LANDESKRIMINALAMT
NIEDERSACHSEN

Lagebild Cybercrime und Kinderpornografie

in Niedersachsen

2023

Impressum

LKA NI

Dezernat 62
Zentralstelle Cybercrime/Kinderpornografie

Am Waterlooplatz 11
30169 Hannover

Erreichbarkeiten:

Tel.: 0511/9873-0
d62@lka.polizei.niedersachsen.de

Stand: 24. Mai 2024

Inhaltsverzeichnis

1 Was Sie erwartet 4
2 Cybercrime in Niedersachsen 5
2.1 Was ist Cybercrime? 5
2.2 Datengrundlage 5
2.3 Das Dunkelfeld 6
2.4 Phänomene der Cyberkriminalität 7
2.4.1 Ransomware 7
2.4.2 Angriffe gegen das Online-Banking 8
2.4.3 Phishing / Smishing 8
2.4.4 Distributed Denial of Service (DDoS) 9
2.4.5 Herausforderung Kryptowerte 9
2.4.6 Betroffenheit KRITIS 10
2.5 Herausragende Sachverhalte 10
2.5.1 Ransomware BlackCat 10
2.5.2 Messenger-Betrug „Hallo Mama, hallo Papa…“ 11
2.6 Prävention - „Vorbeugen ist besser als heilen“ 11
2.6.1 RIK und ProPK für Bürgerinnen und Bürger 12
2.6.2 ZAC für Unternehmen 12
2.6.3 Social Media für alle 13
3 Kinderpornografie in Niedersachsen 14
3.1 Herausforderungen der Kinderpornografie 14
3.2 Entwicklung der Fallzahlen 14
3.2.1 Zunahme der Ermittlungsverfahren 14
3.2.2 NCMEC-Verfahren 15
3.3 Phänomene 16
3.3.1 Inhalte mit fehlgeleitetem Humor 16
3.3.2 Sextortion 16
3.4 Sichergestellte Datenmengen 16
3.5 Herausragende Ermittlungsverfahren 17
3.5.1 Verbreitung von Kinderpornografie und Massendaten 17
3.5.2 Gemeinsamer Aktionstag Kinderpornografie 17
3.5.3 BKA-Öffentlichkeitsfahndung 17
3.6 Informationen zur Prävention 17
4 Blick in die Zukunft 18
4.1 Cybercrime 18
4.1.1 Beweismittelcloud 18
4.1.2 Künstliche Intelligenz und Cybercrime 18
4.2 Kinderpornografie 18
4.2.1 KI-Einsatz im Bereich der Datenaufbereitung 18
4.2.2 Anpassung des Strafrahmens 19

1 Was Sie erwartet

Zum zweiten Mal veröffentlicht das Landeskriminalamt Niedersachsen (LKA NI) das *„Lagebild Cybercrime und Kinderpornografie"*, in dem auf Grundlage der in Niedersachsen polizeilich bekannt gewordenen Straftaten Erkenntnisse und Entwicklungen dargestellt werden.

Unser Ziel ist es, Ihnen einerseits Einblicke und praktische Informationen zu bieten und andererseits die Herausforderungen der Sachbearbeitung zu erläutern.

Im Bereich Cybercrime informieren wir Sie über verschiedene Varianten der Cyber-Straftaten. Dabei werden statistische Zahlen ebenso betrachtet, wie das Dunkelfeld, herausragende Sachverhalte und Präventionsmöglichkeiten für Privatpersonen und Unternehmen.

Im Bereich der Verbreitungshandlungen von sexualisierter Gewalt an Kindern- und Jugendlichen informieren wir Sie unter anderem über Ermittlungsverfahren sowie die Auswirkungen automatisierter Meldesysteme, Herausforderungen bei der Bewältigung digitaler Beweismittel und den Einsatz künstlicher Intelligenz.

An verschiedenen Stellen dieses Lagebildes finden Sie QR-Codes, die Sie auf Wunsch zu Quellen und weiteren Informationen führen. Der nachfolgende QR-Code führt sie zu diesem Bericht auf der Homepage des Landeskriminalamtes Niedersachsen:

Erneut Fallzahlenanstieg bei Cybercrimedelikten

2022: **12.917** - 2023: **13.218**

+2,3 %

Erneut Anstieg bei Angriff gegen das Onlinebanking

- *Fallzahlen*

2022: **2.564** – 2023: **2.803**

+ 9,7 %

- Schadenssummen:

2022: **13,7 Mio** – **2023: 14,4 Mio**

+ 7,1 %

Hohes Dunkelfeld

- Laut Studie des LKA NI haben **24 %** der Befragten eine Cyber-Straftat angezeigt
- Nichtanzeige erfolgt häufig wegen fehlender Erfolgsaussichten

Phishing ist weiterhin Haupteinfallstor für Cyber-Straftaten gegen Privatpersonen und Unternehmen

Starker Fallzahlenanstieg im Bereich Kinderpornografie

Verbreitung Kinderpornografie

2022: **4.702** - 2023: **6.855**

+45,78 %

Besitz/Verschaffen

2022: **786** – 2023: **1.126**

+25,98 %

Menge der auszuwertenden kinderpornografischen Daten auf einem Höchststand

- Anzahl auszuwertender Asservate: **34.218**
- Datenvolumen: ca. **4,7 Petabyte (4.700 Terabyte)**

2 Cybercrime in Niedersachsen

2.1 Was ist Cybercrime?

Die Polizei unterscheidet im Bereich Cybercrime zwischen zwei Kategorien: Cybercrime im *engeren* Sinne und Cybercrime im *weiteren* Sinne.

Unter **CYBERCRIME IM *ENGEREN* SINNE** werden Straftaten erfasst, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme bzw. deren Daten richten, beispielsweise durch 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.

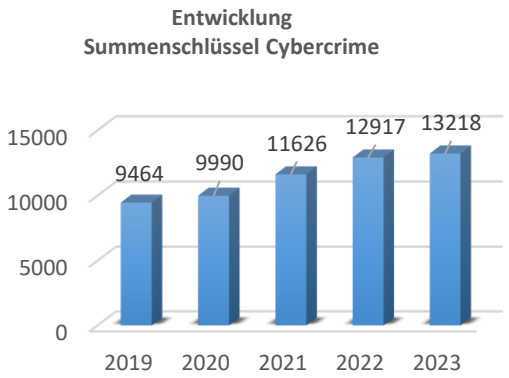
Im Rahmen von **CYBERCRIME IM *WEITEREN* SINNE** werden die oben genannten Informationssysteme lediglich als Mittel genutzt, um andere Ziele zu erreichen, beispielsweise Betrug auf Online-Verkaufsportalen oder Bedrohungen und Beleidigungen anderer Personen in sozialen Netzwerken etc. Diese Straftaten werden von den für das jeweilige Deliktsfeld zuständigen Fachbereichen bearbeitet, u.a. in den Kommissariaten, die für Gewalt, Freiheits- oder Eigentumsdelikte zuständig sind.

