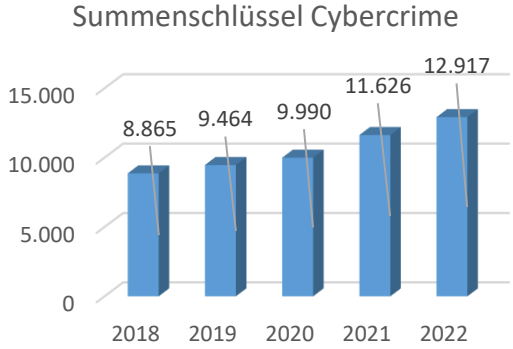
Mit der zunehmenden Digitalisierung ist ein kontinuierlicher Anstieg der Fallzahlen in allen Bereichen der Cybercrime feststellbar.

2.2 Datengrundlage

Die Polizeiliche Kriminalstatistik (PKS) zählt die der Polizei bekannt gewordenen Straftaten sowie deren Versuche. Diese Statistik bildet insofern das so genannte polizeiliche Hellfeld ab. Die Daten werden nach Abschluss der Ermittlungen anhand bundesweit einheitlicher Kriterien erfasst, um wesentliche Erkenntnisse abbilden zu können. Diese Informationen nutzt die Polizei, um die Entwicklungen der Delikte sowie deren Begehungsformen zu beobachten und möglichst zeitnah Strategien der Straftatenverhütung und -verfolgung zu erarbeiten.

Bei der Bewertung der Datenlage im Bereich Cybercrime besteht die Herausforderung im Umstand, dass Taten, deren Tatorte im Ausland liegen oder keinem Land zugeordnet werden können, nicht in der PKS berücksichtigt werden. Da Täterinnen und Täter an jedem Ort der Welt via Internet Taten begehen können und nicht selten ihren Standort verschleiern, ist ein großer Teil der Cyber-Straftaten diesen Kategorien zuzuordnen.

Im Rahmen der PKS werden Cyber-Straftaten bundeseinheitlich anhand von Deliktschlüsseln erfasst, welche im so genannten Summenschlüssel *„897000 – Cybercrime“* zusammengeführt werden. Bei diesen Delikten handelt es sich u.a. um das Ausspähen und Abfangen von Daten inklusive dessen Vorbereitung (§§ 202 a-c StGB), die Datenhehlerei (§ 202d StGB), Computerbetrug (§ 263a StGB), die Fälschung beweiserheblicher Daten (§ 269 StGB), die Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB) sowie Datenveränderung und Computersabotage (§§ 303a, b StGB).



Die Grafik zeigt die Entwicklung des Summenschlüssels Cybercrime.

Um Aufkommen und Entwicklung der Cyber-Straftaten noch zielgenauer erfassen zu können, nimmt das Landeskriminalamt Niedersachsen eine manuelle Auswertung der Strafanzeigen vor, die bei der Polizei erstattet werden und den Phänomenen der Cybercrime zuzuordnen sind. Diese individuelle Betrachtung erlaubt zwar einen unmittelbareren Blick auf diese Phänomene, jedoch ist sie lediglich eine Momentaufnahme, da die fortschreitenden Ermittlungen nicht evaluiert und nachträgliche Veränderungen nicht mehr wahrgenommen werden können.
Die so gewonnenen unterjährigen Statistiken repräsentieren somit den aktuellen Stand der Fallzahlen individueller Phänomene, sind aber aus vorgenannten Gründen weder valide noch reproduzierbar.

In diesem Lagebild werden daher grundsätzlich die PKS-Daten des Landes Niedersachsen betrachtet. Zahlen, welche der beschriebenen, LKA-spezifischen Erhebung zugrunde liegen, werden als solche gekennzeichnet.

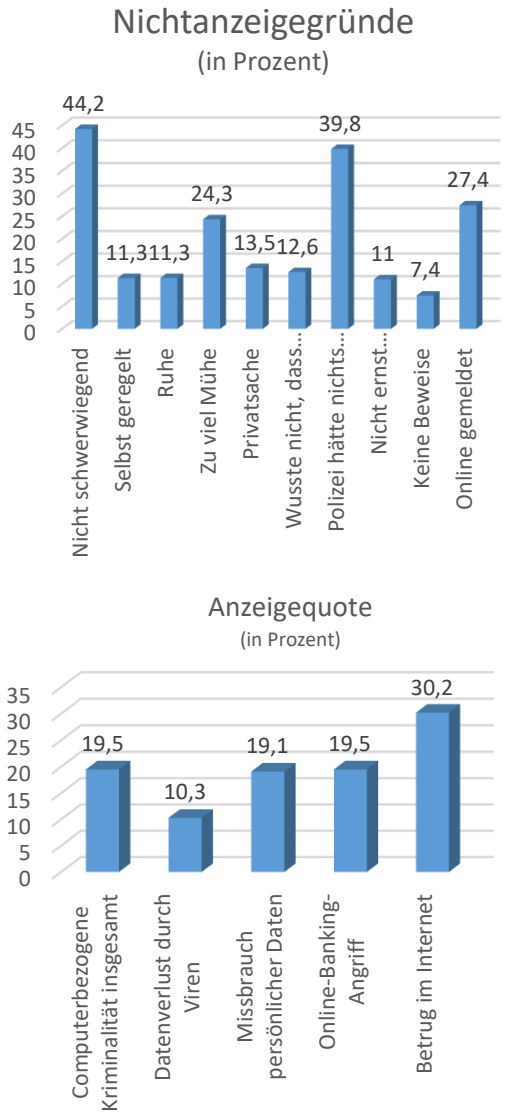
Ein Problem für die statistische Auswertung stellt das Dunkelfeld im Bereich Cybercrime dar, welches im nächsten Kapitel betrachtet wird.

2.3 Das Dunkelfeld

Unter dem so genannten Dunkelfeld versteht man die Straftaten, die nicht angezeigt wurden und somit der Polizei nie bekannt geworden sind. Es gibt verschiedene Studien, die sich mit er Erhellung des Dunkelfeldes beschäftigten.

Der Kernbefundbericht 2021 aus der zurückliegenden niedersächsischen *„Befragung zu Sicherheit und Kriminalität“* blickt auch auf Cyber-Straftaten des Bereichs *„im weiteren Sinne“* und hat den Anspruch, *„ein möglichst realitätsnahes Bild vom Sicherheitsgefühl der Menschen und der tatsächlichen Kriminalitätslage im Land zu zeichnen“*[2]. Diese Dunkelfeldstudie des Landeskriminalamtes Niedersachsen hat sich daher u.a. mit dem Anzeigeverhalten nach ausgewählten, erlebten Cyber-Straftaten befasst. Anhand der Angaben der Teilnehmenden wurde ein Anzeigequotient errechnet. Dieser ergab, dass lediglich 19,5 % aller computerbezogenen Straftaten angezeigt wurden. Die höchste Anzeigequote haben laut der Studie Betrugstaten im Internet mit 30,2 % (vgl. Grafik mittig rechts). Die Studie zeigt ferner auf, dass Betroffene aus verschiedenen Gründen auf die Erstattung einer Anzeige verzichten. Wie die untenstehende Grafik zeigt, werden als Hauptgründe genannt, dass das *Delikt nicht als so schwerwiegend* erachtet wird (44, 2 %) bzw. *die Polizei nichts hätte tun können* (39,8 %).

Nur wenn die Delikte bekannt werden ist es der Polizei möglich, Täter und Täterinnen zu ermitteln, die Phänomene effektiv zu bekämpfen und präventive Strategien dagegen zu entwickeln. Daher ist es von großer Bedeutung, die Taten nach Entdeckung anzuzeigen.



[2]Kernbefundbericht 2021 kann heruntergeladen werden unter https://www.lka.polizei-nds.de/forschung/dunkelfeldstudie/dunkelfeldstudie-vierte-befragung-von-40000-menschen-steht-unmittelbar-bevor-115379.html sowie QR-Code oben

2.4 Phänomene der Cyberkriminalität

2.4.1 Ransomware

Ransomware bezeichnet Schadprogramme, mit deren Aktivierung berechtigte Nutzende eines IT-Systems (beispielsweise eines Computers) dieses ganz oder teilweise nicht mehr nutzen und/oder auf die darauf gespeicherten Daten nicht mehr zugreifen können. Für die in Aussicht gestellte Freigabe des IT-Systems oder der Daten erheben die Täter und Täterinnen häufig einen Anspruch auf Lösegeld (engl. „ransom“).

In der Regel wird zwischen Ransomware unterschieden, die lediglich den Zugriff verhindern, wie z. B. durch einen Sperrbildschirm (sog. Locker-Ransomware), und den Varianten, die Dateien verschlüsseln (sog. Crypto-Ransomware). Der überwiegende Teil der Crypto-Ransomware hat Unternehmen getroffen. Hier gingen die Lösegeld-Forderungen teilweise in den Millionenbereich. Die Schäden durch Angriffe mit Ransomware umfassen jedoch nicht nur den Betrag, der im Rahmen der Erpressung gefordert wird.

Deutlich zurück gegangen sind die Anzeigen von Privatpersonen. Auch ist der Sperrbildschirm als Variante kaum noch aufgetreten. Bei Angriffen auf Unternehmen haben sich folgende Verfahrensweisen entwickelt:

DOPPELTE ERPRESSUNG (DOUBLE-EXTORTION):
Vor der Verschlüsslung der Systeme speichern die Täter und Täterinnen Daten aus dem angegriffenen Computersystem auf eigenen Servern. Nach der Verschlüsselung wird den Opfern zusätzlich mit der Veröffentlichung der teils sensiblen Daten gedroht. Die Opfer müssen zudem befürchten, dass die Daten trotz der Zahlung veröffentlicht werden könnten.

DREIFACHE ERPRESSUNG (TRIPLE-EXTORTION):
Zusätzlich zum Szenario der doppelten Erpressung wird bei den Opfern bei bestehender Verschlüsselung weiter Druck aufgebaut. Dies kann beispielsweise durch DDoS-Attacken auf Opfersysteme geschehen.

ERPRESSUNG MIT ERBEUTETEN DATEN (SECOND-STAGE-EXTORTION):
Eine andere Möglichkeit besteht für die Täter und Täterinnen darin, Lieferanten oder Kunden des eigentlichen Opfers mit der Veröffentlichung der sie betreffenden Daten zu bedrohen und auch bei diesen Lösegelder einzufordern.

BEISPIELSACHVERHALT:

Ende Oktober 2022 wurden mehrere Server eines großen niedersächsischen Unternehmens verschlüsselt. Sowohl interne Kommunikationssysteme als auch kommerzielle Systeme waren betroffen.

Ermittlungen ergaben, dass die verwendete Ransomware-Variante weltweit für Attacken gegen mehrere Unternehmen eingesetzt wurde. Das Landeskriminalamt Niedersachsen führt die Ermittlungen in Zusammenarbeit mit verschiedenen internationalen Partnern.

Zu den aktuell geführten polizeilichen Maßnahmen gehören unter anderem auch Finanzermittlungen sowie Ermittlungen hinsichtlich der für den Angriff genutzten Infrastruktur.

2.4.1.1 Ransomware in Niedersachsen

Im Rahmen einer Datenerhebung bei den spezialisierten Cybercrime-Dienststellen Niedersachsens wurde die Betroffenheit mittelständischer und größerer Unternehmen in Bezug auf Ransomware-Angriffe im Jahr 2022 betrachtet.
Laut dieser Erhebung wurden 55 niedersächsische Unternehmen, die den abgefragten Kriterien (mittelständische und größere Unternehmen) entsprachen, Opfer von Systemverschlüsselungen mit Erpressung.
Verwendete Ransomware-Varianten waren u.a. BianLian, Black Basta, Black Cat, Makop und Royal. In mehreren Fällen führen die technischen Spuren der Täter und Täterinnen nach Osteuropa. Mehrere Ransomware-Gruppierungen behaupten zudem von sich, prorussisch zu agieren. Da aufgrund des russischen Angriffskrieges gegen die Ukraine polizeilich derzeit keine internationale Zusammenarbeit mit Russland möglich ist und durch Verschleierungsmethoden wie VPN (Virtual Private Network) Ermittlungen erschwert werden, kann häufig kein Rückschluss auf die tatsächliche Motivation der Täter und Täterinnen (z.B. finanziell oder politisch) gezogen werden.

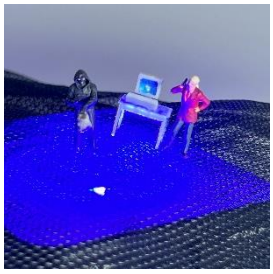
2.4.2 Angriffe gegen das Online-Banking

Der Angriff gegen das Online-Banking zielt auf den unbefugten Zugang zu einem Online-Angebot einer Bank ab (u.a. Zugangsberechtigungen zu Girokonten, Sparkonten, Wertpapierdepots) sowie dessen Missbrauch mittels Computer oder Sprachcomputer.
Beispielsweise gelangen die Täter und Täterinnen durch das Erbeuten von Daten aus der sog. Underground-Economy, vorhergehende Phishing oder Smishing-Attacken oder durch den Einsatz von Schadprogrammen („Malware") an die Konto- und Kontaktdaten ihrer späteren Opfer.
Den größten Anteil aller Varianten dieses Phänomens nehmen die Taten ein, bei denen mit Kontoinhabenden telefonisch Kontakt aufgenommen wurde (vgl. Fallbeispiel rechts).
Auch die Variante mit einer Phishing-Nachricht (meist per SMS), welche suggeriert eilig reagieren zu müssen, um einer Kontosperrung zu entgehen, wird von Tätern und Täterinnen oft angewandt.