Während die Delikte der Cybercrime im *engeren* Sinne in der Mehrzahl Unternehmen betreffen, verursacht die Cybercrime im *weiteren* Sinne überwiegend bei Privatpersonen Schäden. Dieses Lagebild befasst sich mit beiden Ausprägungen der Cybercrime und wird aufzeigen, dass auch Fälle der Cybercrime im *weiteren* Sinne z.B. aufgrund komplexer Täterstrukturen bei Bedarf durch Spezialdienststellen übernommen und bearbeitet werden.

2.2 Datengrundlage

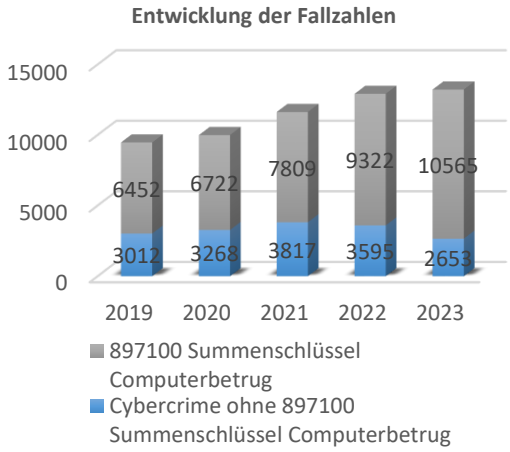
Bei der Polizeilichen Kriminalstatistik (PKS) handelt es sich um die Datenbasis des so genannten polizeilichen Hellfeldes. Mit bundesweit einheitlichen Kriterien werden nach Abschluss der Ermittlungen bekannt gewordene Straftaten und deren Versuche erfasst.

Die Cyberstraftaten, die in der PKS registriert sind, werden unter dem Summenschlüssel "897000 - Cybercrime" zusammengeführt. Hierbei handelt es sich unter anderem um das Ausspähen und Abfangen von Daten einschließlich der Vorbereitung (§§202 a-c StGB), Datenhehlerei (§202d StGB), Computerbetrug (§263a StGB), Fälschung beweiserheblicher Daten (§269 StGB), Täuschung im Rechtsverkehr bei Datenverarbeitung (§270 StGB) sowie Datenveränderung und Computersabotage (§§303a, b StGB). Die folgende Grafik zeigt die weiterhin steigenden Fallzahlen des Summenschlüssels Cybercrime.



Vom Jahr 2022 (12.917) zum Jahr 2023 (13.218) beträgt die Steigerung 2,3 %.

Die Delikte des Computerbetrugs (= Delikte, bei denen nicht ein Mensch, sondern ein System getäuscht wird) haben am Summenschlüssel Cybercrime einen besonders hohen Anteil an der Gesamtzahl. In den Jahren 2021 bis 2023 stiegen die Fallzahlen im Bereich des Computerbetrugs (7.809 auf 10.565), während die der eher qualifizierteren Delikte der Cybercrime im *engeren* Sinne zurückgingen (3.817 zu 2.653 - siehe Grafik unten).



Ein Grund dafür ist, dass die PKS keine Straftaten oder Versuche aufzeigt, deren Tatort[1] vollkommen unbekannt ist oder sich im Ausland befindet.
Da technische Möglichkeiten nicht nur die Identität der Täterinnen oder Täter, sondern auch den Ort der Tathandlung effektiv verschleiern können, werden zahlreiche Cybercrime-Delikte nicht erfasst. Auch in Fällen, in denen der Tatort zwar bekannt ist, sich jedoch im Ausland befindet, spiegeln sich die entsprechenden Verfahren nicht in der PKS wider.
Bei den Taten des Computerbetrugs kommen Ermittlungserfolge mit Tatort in Deutschland häufiger vor als bei den eher qualifizierteren Delikten der Cybercrime im *engeren* Sinne. Da bei diesen qualifizierteren Delikten der Tatort in den meisten Fällen unbekannt ist oder im Ausland liegt, werden sie in der PKS häufig nicht berücksichtigt. Dies betrifft auch besonders komplexe Verfahren, die oft über Jahre hinweg in Kooperation mit internationalen Behörden aufwendig geführt werden.

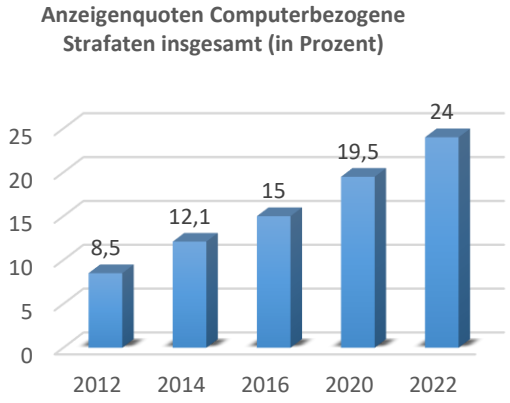
Um über die PKS hinaus ein realistischeres Bild darüber zu erhalten, wie häufig Cyber-Straftaten auftreten und wie sich ihre Phänomene verändern, analysiert das LKA NI im Rahmen eines spezifischen Monitorings die Sachverhalte der angezeigten Straftaten manuell und ordnet diese den Phänomenen zu. Obwohl diese Erkenntnisse Momentaufnahmen sind und den individuellen Fortschritt der Ermittlungen nicht berücksichtigen, ermöglicht diese Art der Analyse dennoch wertvolle Einblicke in die Entwicklung der Varianten.
Da diese Datenbasis jedoch weder valide noch reproduzierbar ist, werden im Lagebild grundsätzlich PKS-Daten des Landes Niedersachsen wiedergegeben. Zahlen, die der LKA-spezifischen Erhebung zugrunde liegen, werden auch als solche benannt.

Wie im nächsten Kapitel zu lesen ist, führt neben der PKS auch das Dunkelfeld zu Herausforderungen bei der Bewertung der Fallzahlen.

2.3 Das Dunkelfeld

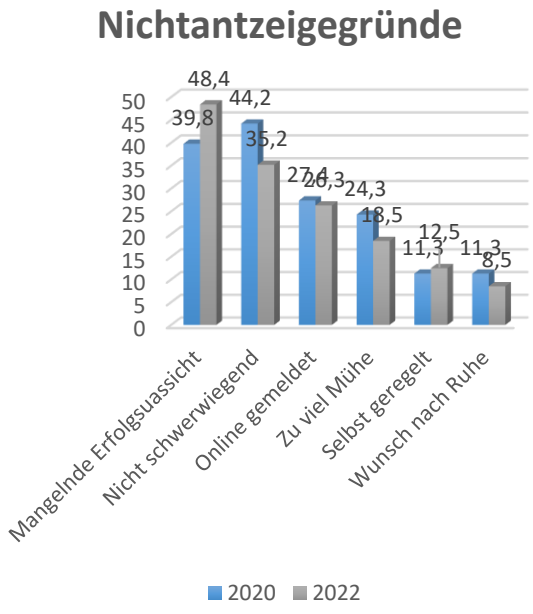
Unter dem so genannten Dunkelfeld versteht man die Straftaten, die nicht angezeigt wurden und somit der Polizei nie bekannt geworden sind. Es gibt verschiedene Studien, die sich mit er Erhellung des Dunkelfeldes beschäftigten.

Im Rahmen der fünften "*Befragung zu Sicherheit und Kriminalität*" (s. QR-Code links) wurden 2022 durch das LKA NI das Sicherheitsempfinden und Kriminalitätserleben der Bürgerinnen und Bürger auch in Hinsicht auf Cyberkriminalität erfragt. Fast 16.000 Teilnehmende aus Niedersachsen gaben unter anderem Auskunft über ihr Anzeigeverhalten bzw. Gründe der Nichtanzeige bei Cyber-Straftaten. Dem Kernbefundbericht 2023 ist zu entnehmen, dass lediglich 24 % der computerbezogenen Straftaten angezeigt wurden. Drei Viertel der Taten werden der Polizei nicht bekannt. Die untenstehende Grafik zeigt, dass sich seit 2012 das Anzeigenaufkommen von lediglich 8,5 Prozent auf immerhin 24 Prozent fast verdreifacht hat. Laut dem Bericht wurden die



Betrugstaten im Internet mit 34,2 % am häufigsten angezeigt.

Die meisten Teilnehmenden gaben als Grund für das Nichtanzeigen einer computerbezogenen



[1] Ort, an dem die Täterin oder der Täter gehandelt hat.

Straftat die Einschätzung an, dass die Polizei die Tat nicht hätte aufklären können (48,4 %). Dieser Wert hat sich im Vergleich zur vorherigen Befragung im Jahr 2020 (39,8 %) um knapp neun Prozent erhöht. 35,2 % der Teilnehmenden empfanden die erlebte Tat als nicht schwerwiegend (2020: 44,2 %) und 26,3 % gaben lediglich eine Online-Meldung bei einem Provider oder dergleichen ab, statt die Tat anzuzeigen (2020: 27,4 %).

Für Delikte aus dem Bereich Kinder- und Jugendpornografie lassen sich keine Aussagen über das Ausmaß des Dunkelfelds treffen. Hier liegen weder Studien noch anderweitige Forschungsergebnisse vor. Auch wenn automatisierte Meldesysteme wie z.B. NCMEC (siehe auch Punkt 3.2.2) einen besseren Erkenntnisgewinn ermöglichen, muss doch von einem enormen Dunkelfeld ausgegangen werden.

Für die Deliktsbereiche Cybercrime sowie Kinder- und Jugendpornografie gilt daher gleichermaßen, dass eine Anzeigenerstattung für die Bekämpfung der Kriminalität sowie Entwicklung von Präventionsstrategien von großer Bedeutung ist.

2.4 Phänomene der Cyberkriminalität

Im folgenden Abschnitt werden diejenigen Phänomene der Cyberkriminalität beleuchtet, die derzeit aus polizeilicher Sicht am Bedeutsamsten sind und sowohl für Unternehmen als auch für Privatpersonen schwerwiegende Folgen haben können.

2.4.1 Ransomware

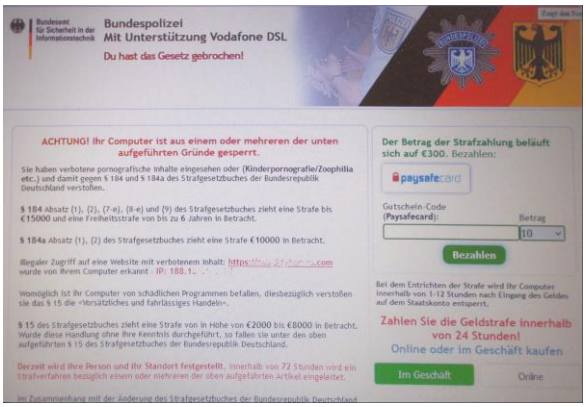
Ransomware, auch bekannt als Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner, ist eine Art von Schadsoftware. Sie ermöglicht einem Angreifer, den Zugriff des Computerinhabers auf Daten oder das gesamte Computersystem zu verhindern. Dabei werden entweder Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie blockiert. Anschließend wird in der Regel ein Lösegeld gefordert, um die Daten wieder freizugeben oder das System zu entsperren. Die Bezeichnung setzt sich zusammen aus dem englischen Wort für Lösegeld (ransom) und ware, entsprechend dem für verschiedene Arten von Computerprogrammen üblichen Benennungsschema (Software, Malware etc.).

Es gibt zwei Haupttypen von Ransomware:

1. **Locker-Ransomware:** Diese Variante verhindert den Zugriff beispielsweise durch einen Sperrbildschirm.
2. **Krypto-Ransomware:** Dabei werden Dateien verschlüsselt, sodass Nutzende nicht mehr auf sie zugreifen können.

LOCKER-RANSOMWARE

Wurden 2022 im Rahmen der LKA-spezifischen Erhebung lediglich zwei Fälle der Ransomware-Variante mit dem Sperrbildschirm auf PCs bekannt, sind 2023 wieder mehr Fälle als im Vorjahr angezeigt worden (57). In den meisten Fällen wurde die Bundespolizei als angeblicher Absender vorgetäuscht und es wurden Zahlungsmöglichkeiten über paysafecard oder Google Play-Gutscheincode angeboten.



In der Regel ist es den Tätern im Vorfeld gelungen, die Geschädigten dazu zu bringen, über E-Mails oder Werbebanner Schadsoftware auf dem eigenen PC zu installieren. Diese nistet sich soweit in dem System ein, dass sie auch bei einem Neustart wieder aufgerufen wird.