Verschiedene Varianten von Angriffen gegen das Online-Banking haben gemein, dass die Kontoinhabenden von den Tätern und Täterinnen dazu gebracht werden, Passwörter, PushTAN oder ähnlich sensible Daten bekannt zu geben und damit den Zugriff auf die Bankkonten zu ermöglichen.
Anhand der LKA-spezifischen Erhebung ließ sich feststellen, dass bereits von 2020 (543 Fälle) auf 2021 (1593 Fälle) die Fallzahlen um rund 300% anstiegen. 2022 stiegen die Fallzahlen wiederrum um ca. 60% an (2687 Fälle).
Auch die Gesamtschadenssumme erhöhte sich von 10,5 Millionen im Jahr 2021 auf 13,5 Millionen Euro in 2022.

BEISPIELSACHVERHALT:
Im Juni 2022, war die täuschend echt gefälschte Internetseite eines Bankinstituts auf einem russischen Server gehostet. Diese Seite wurde mittels Bezahldienst bei Google so gerankt, dass sie als erstes Ergebnis einer Suche erschien. Kunden dieser Bank, welche sich über die falsche Seite im Online-Banking anmelden wollten, gaben ihre Daten unwissentlich den Tätern und Täterinnen preis. Diese hatten somit Zugriff auf das Online-Banking, jedoch nicht auf das notwendige pushTAN Verfahren. Deshalb erschien auf der falschen Internetseite in der Folge ein Hinweis, dass es zu Störungen gekommen sei und sich eine Mitarbeiterin (namentlich benannt) telefonisch bei den Kunden melden würde. Um die Seriosität der angeblichen Mitarbeiterin zu erhöhen, wurde eine Legitimations-ID mitgeteilt. Im Rahmen des Telefonats entlockte die vermeintliche Mitarbeiterin den Kunden durch geschickte Gesprächsführung und Nennung von richtigen Kundendaten pushTAN Nummern, angeblich, um damit die Störungen zu beseitigen. In Wahrheit wurde mit den Nummern das Überweisungslimit erhöht und dann Überweisungen auf Konten von Finanzagenten getätigt. Hierbei entstand in 46 Fällen im Jahr 2022 ein Schaden von rund 470.000 Euro. Insgesamt konnten bislang 14 Finanzagenten identifiziert werden.

2.4.3 Phishing



Phishing war, ist und bleibt sowohl für Privatpersonen als auch für Unternehmen eine große Gefahr im Umgang mit digitalen Medien. Es gibt unzählige Varianten dieses Phänomens, beispielsweise angebliche Gewinnspiele im Internet, Anrufe bei den Geschädigten oder augenscheinlich seriös wirkende E-Mails, die jedoch Schadsoftware beinhalten. Täter und Täterinnen verwenden die so erlangten Daten, um zum Beispiel in Online-Shops betrügerisch Waren zu bestellen, Unternehmen auszuspionieren oder Privatpersonen via Online-Banking um ihr Geld zu bringen.

Weil das Phishing selbst als Vorbereitung der Täter und Täterinnen auf ihr eigentliches Ziel oft von den Geschädigten nicht bemerkt wird, liegen der Polizei deutlich weniger Anzeigen vor als tatsächliche Straftaten zu vermuten sind. Der größte Anteil der Cyber-Straftaten aus dem Bereich Cybercrime *im engeren Sinne* ist nur möglich, da Täter und Täterinnen zuvor in den Besitz von relevanten Daten wie z.B. Bankdaten, Ausweiskopien, Personalien, etc. gelangen konnten und diese für kriminelle Zwecke einsetzen. Deshalb wird die Bekämpfung des Phänomens Phishing auch zukünftig eine wesentliche Bedeutung für die Ermittlungsbehörden haben.

Beispielsweise gelangen Cyberkriminelle über eine Phishing-E-Mail an Firmen- und Login-Daten von Mitarbeitenden eines Unternehmens und verwendeten diese, um sich selbst Zugang zum Firmennetzwerk zu verschaffen. Innerhalb des Netzwerkes verschaffen sie sich im Laufe der Zeit unbemerkt Berechtigungen von Administratoren, um so an sensible Daten zu gelangen und/oder eine Schadsoftware zur späteren Verschlüsselung zu platzieren.

2.4.4 Smishing

Dieses Kunstwort setzt sich zusammen aus *„SMS“* und *„Phishing“* und bezeichnet ein Phänomen, das 2022 nicht nur in Niedersachsen vermehrt auftrat.

Neben der unter Punkt „2.4.2 - Angriffe gegen das Onlinebanking“ beschriebenen Phishing-SMS bestand im Jahr 2022 eine weitere Variante darin, dass in vielen Fällen Geschädigte eine SMS empfingen, die dazu aufforderte, einen Link anzuklicken um eine Voicemail abhören zu können. Nach dem Anklicken wurde eine Schadsoftware auf das Gerät geladen, die je nach Art der Software zu einem Massenversand von SMS/MMS führte und/oder die Daten der Geräte auslas und an die Täter übermittelte.

2.4.5 Distributed Denial of Service (DDoS)

Bei einer DDoS-Attacke wird eine Webseite oder eine ganze Netzinfrastruktur durch ein so genanntes Botnetz angegriffen. Der Begriff Botnetz meint einen Verbund von Rechnern, welche nach Befall mit einer Schadsoftware vom Botnetz-Betreibenden übernommen und gesteuert werden. Für die DDoS-Attacke werden die Server von Unternehmen oder öffentlichen Einrichtungen von dem Botnetz mit Anfragen „geflutet“, bis sie überlastet sind oder zusammenbrechen.

Wenn durch diese Form der Cyberangriffe Unternehmen nicht erreichbar sind, können Kunden z.B. weder in den Onlineshops einkaufen oder Verträge abschließen, was für betroffene Unternehmen große Umsatzverluste bedeuten kann.

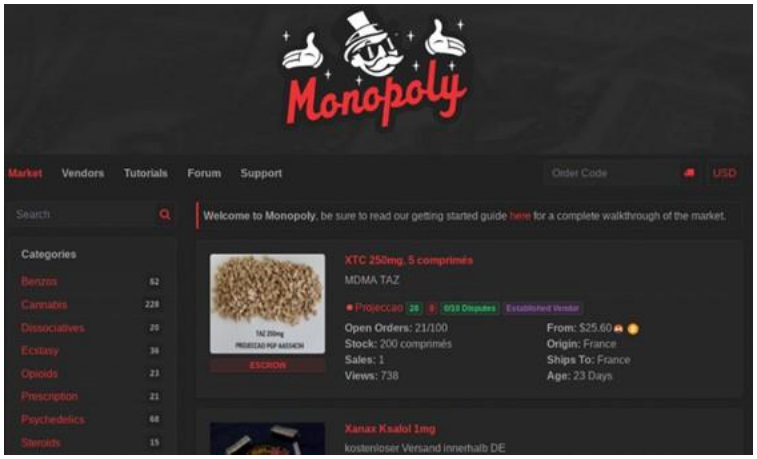
Laut der LKA-spezifischen Erhebung sind die Fallzahlen in Niedersachsen bezogen auf dieses Phänomen im Jahr 2022 im Vergleich zum Vorjahr um 10 Fälle auf insgesamt 15 Fälle gesunken. Betroffen waren neben Unternehmen u.a. auch Schulen und Vereine. In wenigen Einzelfällen waren auch Privatpersonen betroffen. Die geringen Zahlen können u.a. damit erklärt werden, dass durch verbesserte IT-Sicherheitskonzepte Angriffe häufig erfolglos bleiben. Betroffene von abgewehrten Attacken zeigen wegen des fehlenden Schadenseintritts eine geringere Anzeigebereitschaft.

BEISPIELSACHVERHALT:

Bei einem Unternehmen mit Online-Shop wurde eine DDoS-Attacke in so genannter „Add-to-Cart-Operation“ ausgeführt. In kürzester Zeit wurden Unmengen an Produkten des Online-Shops in den Warenkorb gelegt und wieder daraus entfernt. Die enorme Anzahl der Serveranfragen belastete die Systeme zeitweise so stark, dass das Unternehmen sich gezwungen sah, den Shop einige Tage vom Netz zu nehmen. Da die Herkunft der Angriffe über VPN verschleiert wurde, konnten die Urheber der Attacke bislang nicht ermittelt werden.

2.5 Herausragende Sachverhalte

2.5.1 Cyberkriminalität im Darknet



INFORMATIONEN ZUM MARKTPLATZ:

ONLINE SEIT MITTE 2019

403 VERKÄUFER

MIND. 30.000 KÄUFER

1 ADMINISTRATOR

132.000 VERKÄUFE

UMSATZ CA. 17,3 MILLIONEN EURO IN KRYPTOWÄHRUNGEN

INKL. FORUM MIT 11.200 NUTZERN

Das Darknet ist ein „versteckter" Bereich des Internets, welcher nur mit spezieller Software aufgerufen werden kann. Die Kommunikation innerhalb des Darknets ist verschlüsselt, um die Anonymität der Urheber sowie Betrachter der Inhalte zu gewährleisten. Gewöhnliche Suchmaschinen können Inhalte des Darknets nicht finden. Die Nutzung des Darknets ist grundsätzlich legal. Beispielsweise nutzen in diktatorischen Regimen Bürgerrechtler und -rechtlerinnen das Darknet um beim Informationsaustausch vor staatlicher Verfolgung geschützt zu sein. Aber auch Kriminelle nutzen die Anonymität des Darknets zur Verschleierung ihrer Identität bei der Begehung von Straftaten.

Die Zentrale Kriminalinspektion (ZKI) Oldenburg führte unter Sachleitung der Generalstaatsanwaltschaft Hessen (ZIT[3]) in Kooperation und enger Absprache mit dem FBI, ein Verfahren gegen die Betreibenden der Darknet-Plattform *„MonopolyMarket"*, die zum Verkauf von Betäubungsmitteln diente. Der Gesamtumsatz dieser illegalen Geschäfte betrug umgerechnet ca. 17,3 Millionen Euro.

In Zusammenarbeit mit weiteren internationalen Strafverfolgungsbehörden gelang es, die Serverstandorte in mehreren Ländern zu lokalisieren sowie im Rahmen polizeilicher Maßnahmen alle erforderlichen Serverdaten zu sichern.

Die durch die ZKI Oldenburg und das FBI gesicherten Daten der Plattform führten neben weiteren Sicherstellungen zu verschiedenen von Europol und FBI koordinierten internationalen Ermittlungsverfahren (OP SpecTOR) mit insgesamt 288 Festnahmen weltweit sowie der Sicherstellung von 850 kg Betäubungsmitteln, 117 Waffen und gesicherten Vermögenswerten in Höhe von insgesamt 50,8 Millionen Euro.

Dieser QR-Code führt Sie zur offiziellen Mitteilung von Europol auf der Plattform YouTube. (Dauer: 1.14 Min.)

[3] Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität

2.5.2 Erfolge internationaler Zusammenarbeit

Der Zentrale Kriminaldienst der Polizeidirektion Hannover führt seit dem 3. Quartal 2019 die Ermittlungen bezüglich einer Ransomware-Gruppierung, die bis Juni 2021 sowohl in Deutschland für Cyberangriffe verantwortlich war als auch international agierte.
Mit Stand 04.01.2023 sind 169 Verfahren im Bundesgebiet mit einer Schadenshöhe von ca. 7,7 Millionen Euro (erpresste Gelder) bekannt geworden. Der tatsächliche Schaden inkl. der Produktions- und Verkaufsausfälle sowie der Wiederherstellungskosten der Systeme von den betroffenen Institutionen dürfte im hohen achtstelligen Bereich liegen.

Durch die Ermittlungen wurden Täter dieser Gruppierung sowie Geldwäscher und Geldwäscherinnen, über welche die erpressten Lösegelder gewaschen worden sind, identifiziert.

Diese Ermittlungen führten ferner auf die Spur eines VPN-Dienstleisters, der Cyber-Kriminellen Schutz durch Anonymität bot. Im Zuge internationaler Zusammenarbeit gelang es, in einem gemeinsamen Action Day mit 10 beteiligten Ländern sowie mit Europol und Eurojust diesen VPN-Anbieter vom Netz zu nehmen. (Splash-page siehe unten)

2.5.3 Datendiebstahl und Drohung mit Veröffentlichung

Im August 2022 wurde das DAX-Unternehmen Continental AG Opfer eines Cyberangriffs. Es wurden weder Systeme verschlüsselt, noch war der Geschäftsbetrieb gestört. Allerdings wurden nach ersten Einschätzungen Daten mit einem Volumen von ca. 40 Terabyte entwendet. Die Täterschaft forderte 40 Millionen US-Dollar in Kryptowerten und drohte bei Nichtzahlung mit der Veröffentlichung der Daten.

In der Kommunikation mit der Continental AG erklärte sich die Ransomware-Gruppierung Lockbit für den Angriff verantwortlich. Auch hier führten technische Spuren nach Russland.

Da das Unternehmen der Forderung nicht nachkam, wurde eine Textdatei im Darknet auf dem Leak-Portal von Lockbit veröffentlicht, welche ca. 56 Millionen Dateipfade beinhaltete, ohne jedoch detailliertere Daten zu veröffentlichen. (Leak-Seite siehe oben)

Sowohl auf nationaler als auch auf internationaler Ebene werden Informationen regelmäßig unter Ermittlungsbehörden sowie der Continental AG ausgetauscht. Im Februar 2023 führte die Continental AG eine Transparenzveranstaltung mit deren Kunden unter Einbindung der beteiligten Ermittlungsbehörden sowie dem BSI[4] durch.