Die Polizei rät davon ab, auf die Forderung einzugehen. Es ist nicht garantiert, dass nach der Zahlung der Sperrbildschirm verschwindet und es kann gegebenenfalls noch weitere Schadsoftware auf dem Rechner verbleiben. Abhilfe kann in diesen Fällen die Nutzung von Rettungssoftware bringen, die beim Starten des Systems über USB oder CD gebootet werden kann.

KRYPTO-RANSOMWARE

Institutionen und besonders Unternehmen sind durch diese Variante betroffen, da unter anderem durch Produktionsausfall und Wiederherstellung der Arbeitsfähigkeit die Kosten den Millionenbereich erreichen können und somit existenzbedrohend sein können.

In Niedersachsen ist bei der LKA-spezifischen Erhebung der Einsatz der Ransomware-Varianten Lockbit, NoEscape, Blackcat sowie 24 weitere Varianten festgestellt worden. In fast allen Fällen wurden die Daten vor der Verschlüsselung ausgeleitet und es wurde zusätzlich mit der

Veröffentlichung dieser internen Daten gedroht (Double Extortion). Die höchste geforderte Erpressungssumme betrug in Niedersachsen umgerechnet 2,5 Mio. Euro.

Zwar ist in Niedersachsen von 2022 (104 Fälle) auf 2023 (81 Fälle) ein Rückgang von ca. 20 % bei den Anzeigen von betroffenen Institutionen zu erkennen. Allerdings kann dies kein Zeichen der Entspannung sein, da die Täter sich nicht nach geografischen Regionen richten, sondern angreifen, wenn sich eine Gelegenheit bietet. Weltweit wurde im Jahr 2023 eher von einer Zunahme der Ransomware-Angriffe berichtet und auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezeichnet im Bericht[2] *„Die Lage der IT-Sicherheit in Deutschland 2023"* Ransomware-Angriffe als Hauptbedrohung.

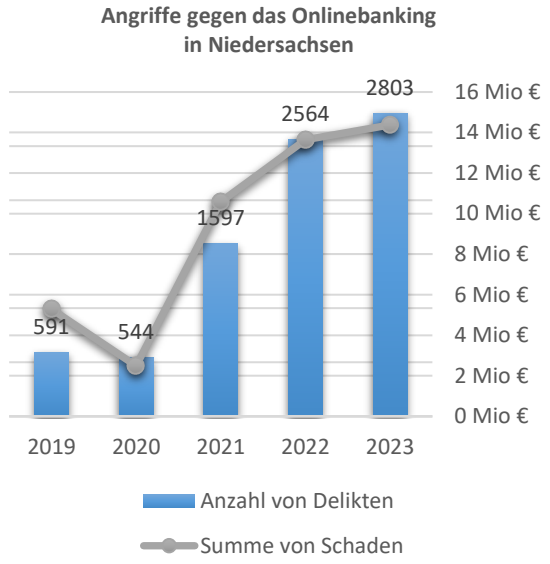
2.4.2 Angriffe gegen das Online-Banking

Beim Angriff gegen das Onlinebanking versuchen Täter unbefugten Zugriff auf die Online-Banking-Dienste einer Bank zu erlangen und diese Zugangsberechtigungen missbräuchlich zu verwenden.

Zu den betroffenen Online-Banking-Angeboten gehören Girokonten, Sparkonten, Wertpapierdepots und ähnliche Dienste. Die Täter nutzen verschiedene Methoden, um an die Zugangsdaten zu gelangen. Dazu gehören weniger direkte Angriffe auf die Webseiten der Banken, sondern vor allem Vorbereitungshandlungen wie das Einsetzen von Phishing und Malware gegenüber Bankkunden.

Cyberkriminelle nutzen verschiedene Techniken wie Phishing-E-Mails, Malware und sog. Keylogger um Zugriff auf Bankdaten von Personen zu erhalten. Aber auch Fakeshops werden extra dafür eingerichtet, um an Zugangsdaten für das Onlinebanking zu gelangen. Gestohlene Daten werden in der Regel im Darknet verkauft oder direkt für betrügerische Zwecke verwendet.
Die entwendeten Daten werden durch weitere Täter dazu genutzt, um sich beispielsweise telefonisch als Mitarbeitende der Bank auszugeben und die kontoführende Person dazu zu bringen, eine im Hintergrund vorbereitete Änderung oder Überweisung zu autorisieren. Gelingt es der Täterin oder dem Täter auf diesem Weg ein zweites Gerät für die Nutzung des Onlinebanking freizuschalten, ist nicht nur eine betrügerische Überweisung möglich, sondern auch ein Zugriff auf alle Konten des Onlinebanking, wodurch ein noch größerer Schaden droht.

Für Niedersachsen konnte in der LKA-spezifischen Erhebung für 2023 das dritte Jahr in Folge eine deutliche Zunahme der Anzeigen festgestellt werden. Seit 2020 ist die Zahl der Straftaten um das Fünffache auf 2.803 Fälle gestiegen, wie in der folgenden Grafik zu sehen ist:



2.4.3 Phishing / Smishing

Beim **PHISHING** versuchen Betrüger, an sensible Informationen wie Personalien, Login-Daten, Kreditkarten- oder Bankdaten zu gelangen, indem sie sich als vertrauenswürdige Quellen ausgeben. Hierbei werden potenzielle Opfer unter einem Vorwand dazu aufgefordert, ihre Daten an die Cyberkriminellen zu übermitteln. 2023 traten folgende Methoden vermehrt auf:

- So genannte Fakeshops, bei denen vermeintlich gute Angebote zur Bestellung verleiten, tatsächlich jedoch nur darauf abzielen, Daten abzuschöpfen. Die Ware wird nicht geliefert und der Kontakt zum Verkäufer bricht ab
- Vorgetäuschte Käufe bei Online-Verkaufsportalen. Den Verkäufern wird anhand eines Links und einer täuschend echt aussehenden Seite suggeriert, die Zahlung für die Ware zu erhalten. Tatsächlich werden die Angaben missbraucht, um die mitgeteilten

[2] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Kreditkartendaten unbefugt einzusetzen oder Echtzeitüberweisungen vom Girokonto zu veranlassen

Der Begriff **SMISHING** beschreibt das gleiche Phänomen. Der Unterschied besteht darin, dass das Opfer eine SMS erhält in der es aufgefordert wird, einen Link zu klicken oder eine Nummer anzurufen. Auch hier verfolgen Täterinnen und Täter das Ziel, die Daten der Nachrichtenempfänger zu erhalten und diese missbräuchlich einzusetzen.
2023 wurden unter anderem folgende Varianten bekannt:

- Angebliche Hausbank täuscht vor, dass das Push-TAN-Verfahren abläuft bzw. Daten zu verifizieren sind
- Angeblicher Paketzusteller gibt vor, dass ein Paket nicht zugestellt werden könne und die Kreditkartenzahlung eines Kleinbetrags erforderlich sei
- Angebliche Angehörige teilen mit, dass das Handy kaputt sei und fordern den Empfänger der Nachricht auf, über WhatsApp an die mitgeteilte Nummer zu schreiben. Hierüber finden Sie nähere Informationen unter Punkt 2.5.2

Es ist festzustellen, dass das „Phishen" von Daten bei Account-Missbrauch, diversen Betrugsvarianten, bei Angriffen gegen das Onlinebanking bis hin zu vielen Ausprägungen von Ransomware-Attacken die Hauptursache dafür ist, dass Cyber-Straftaten zum Erfolg führen oder erst ermöglicht werden.