[4] Bundesamt für Sicherheit in der Informationstechnik

2.6 Informationen für Ihre Sicherheit

Die vorgestellten Phänomene und Verfahren zeigen deutlich, dass der Kriminalprävention ein großer Stellenwert beizumessen ist, um Unternehmen wie auch Bürgerinnen und Bürger gleichermaßen zu informieren und zu sensibilisieren. Insbesondere bei Ransomware-Angriffen zeigt sich, dass selbst wenn die Daten aus einem Backup wiederhergestellt werden können, die Schäden durch Ausfallszeiten und Kosten durch Wiederinbetriebnahme immens sind.

Informations- und Beratungsangebote stehen in der Polizei Niedersachsen wie folgt zur Verfügung:

2.6.1 Prävention für Privatpersonen

Auf der Homepage POLIZEI-PRAEVENTION.DE bietet das Landeskriminalamt Niedersachsen mit dem Ratgeber Internetkriminalität Informationen zu Betrugsmaschen, Phishing-Varianten und vielen weiteren Phänomenen von Cybercrime an. Übersichtlich und anhand aktueller Beispiele werden unter anderem die Methoden vorgestellt, die von den Tätern und Täterinnen angewandt werden. Weiterhin erklären konkrete Sicherheitstipps, wie man sich vor diesen Methoden schützen kann. Geschädigte von Straftaten finden hier Hinweise, was nun zu tun ist.

Das Programm Polizeiliche Kriminalprävention (ProPK) gibt auf der Internetseite POLIZEI-BERATUNG.DE Sicherheitstipps zum Schutz vor Straftaten und informiert u.a. über Opferrechte und Entschädigungsmöglichkeiten. Dabei werden nicht nur die Delikte aus der „analogen Welt“, sondern auch Taten im Cyberraum betrachtet. Den Lesenden werden in verschiedenen Kategorien sowohl verschiedene Begehungsformen von (Cyber-) Straftaten nähergebracht, als auch verschiedene Hilfsangebote vorgestellt, die angenommen werden können, um sich über Opferrechte wie auch über die Durchsetzung von Ansprüchen zu informieren.

2.6.2 Prävention für Unternehmen

Die Zentrale Ansprechstelle Cybercrime für die niedersächsische Wirtschaft (ZAC) im Landeskriminalamt Niedersachsen ist der polizeilicher Berater für Firmen, Verbände und Behörden bei der Prävention von Cyberkriminalität und der erste Ansprechpartner im Schadensfall.
Zu den Kerntätigkeiten der ZAC gehört die Beratung von Unternehmen. Ebenfalls bietet die ZAC Veranstaltungen an, die auf die Gefahren von Angriffen und die Art und Weise der Durchführung hinweisen, so dass Firmen ein Gefühl dafür bekommen, wie sie sich schützen können. So werden zielgerichtet unterschiedliche Veranstaltungen für Geschäftsführung, Mitarbeitende oder die IT-Bereiche angeboten.

Zum Zwecke der Beratung bietet die Webseite ZAC-NIEDERSACHSEN.DE umfangreiche Informationen über die unterschiedlichen Varianten von Cyberangriffen sowie einen Newsletter zu aktuellen Cybercrime-Phänomenen an. Es sind verschiedenste Videos zur Sensibilisierung von Mitarbeitenden zum freien Download verfügbar. Checklisten erleichtern Geschäftsführungen, die richtigen Fragen an ihre IT zu richten, um die eigenen Systeme abzusichern.
Zur Vor-Ort-Beratung und Unterstützung bei der Abwehr von bedeutenden Cyberangriffen wurde eine sogenannte Quick-Reaction-Force (QRF) ins Leben gerufen, der auch das Team der ZAC angehört.

Als zusätzliches Angebot steht allen Bürgerinnen und Bürgern die E-Mail-Adresse TROJANER@POLIZEILABOR.DE zur Verfügung, um der Polizei Spam-E-Mails oder Schadsoftware mitzuteilen und sie so in die Lage zu versetzen, frühzeitig neue Deliktsvarianten zu erkennen und zu bekämpfen.

2.6.3 Prävention in Social Media

Seit Anfang 2022 betreibt die Zentrale Kriminalinspektion Braunschweig den Instagram-Kanal POLIZEI.BRAUNSCHWEIG.ZKI. Mit ihm bleiben die Follower dieses Social Media Dienstes in Cybercrime-Themen up to date. Bei den Beiträgen handelt es sich um Bilderreihen oder Erklär-Videos, in denen Phänomene vorgestellt, konkrete Sicherheitstipps vermittelt, aber auch allgemeine Themen aus dem Bereich Internetsecurity aufgegriffen werden.

Auch das Landeskriminalamt Niedersachsen nutzt mit dem Facebook-Account @LKANIEDERSACHSEN die Möglichkeit, zeitnah über aktuelle Cybercrime-Phänomene zu informieren und Tipps zu geben, wie man sich davor schützen kann.
Anhand von Bild- und Videobeiträgen werden sowohl neu entdeckte wie auch altbekannte Phänomene in das Bewusstsein der Betrachtenden gerückt.

Link zum Facebook-Account:

3 Kinderpornografie in Niedersachsen

3.1 Herausforderungen der Kinderpornografie

Kinderpornografie ist die foto- und video-realistische Darstellung des sexuellen Missbrauchs einer Person unter 14 Jahren. Hinter den Darstellungen stecken also reale Handlungen oftmals schwerer Sexualdelikte, die von den Tätern und Täterinnen selbst gefilmt oder fotografiert wurden. Durch die oft weltweite Verbreitung und Verfügbarkeit des Datenmaterials erfolgt eine dauerhafte Viktimisierung der Opfer. Zur Befriedigung des Sexualtriebes und als Tausch-währung in einschlägigen Internetforen streben die Täter und Täterinnen eine fortwährende Herstellung solcher Dateien an.

Nach den polizeilichen Beobachtungen haben die technologischen Entwicklungen der vergangenen Jahre dazu geführt, dass insbesondere das Internet und Mobile Devices wie Smartphones, Tablets usw. für die Verbreitung der Daten genutzt werden. Verbunden mit immer größer werdenden Speichervolumina der Geräte ist es möglich, eine enorme Anzahl von Bildern und Videos zu besitzen. Amerikanische Provider übermitteln verstärkt die ihnen vorliegenden Verdachtsfälle, was zu einem immensen Anstieg der Fallzahlen und einem Schwerpunkt der polizeilichen Sachbearbeitung in Niedersachsen sowie bundesweit führt.

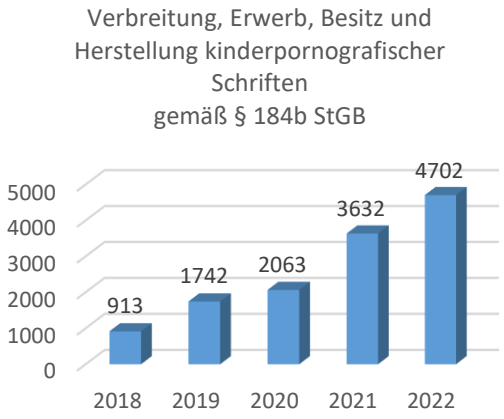
Im Kontext des Kinderschutzes nimmt die Polizei die Aufgaben der Prävention und der Abwehr von Gefahren für schutzbedürftige Kinder sowie der Strafverfolgung wahr. Ihr oberstes Ziel ist dabei die Verhütung von Missbrauchstaten an Kindern und Jugendlichen. Maßgeblich in der Bekämpfung der Kinder- und Jugendpornografie ist es, den realen, möglicherweise noch andauernden sexuellen Missbrauch schnellstmöglich zu erkennen und frühzeitig zu unterbinden sowie Verbreitungshand-lungen konsequent zu verfolgen. Aus diesem Grund sind bislang sämtliche sichergestellte Daten zu sichten und zu bewerten.

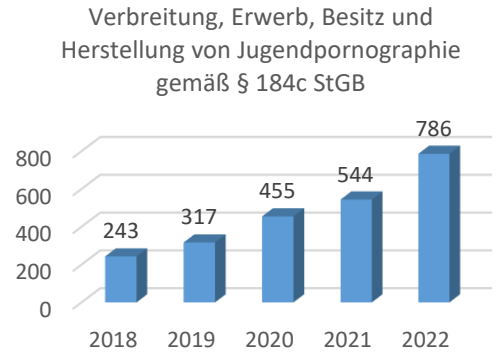
3.2 Entwicklung der Fallzahlen

3.2.1 Zunahme der Ermittlungsverfahren

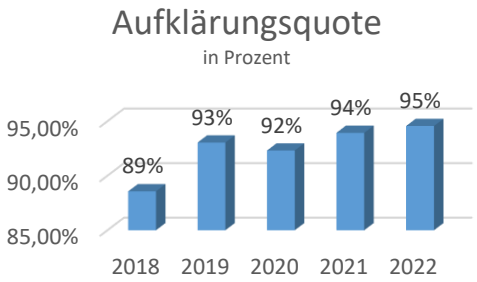
Die Fallzahlen der Delikte im Bereich Kinder- und Jugendpornografie stiegen in Niedersachsen in 2022 erneut an. Im Deliktsbereich der Verbreitung pornografischer Inhalte stiegen sie von 1.444 Fällen im Jahr 2018 auf nun 6.111 und steigerten sich damit um mehr als das Vierfache in nur fünf Jahren.

Der Großteil dieser Verbreitungsdelikte bezieht sich auf Kinder- und Jugendpornografie. Im Bereich der Verbreitung von kinderpornographischen Inhalten registrierte die Polizei im Jahr 2022 insg. 4.702 Fälle, ein Anstieg um rund 30% gegenüber dem Jahr 2021.





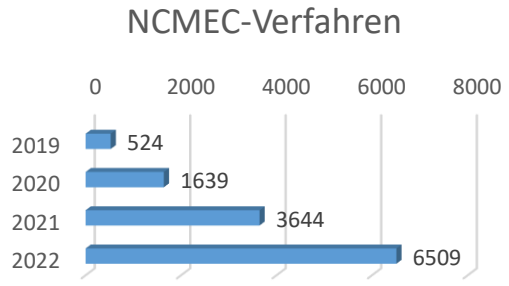
Die Aufklärungsquote lag 2022 bei ca. 95%.



Viele Taten werden durch Kinder und Jugendliche selbst, überwiegend durch unbedachtes Verhalten oder digitaler Naivität begangen. Teilweise werden selbstgefertigte Aufnahmen von sich oder gleichaltrigen verbreitet, ohne sich der straf-rechtlichen Konsequenzen bewusst zu sein.

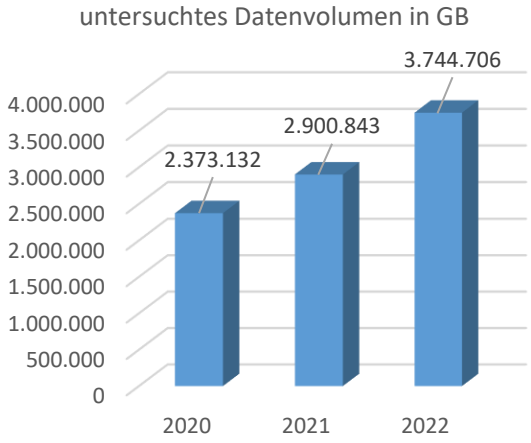
3.2.2 NCMEC-Verfahren

Über Messenger-Dienste und Chatforen wie Facebook, WhatsApp und KIK werden häufig strafbare Inhalte ausgetauscht. Das Internet bleibt das meist genutzte Tatmittel im genannten Phänomenbereich. Die US-amerikanische, halbstaatliche Nichtregierungsorganisation *„National Center for Missing and Exploited Children"* (NCMEC) meldet vermeintlich strafrechtliche Verstöße deutscher Nutzer aus dem Internet automatisiert an das Bundeskriminalamt (BKA). Die Hinweise werden dem BKA in Form von so genannten Reporten gemeldet und von dort aus wöchentlich an die zuständigen Landeskriminalämter verteilt. Im Landeskriminalamt Niedersachsen erfolgt eine umfassende Prüfung der übersandten Daten durch einen eigens dafür eingerichteten Arbeitsbereich in der im November 2021 neu gegründeten Abteilung 6 – Digitales Service- und Kompetenzzentrum. In diesem Arbeitsbereich werden polizeiliche Datenbanken und öffentlich zugängliche Quellen zu Recherchen genutzt, um die Täter und Täterinnen zweifelsfrei zu identifizieren. Inkriminierte Daten werden gesichtet und bewertet sowie Ermittlungsberichte gefertigt. Die Bearbeitung mündet in einer abgabereifen Ermittlungsakte an die zuständige Staatsanwaltschaft. Die Bearbeitung dieser so genannten NCMEC-Hinweise macht einen hohen Anteil der in der PKS erfassten Gesamtfälle der Kinder- und Jugendpornografie aus und wird auch zukünftig personelle und zeitliche Ressourcen in besonderem Umfang in Anspruch nehmen. Die untenstehende Grafik beschreibt die enorme Fallzahlensteigerung der vergangenen Jahre. Hierbei ist zu beachten, dass die Anzahl der im Jahr 2022 vom BKA eingegangenen NCMEC-Hinweise die der bearbeiteten Verfahren in Niedersachsen (PKS) überstiegen hat. Dies liegt darin begründet, dass es aufgrund der großen Fallzahlensteigerung zunächst nicht möglich war, alle eingegangenen Hinweise abzuarbeiten. Dieser Entwicklung wurde durch eine deutliche Personalverstärkung entgegengewirkt.