2.4.4 Distributed Denial of Service (DDoS)

Mit DDoS-Attacken werden Webserver oder ganze Netzwerke durch eine Flut von gleichzeitigen Anfragen von mehreren Computern lahmgelegt. Diese Angriffe, die oft durch sog. Botnetze koordiniert werden, können Server im Internet temporär zum Ausfall bringen, zu Beeinträchtigungen führen und potenziell erheblichen Schaden verursachen.

Gemäß der LKA-spezifischen Erhebung ist die Anzahl der gemeldeten DDoS-Angriffe in Niedersachsen im Jahr 2023 mit 15 bekannten Angriffen im Vergleich zum Vorjahr gleichgeblieben. Besorgniserregend ist jedoch der Anstieg der Angriffe auf öffentliche Institutionen. Diese Zunahme wird u.a. mit dem Ukraine-Krieg in Verbindung gebracht.

Während Medienberichte von einem starken Anstieg der DDoS-Angriffe sprechen, zeigen die polizeilichen Anzeigen ein anderes Bild. Dies lässt sich auf zwei Faktoren zurückführen:

Viele Unternehmen und Institutionen haben ihre IT-Sicherheitssysteme durch effektive Schutzmaßnahmen gegen DDoS-Angriffe verstärkt. Diese Maßnahmen verhindern Angriffe oft im Vorfeld oder mildern diese derart ab, dass häufig kein Schaden eintritt, womit eine geringere Anzeigebereitschaft einhergeht.

Die Hackergruppe NoName057(16), die im März 2022 erstmals in Erscheinung trat, hat sich 2023 durch zahlreiche Angriffe auf Webseiten von Behörden und Unternehmen - auch in Niedersachsen - hervorgetan. Die Gruppe, die sich selbst als pro-russisch bezeichnet, zielt mit ihren Aktionen darauf ab, Staaten zu bestrafen, die die Ukraine unterstützen.
NoName057(16) geht dabei strategisch vor und rechtfertigt entsprechende Angriffe auf ihren einschlägigen Social-Media-Kanälen. Sobald beispielsweise die Bundesrepublik Deutschland neue Hilfslieferungen an die Ukraine beschließt, starten die Cyberkriminellen eine Angriffswelle. Ihre Ziele sind dabei insbesondere Websites von staatlichen Institutionen, Polizeibehörden und verschiedenen Verkehrsunternehmen.
Bislang konnten jedoch im Jahr 2023 in keinem Fall gravierende Schäden durch Angriffe festgestellt werden.

Die Aktivitäten von NoName057(16) stellen zwar eine Bedrohung für die digitale Infrastruktur dar und sollten ernst genommen werden. Die Gruppe zeigt jedoch, dass sie ihre Angriffe scheinbar bewusst so plant, dass sie keine gravierenden Schäden verursachen. Es ist daher wahrscheinlich, dass es NoName057(16) in erster Linie um Aufmerksamkeit und politische Einflussnahme geht, weniger um unmittelbaren Schaden.

2.4.5 Herausforderung Kryptowerte

Cyberkriminelle nutzen als bevorzugte Zahlungsmethode so genannte Kryptowerte wie z.B. Bitcoin oder Ethereum, deren Vorteil für die Kriminellen unter anderem darin liegt, dass Geldtransfers zwar pseudonym[3] durchgeführt werden können, jedoch mittels Methoden zur Anonymisierung in öffentlich verwendbaren Portalen nicht nachvollzogen werden können. Zur weiteren Verschleierung werden die Kryptowerte in

[3] Transaktionsdetails können öffentlich eingesehen werden, welche ggf. Rückschlüsse auf Beteiligte zulassen können.

der Regel zusätzlich über so genannte Krypto-Mixer[4] weitergeleitet und beispielsweise auch in andere Krypto-Assets umgewandelt. Die letztendliche Auszahlung von Kryptowerten in „echtes Geld" erfolgt häufig erst nach Durchführung diverser Transfers, Nutzung der benannten Krypto-Mixer und anderer Methoden wie der Verwendung von Geldwäschestrukturen.
Polizeibehörden müssen auf spezielle Softwarelösungen zurückgreifen, um die hochkomplexen Ermittlungen zu Kryptowerten überhaupt führen zu können.

2.4.6 Betroffenheit KRITIS

KRITIS steht für „Kritische Infrastrukturen" und umfasst lebenswichtige Einrichtungen, u.a. der Energie- und Wasserversorgung, das Gesundheitswesen und Telekommunikations-anbieter, deren Ausfall schwerwiegende Folgen für die öffentliche Sicherheit und das Gemeinwohl haben könnte.

Im Jahr 2023 waren in Niedersachsen insbesondere der Versicherungsbereich, das Gesundheitswesen, der Luftfahrt- und Lebensmittelsektor sowie der Verkehrsbereich von Cyberangriffen betroffen.
Darüber hinaus waren staatliche Einrichtungen ebenfalls Ziel von Angriffen. Die führenden Angriffsarten waren DDoS- und Ransomware-Angriffe. Die DDoS-Angriffe fokussierten sich in Niedersachsen primär auf staatliche Einrichtungen.
Angriffe unter Einsatz von Ransomware konnten über alle Bereichen hinweg festgestellt werden. Vereinzelt kam es zusätzlich zu Rechnungsmanipulationen und Angriffsversuchen unter Ausnutzung von Sicherheitslücken in Softwareprodukten.
Durch die Angriffe kam es zu internen Störungen der Unternehmensprozesse und langfristig erhöhtem Arbeitsaufkommen. Die kritischen Infrastrukturen konnten allerdings zu jeder Zeit aufrechterhalten werden.