3.2.3 Sichergestellte Datenmengen

Im Jahr 2022 wurden in Niedersachen durch die Polizei im Rahmen von Ermittlungsverfahren ca. 7,9 Petabyte an Daten sichergestellt und ausgewertet. Davon entfielen ca. 3,74 Petabyte[5] der Daten auf Ermittlungsverfahren im Bereich Kinderpornografie. Im Vergleich zum Vorjahr (2021: 2,9 PB) ist es erneut zu einer deutlichen Steigerung des auszuwertenden Datenbestandes gekommen.



Der Phänomenbereich der Kinderpornografie zeichnet sich in den letzten Jahren durch eine bundes- wie landesweit kontinuierlich und signifikant steigende Anzahl von Verfahren und durchschnittlich zu sichtenden Asservaten je Verfahren aus. Diese Entwicklung stellt die bearbeitenden Polizeibehörden selbst unter Ausschöpfung aller vorhandener Personal- und Sachmittel vor erhebliche Schwierigkeiten.

[5] Die Datenmenge von 3 Petabyte entspricht 3072 Gigabyte (=3,145728 x 10^6 Megabyte)

3.3 Herausragende Ermittlungsverfahren

3.3.1 Verbreitung von Kinderpornografie und Massendaten

Die Polizeiinspektion Oldenburg führt ein Verfahren gegen einen Beschuldigten, welcher in fünf verschiedenen WhatsApp-Gruppen mit jeweils mehreren hundert Teilnehmenden (zum Teil tausende Mitglieder) inkriminierte Dateien versendet und empfangen hat.

In Absprache mit der zuständigen Staatsanwaltschaft sollen gegen knapp 1000 Anschlussinhabende deutscher Mobilfunknummern und gleichzeitig Teilnehmende der Chats Verfahren eingeleitet werden. In den Chats wird ein jugendtypischer Sprachgebrauch festgestellt, weshalb davon auszugehen ist, dass es sich insbesondere um jugendliche und heranwachsende Beschuldigte handeln könnte.

Die Polizei Lüneburg ist mit einem Ermittlungskomplex befasst, welcher seinen Ursprung bereits im Jahr 2020 hat. Es handelt sich hierbei um 150 Skype-User-Gruppen. Der Beschuldigte hat in 10 von diesen Gruppen kinder- und jugendpornografische Inhalte verbreitet und erworben. Im Tatzeitraum 2016-2018 erhielten 2998 andere Nutzer kinder- und jugendpornografische Inhalte über diese Gruppen.

3.3.2 Verbreitung im Schulkontext

Wie bereits beschrieben, werden vermehrt Taten durch Kinder und Jugendliche durch unbedachtes Verhalten bzw. aus digitaler Naivität begangen. Daraus resultieren vermehrt Verfahren im so genannten Schulkontext, welche die Fachkommissariate, hier insbesondere den Bereich der Jugendsachbearbeitung fordern, wie das nachfolgende Fallbeispiel aufzeigt:

In einer Schule im Bereich Gifhorn erhielt die Schulleiterin Kenntnis, dass in einer Klassenchatgruppe kinderpornografische Dateien durch einen 11-jährigen Schüler eingestellt worden sind und informierte neben den Eltern auch die Polizei von dem Vorfall.

Die Mutter zeigte sich erschüttert und erklärte, sich das Verhalten ihres Sohnes nicht erklären zu können.

Bei der Inaugenscheinnahme des Mobiltelefons durch die Polizei bestätigte sich der Verdacht. Der Schüler gab an, die Bilder selber zugesandt bekommen, jedoch nur selten mit anderen geteilt zu haben. Weitere Angaben machte er nicht.

Das Mobiltelefon wurde zur Durchsicht sichergestellt und später auf Anordnung der Staatsanwaltschaft auf Werkseinstellungen zurückgesetzt. Der Schüler erhielt nach dieser Form der Löschung aller Daten sein Mobiltelefon zurück.

Weiterhin wurde durch die Polizei ein erzieherisches Gespräch geführt und der Vorfall wurde durch Schule und Eltern aufgearbeitet.

Da es sich bei dem Schüler um ein Kind handelte, konnte er das Mobiltelefon zurückbekommen und der Vorfall ohne Einleitung eines Strafverfahrens abgeschlossen werden. Bei jugendlichen Tätern wird hingegen ein Strafverfahren eröffnet. Bei den Ermittlungsverfahren gem. 184b ff. StGB handelt es sich um Verbrechenstatbestände mit einem Strafrahmen von mindestens einem Jahr Freiheitsstrafe. Auch wenn die Verfahrensweise nach dem Jugendgerichtsgesetz erfolgt, handelt es sich nicht um ein Bagatelldelikt. Auch eingezogene Gegenstände werden hierbei beispielsweise nicht zwingend wieder herausgegeben, sondern vielfach vernichtet, ganz abgesehen von den möglichen Bestrafungen und/oder Auflagen.

Auch wenn diese Verfahren im Einzelfall keine herausragende kriminalistische Bedeutung aufweisen, bilden sie einen Teil des Schwerpunkts der Sachbearbeitung.

4 Blick in die Zukunft

4.1 Cybercrime

Mehr Digitalisierung – mehr Straftaten
Die Geschwindigkeit der Digitalisierung der Gesellschaft wird sich voraussichtlich in den kommenden Jahren weiter beschleunigen. Die steigenden Fallzahlen der Delikte im Bereich Cybercrime *im engeren Sinne* sowie eine dynamische Entwicklung der Angriffsmöglichkeiten deuten darauf hin, dass es sich dabei für Strafverfolgungsbehörden auch zukünftig um eine große Herausforderung handeln wird. Ein wichtiger Aspekt der polizeilichen Arbeit zur Prävention der Cyberkriminalität wird daher sein, Privatpersonen wie Unternehmen über bekannte Varianten zu informieren und gleichzeitig für den sorgsamen Umgang mit Daten zu sensibilisieren.

Politisch motivierte Cyberangriffe
Cyber-Angriffe mit Zusammenhang zum russischen Angriffskrieg auf die Ukraine hatten bislang keine erkennbar größeren Auswirkungen in Niedersachsen. Denkbar ist jedoch, dass im weiteren Verlauf der kriegerischen Handlungen der Konflikt vermehrt in Form von Cyberattacken ausgetragen wird. Staatliche Hacker und unabhängige „Hacktivisten" greifen im digitalen Raum über Ländergrenzen hinweg weltweit IT-Systeme an. Am Beispiel des im Februar 2022 in den Medien beschriebenen Angriffs auf den Kommunikationssatelliten KA-SAT, welcher gleichzeitig europaweit Störungen bei Windkraftanlagen zur Folge hatte, wird deutlich, wie schnell es zu solchen unerwarteten Auswirkungen kommen kann.