2.5 Herausragende Sachverhalte

2.5.1 Ransomware BlackCat

Die Zentrale Kriminalinspektion der Polizeidirektion Göttingen führt unter der Sachleitung der Staatsanwaltschaft Göttingen – Zentralstelle Internet- und Computerkriminalität (Cybercrime) seit Dezember 2021 in Zusammenarbeit mit Europol, europäischen und US-amerikanischen Ermittlungsbehörden zentrale Ermittlungen gegen die international agierende Ransomware-Gruppierung „ALPHV/Blackcat", u.a. wegen des Verdachts der banden- und gewerbsmäßigen Erpressung.
Die erstmalig im November 2021 in Erscheinung getretene Ransomware „BlackCat" wurde auf Darknet-Seiten durch die Gruppierung ALPHV als „Ransomware-as-a-Service" zur Verfügung gestellt.

Mit der Ransomware können betroffene IT-Systeme vollständig verschlüsselt und erst unter Verwendung eines Entschlüsselungs-Tools, das die Tätergruppierung gegen eine hohe Lösegeld-zahlung zur Verfügung stellt, entsperrt werden. Interessierte „Affiliates", also Kunden der Gruppierung, konnten die zur Verfügung gestellte Ransomware nutzen und in erpresserischer Absicht eigeninitiativ gegen Unternehmen für eine Teil- oder Vollverschlüsselung einsetzen.

Im Rahmen der zentralen Ermittlungen konnten für das Bundesgebiet bisher 76 geschädigte Unternehmen registriert werden. Die weltweit bekannt gewordenen Fallzahlen liegen bei über 750, wobei die Dunkelziffer noch höher zu vermuten ist. Die Tätergruppe zeichnet weltweit für einen Schaden im Milliardenbereich verantwortlich,

[4] Dienste / Software zur Verschleierung der Transaktionen

wobei alleine in Deutschland Forderungen in Höhe von fast 450 Mio. USD gestellt wurden.

Die Ermittlungen der im März 2022 eingerichteten internationalen Ermittlungsgruppe „Chimera" führten zur Identifizierung und Lokalisierung der Server der Tätergruppierung.

Durch den Einsatz technischer Maßnahmen konnte die Zentrale Kriminalinspektion der Polizeidirektion Göttingen Details zu der Ransomware „Blackcat" erlangen. Durch die im Rahmen der Ermittlungen gewonnenen Erkenntnisse konnten aus dem Verbund der international agierenden Behörden mehrere Webseiten und die auf den entsprechenden Servern befindlichen Daten im Dezember 2023 beschlagnahmt werden. Bei Aufruf der täterseitig genutzten Webseiten wird nunmehr ein Banner angezeigt, der darauf hinweist, dass die jeweilige Seite beschlagnahmt wurde. Die Ermittlungen dauern an.

2.5.2 Messenger-Betrug „Hallo Mama, hallo Papa…"

Texte mit gleichem oder ähnlichem Inhalt erreichten und erreichen tausende Handynummern via SMS oder WhatsApp Nachricht. Seit September 2023 ermittelt das Fachkommissariat Cybercrime der Zentralen Kriminalinspektion Osnabrück gegen zunächst unbekannte Personen im Rahmen eines Strukturermittlungsverfahrens.
Durch Auswertung von gleichgelagerten Fällen sowie durch Überwachung von Mobilnummern, welche die betrügerischen Nachrichten übersandt hatten, konnten zwei Tatverdächtige in Frankfurt am Main lokalisiert werden. Die weiteren Ermittlungen ergaben, dass die Tatverdächtigen Hotelzimmer im Bereich Frankfurt am Main mit falschen Personalien anmieteten und diese dann mit Kreditkarten bezahlten, für die sie nicht verfügungsberechtigt waren. Aus den Hotelzimmern verschickten sie teilweise bis zu 40.000 Nachrichten pro "Spam-Welle" nach dem im Bild erkennbaren Muster.

Derzeit können den beiden Tatverdächtigen etwa 220.000 Nachrichten zugeordnet werden. Dabei übermittelten die Tatverdächtigen lediglich die SMS mit der Mobilnummer. Die weitere Kommunikation wurde durch andere Personen geführt.

Die beiden 20-jährigen Tatverdächtigen konnten identifiziert und im Dezember 2023 an ihren Wohnanschriften festgenommen werden. Das Amtsgericht Osnabrück erließ für beide Beschuldigte einen Haftbefehl.

Die Durchsuchung der Wohnobjekte führte zum Auffinden von umfangreichem Beweismaterial. Erste Erkenntnisse der Auswertungen lassen darauf schließen, dass die Beschuldigten für zahlreiche weitere Straftaten in Frage kommen. Die Ermittlungen dauern an.

Fälle mit dieser Betrugsmasche, wie der zuvor beschriebenen, sind seit 2022 bekannt. Diese Variante war daher 2023 ein Schwerpunkt im Bereich der polizeilichen Prävention, da viele Angeschriebene der Aufforderung folgten und sich im weiteren Gesprächsverlauf zu Echtzeitüberweisungen überreden ließen.
Das LKA NI stand für Interviews in diversen Produktionen (z.B. Panorama, Aktenzeichen XY, Regionale Nachrichten diverser Sender) zur Verfügung. Das ZDF ließ für die Live-Sendung von Aktenzeichen XY im Mai 2023 einen Kurzfilm zu dieser Masche produzieren. Zudem wurde eine bundesweite Kampagne zu der Thematik durch das Programm Polizeiliche Kriminalprävention (ProPK) in den Sozialen Medien veröffentlicht.

Auch 2024 gibt es weiterhin Fälle, in denen unbekannte Täter bei vermeintlichen Angehörigen hohe Summen erbeuten. Die Masche wurde in Einzelfällen bereits dahingehend erweitert, dass per WhatsApp behauptet wird, dass die Täter verurteilt wurden und Geschädigte nun den Schaden ersetzt bekämen. Hierzu werden die aus der Vortat bekannten Daten und Schadenssummen genutzt, um Seriosität vorzutäuschen und die Geschädigten zur Herausgabe weiterer Daten bzw. Zahlung einer "Gebühr" zu verleiten. Im nächsten Kapitel finden Sie Informationen über Präventionsangebote zu diesem und vielen anderen Phänomenen.

2.6 Prävention - „Vorbeugen ist besser als heilen"

Dieses alte Sprichwort ist in der heutigen digitalen Zeit besonders relevant. Wie bereits auf den vorangegangenen Seiten berichtet wurde, stellen Cyberangriffe eine Bedrohung sowohl für Privatpersonen als auch für Unternehmen dar. Die

Folgen, sobald Daten in die Hände von Angreifern gelangen, sind oft schwerwiegend. Angesichts der Tatsache, dass das Internet bekanntlich nichts vergisst, besteht die Gefahr, dass persönliche Informationen und sogar sensible Unternehmensdaten noch Jahre später missbraucht werden können.
Im Weiteren stellen wir Ihnen verschiedene Informationsquellen vor, die Ihnen helfen können, sich besser zu schützen.