Regulierung von Kryptowerten
Die Straftäter und -täterinnen nutzen zunehmend die für sie vorteilhaften Möglichkeiten der Zahlungsabwicklung mittels Kryptowerten. Diese Zahlungswege lassen sich zwar grundsätzlich im Internet auf öffentlichen Seiten für jedermann nachverfolgen. Anbieter so genannter „Mixer" stellen jedoch eine Möglichkeit der Verschleierung zur Verfügung. Andere, unseriöse Anbieter bieten den Cyberkriminellen Mittel und Wege, die Zahlungen in Echtwährungen umzuwandeln, ohne dabei identifiziert zu werden. Die Nachverfolgung dieser Zahlungswege bis zu den Tätern und Täterinnen ist eine weitere Herausforderung für die Ermittlungsbehörden.

Das EU-Parlament hat im April 2023 eine erste Regelung zur Rückverfolgung von Transfers von Kryptowerten wie Bitcoin und E-Money.Token angenommen. Wie auch im traditionellen Zahlungsverkehr sollen von Kryptodienstleistern Angaben zu Zahlenden und Zahlungsempfangenden gewährleistet werden können. Inwieweit damit zukünftig auch das Problem der Mixer gelöst werden kann, bleibt abzuwarten.

Künstliche Intelligenz und Cybercrime
Auch das Thema Künstliche Intelligenz (KI) liegt im Fokus polizeilicher Arbeit. Beispielsweise nutzen Kriminelle die Möglichkeiten so genannter „Deep Fakes" für die Begehung von Straftaten. Bei Deep Fakes handelt es sich um technisch hochwertige und kaum erkennbare Fälschungen von Bildern oder Videos. Auf den Betrachtenden wirkt es, als sei eine bestimmte Person auf Bildern bzw. in Videos zu sehen. Die Möglichkeit, Mimik und Stimme in Videos täuschend echt zu imitieren könnte missbraucht werden, um z.B. bekannte Persönlichkeiten gefälschte Reden halten zu lassen, pornografische Aufnahmen von Personen zu fälschen oder Unternehmen durch Vortäuschen einer hochrangigen Führungsperson zu schädigen.

Herausforderung Cybercrime-as-a-Service
Die unter Punkt „2.5 Herausragende Sachverhalte" vorgestellten Verfahren machen deutlich, dass Cyberkriminelle aus verschiedenen Ländern heraus arbeitsteilig vorgehen. Die kontinuierliche Verbesserung der digitalen Infrastruktur mit neuen Möglichkeiten wird diesen internationalen Trend weiter verstärken. Für eine wirkungsvolle Bekämpfung der Cyberkriminalität wird die international vernetzte und vor allem schnelle Zusammenarbeit der beteiligten Ermittlungsorgane

damit zu einem Schlüsselfaktor erfolgreicher Ermittlungsverfahren im Bereich international organisierter Cyberkriminalität.
Die zunehmende Verlagerung der Kriminalität hin zu Delikten, die im oder über das Internet begangen werden, macht die Verfügbarkeit von IP-Adressen und Portnummern zur Täter-identifizierung wichtiger denn je. Die Einführung einer entsprechenden, wenigstens kurzzeitigen Speicherpflicht in Deutschland ist daher dringend geboten.

4.2 Kinderpornografie

Die durch das BKA, als zentral annehmende Stelle der NCMEC-Hinweise, prognostizierten Hoch-rechnungen für 2023 lassen einen weiteren Zuwachs der Fallzahlen erwarten. Nicht vergessen werden darf hierbei, dass diese Anzahl von Fällen einen großen Anteil, aber nicht die einzigen Fälle von Ermittlungsverfahren im Bereich Kinder-pornografie ausmachen. In Summe hat dies zusätzlich unmittelbare Auswirkungen auf das bereits beschriebene schon jetzt sehr hohe Datenvolumen, welches aufbereitet und ausgewertet werden muss.

KI-Einsatz im Bereich der Datenaufbereitung
Die Ermittlungsbehörden werden in dem genannten Phänomenbereich mehr denn je auf performante technische Unterstützung angewiesen sein. Gleichzeitig wird diese die manuelle Auswertung aber nicht gänzlich entbehrlich machen. Die Anwendung Künstlicher Intelligenz stellt eine aktuelle Zukunftsinvestition in elaborierte Vorselektionsmöglichkeiten dar, die perspektivisch die Ermittlungen erleichtern und beschleunigen kann und soll. Neben finanziellen Aufwänden bedeutet diese Investition aber auch den Einsatz personeller Ressourcen bei der Weiterentwicklung jener Technik.

Die Ermittlungsbehörden bewegen sich bei der Bearbeitung der Massendaten im direkten Spannungsfeld möglicher Ermittlungsansätze und leistbarer Ermittlungsaufwände. Angesichts des großen Dunkelfeldes im Deliktsbereich Kinder-pornografie scheint es dennoch angezeigt, dass die Polizei mit den neu geschaffenen Strukturen im Landeskriminalamt Niedersachsen zukünftig auch initiativ die bestehenden Möglichkeiten nutzt, andauernden Missbrauch aufzuspüren, zu unterbinden sowie die Täterstrukturen zu identifizieren und zu zerschlagen.

Bisher werden eine hohe Anzahl von Ermittlungsverfahren insbesondere durch die in den USA und Kanada zum Hinweis auf inkriminierte Daten an das NCMEC verpflichteten Unternehmen initiiert. Mit der Einführung des sog. „Digital Service Act“[6], in dem auch europäische Unternehmen zur ver-stärkten Kontrolle ihrer Plattformen verpflichtet werden, ist mit einem weiteren bisher nicht genau zu beziffernden Zuwachs an Hinweisen zu rechnen. Eine Umsetzung ist zu Beginn des nächsten Jahres zu erwarten. Inwiefern die sog. CSA-Verordnung[7], die u.a. eine aktive Chat-Kontrolle beinhaltet, auch zu weiteren Hinweisen oder der Veränderung von Nutzungsverhalten führt, bleibt abzuwarten. Aus bisherigen Verfahren ist allerdings bekannt, dass die Anzahl der Taten zur Verbreitung Kinder- und jugendpornografischer Schriften (siehe auch Schulkontext) und die Anbahnung und Umsetzung sexueller Missbräuche (auch Cybergrooming) nicht gering ist.

[6] Es handelt sich um eine Verordnung der EU, welche November 2022 in Kraft getreten ist. Sie enthält vielfältige und teils völlig neuartige Regeln für digitale Vermittlungsdienste. Diese beinhalten Haftungsvorschriften für illegale Inhalte, ein weitreichendes System von verschärften und neuen Sorgfaltspflichten sowie ein effektives Durchsetzungsregime. https://www.bundesregierung.de/breg-de/suche/eu-regeln-online-plattformen-1829232

[7] Der Cybersecurity Act ist eine 2019 in der EU in Kraft getretene Verordnung zur Cybersicherheit. Diese führt ein einheitliches europäisches Zertifizierungsrahmenwerk für ITK-Produkte und Dienstleistungen ein. Die EU-Staaten sind verpflichtet, den CSA in vollem Umfang umzusetzen. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0209&from=EN