2.6.1 RIK und ProPK für Bürgerinnen und Bürger

Bereits seit 2013 informiert der Ratgeber Internetkriminalität (RIK) des LKA NI die Bevölkerung über aktuelle Phänomene der Internetkriminalität.

Schnellstmöglich werden auf der Homepage des RIK **WWW.POLIZEI-PRAEVENTION.DE** Tatvarianten anschaulich vorgestellt und gleichzeitig Tipps gegeben, wie Sie sich davor schützen können, bzw. was im Falle eines Schadens zu tun ist.

In den vergangenen 10 Jahren wurden
- Über 600 Warnmeldungen veröffentlicht
- die Homepage millionenfach aufgerufen
- rund 10.000 Anfragen beantwortet

Die Homepage ist damit zu einer wichtigen Anlaufstelle für die Prävention im Bereich der Internetkriminalität geworden

Das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) bietet auf der Internetseite **WWW.POLIZEI-BERATUNG.DE** umfassende Sicherheitstipps zum Schutz vor Straftaten. Es informiert nicht nur über Opferrechte und Entschädigungsmöglichkeiten, sondern betrachtet auch Delikte sowohl in der realen als auch in der virtuellen Welt. Dabei werden verschiedene Begehungsformen von (Cyber-) Straftaten detailliert erläutert und verschiedene Hilfsangebote zur Durchsetzung von Ansprüchen vorgestellt.

2.6.2 ZAC für Unternehmen

Die Zentrale Ansprechstelle Cybercrime für die niedersächsische Wirtschaft (ZAC) im LKA NI ist die polizeiliche Beratungsstelle für Firmen, Verbände und Behörden bei der Prävention von Cyberkriminalität und erster Ansprechpartner im Schadensfall (Anfragen 2023: 431; 2022: 329).

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 (Vorträge 2023: 114; Vorträge 2022: 84).

Die ZAC veranstaltet seit Anfang des Jahres 2023 gemeinsam mit der IHK Niedersachsen sowie einer Unternehmensberatungsfirma als neues Präventionsformat Cyberabwehrübungen bzw. Planspiele für die niedersächsische Wirtschaft. Im Rahmen der Cyberabwehrübungen versuchen die Teilnehmenden in Krisenteams einen simulierten (realitätsnahen) - Ransomware-Angriff - auf eine fiktive Firma zu bewältigen. Dabei werden die Teilnehmenden zielgerichtet durch die ZAC beraten und unterstützt. Das Ziel der Übungen besteht insbesondere darin, die notwendigen Reaktionen bei einem Ransomware-Angriff kennenzulernen bzw. zu optimieren sowie grundsätzlich die Resilienz der Unternehmen im Bereich Cyberabwehr zu fördern. Darüber hinaus werden u. a. auch die polizeilichen Unterstützungsleistungen im Schadensfall sowie in dem präventiven Bereich vermittelt. Die durchgeführten Planspiele wurden seitens der Teilnehmenden bisher durchweg positiv bewertet. Das positive Feedback spiegelt sich u.a. auch durch die vielen Kontaktaufnahmen der teilnehmenden Firmen wider, welche nach dem Angebot der Awareness-Vorträge zum Thema „aktuelle Cybercrime Phänomene sowie präventive Maßnahmen und Maßnahmen für den Schadensfall“ fragen. Denn es ist mehr als nur eine Plattitüde, wenn man sagt, dass es keine Frage ist, ob ein Unternehmen Opfer eines Cyberangriffs wird, sondern vielmehr die Frage, wann es ein Unternehmen trifft.

Weitere Informationen und Angebote finden Sie unter **WWW.ZAC-NIEDERSACHSEN.DE**.

2.6.2.1 Spam-Mail oder Schadsoftware?

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 uns so in die Lage zu versetzen, frühzeitig neue Deliktsvarianten zu erkennen, zu veröffentlichen und zu bekämpfen.

2.6.3 Social Media für alle

In den Beiträgen des Instagram-Kanals **POLIZEI.BRAUNSCHWEIG.ZKI** werden Phänomene erläutert und Sicherheitstipps vorgestellt. Zu einigen Themen wurden so genannte Highlights angelegt, welche Zusammenstellungen verschiedener Informationen zu einem Thema beinhalten.

Das LKA NI nutzt aktiv den Facebook-Account **@LKANIEDERSACHSEN**, um zeitnah über aktuelle Cybercrime-Phänomene zu informieren und Tipps zur Prävention zu geben. Mithilfe von Bild- und Videobeiträgen werden sowohl neu entdeckte als auch altbekannte Phänomene präsentiert.

3 Kinder- und Jugendpornografie in Niedersachsen

3.1 Herausforderungen der Kinder- und Jugendpornografie

Kinder- und Jugendpornografie bezeichnet Abbildungen pornografischer Inhalte in Form von Foto-/ oder Videodateien, die sexuelle Handlungen von, an oder vor einer Person unter 14 bzw. unter 18 Jahren zeigen. Durch die weltweite Verbreitung und Verfügbarkeit erfolgt eine dauerhafte Viktimisierung der Opfer. Der Begriff „Kinderpornografie" ist mittlerweile umstritten. Nach herrschender Meinung wirke der Begriff verharmlosend und stelle nicht hinreichend heraus, dass der Herstellung derartiger Darstellungen in der Regel ein realer sexueller Missbrauch zugrunde liegt. Nach Einschätzung der Expertinnen und Experten könnte sich die Begrifflichkeit „Darstellungen sexueller Missbrauchshandlungen an Kindern und Jugendlichen" auf lange Sicht durchsetzen. Im Strafgesetzbuch (StGB) wird gleichwohl explizit von Kinder- und Jugendpornografie gesprochen. In der vorliegenden Lagebild-darstellung erfolgt keine Differenzierung der Begriffe.

Mit dem Internet verbundene Endgeräte wie Smartphones, Tablets, PCs oder auch Spielekonsolen sind aus dem Alltag der Gesellschaft nicht mehr wegzudenkenden. Verbunden mit immer größer werdenden Speichervolumen der Geräte ist es möglich, eine enorme Anzahl von Bildern und Videos abzulegen.

Im Deliktsbereich Kinder- und Jugendpornografie bietet das Internet als Tatmittel ein stetig wachsendes Spektrum an Nutzungsmöglichkeiten, die sowohl die Prävention, als auch die Strafverfolgung vor immer neue Herausforderungen stellen. Die Verbreitung der Inhalte in Foren, Chats und über Messenger jeglicher Art sind dabei weiterhin von großer Bedeutung. Hinweise durch ausländische Provider führen weiterhin zu einem immensen Anstieg der Fallzahlen.

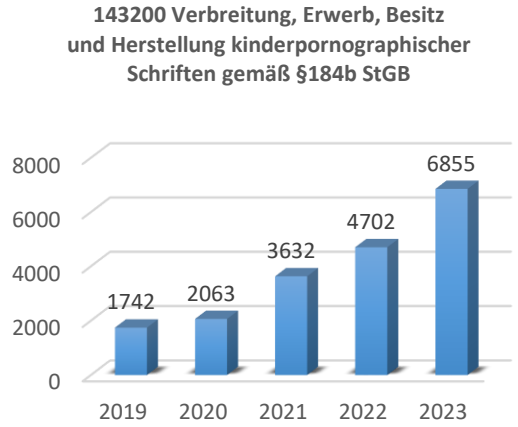
Kinder und Jugendliche begehen selbst, überwiegend durch unbedachtes Verhalten oder digitale Naivität, viele Einzeltaten in dem Deliktsbereich. Dazu gehören selbstgefertigte Aufnahmen, die von sich oder gleichaltrigen Personen verbreitet werden, ohne sich der strafrechtlichen Konsequenzen bewusst zu sein.

Mit einer Verringerung der Fallzahlen ist auch in Zukunft nicht zu rechnen.

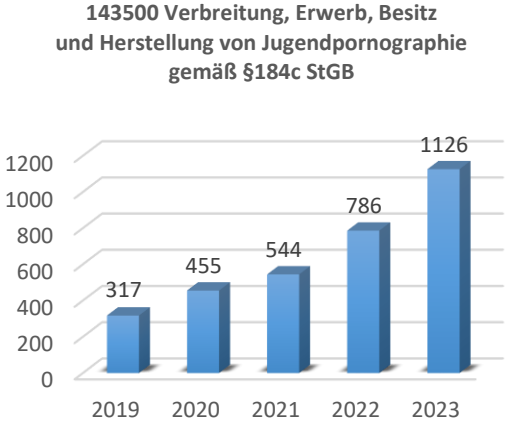
3.2 Entwicklung der Fallzahlen

3.2.1 Zunahme der Ermittlungsverfahren

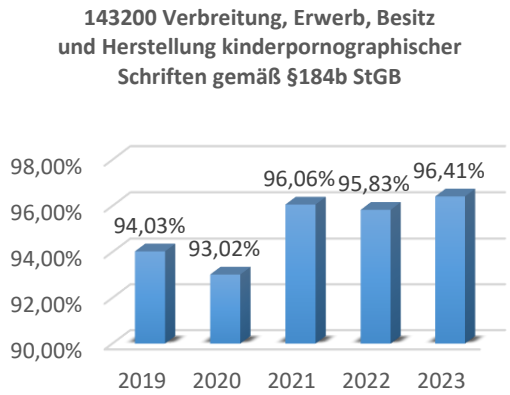
Die Fallzahlen der Delikte im Bereich Kinder- und Jugendpornografie stiegen in Niedersachsen im Jahr 2023 erneut an. Im Deliktsbereich von Verbreitung, Erwerb, Besitz und Herstellung kinderpornografischer Schriften ist ein Anstieg von 4.702 Fällen im Jahr 2022 auf 6.855 im Jahr 2023 zu verzeichnen.

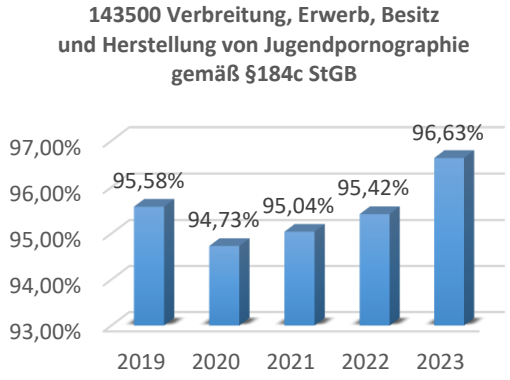


Im Bereich von Verbreitung, Erwerb, Besitz und Herstellung von Jugendpornografie registrierte die Polizei im Jahr 2023 insgesamt 1.126 Fälle.



Die Grafik auf der folgenden Seite zeigt auf, dass auch die Aufklärungsquoten in dem Deliktsfeld im Jahr 2023 erneut angestiegen sind. Das liegt u.a. an der hohen Anzahl von sog. NCMEC-Hinweisen (vgl. 3.2.2), die oftmals konkrete Informationen (Personalien) zu Tatverdächtigen beinhalten.





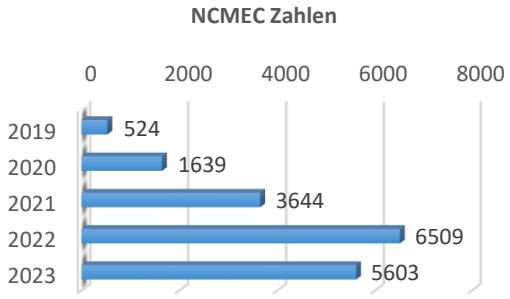
3.2.2 NCMEC-Verfahren

Zum Austausch strafbarer Inhalte werden verschiedenste Messenger-Dienste und Chatforen wie z. B. WhatsApp, Snapchat und Instagram genutzt. In vielen Fällen handelt es sich um Plattformen, deren Provider in den USA ansässig sind.

Werden in Deutschland kinder- oder jugendpornografische Inhalte ins Internet hochgeladen und von automatisierten Systemen der verschiedenen Provider als solche erkannt, leiten diese Systeme entsprechende Schritte ein. Die amerikanischen Provider sind gesetzlich dazu verpflichtet, strafrechtliche Verstöße an die halbstaatliche Organisation *„National Center for Missing and Exploited Children“* (NCMEC) zu melden. Der Zugang zur Plattform wird in der Regel gesperrt, der strafbare Inhalt isoliert und die IP-Adresse gespeichert. Die Hinweise werden durch das NCMEC in Form sog. CyberTipline-Reports über das BKA an das zuständige LKA weitergeleitet. Im LKA NI werden diese Reporte bearbeitet und als Ermittlungsakte an die zuständige Zentralstelle der Staatsanwaltschaft Hannover zur Bekämpfung gewaltdarstellender, pornografischer oder sonst jugendgefährdender Schriften weitergeleitet. Von dort aus gelangen die Akten an die örtlich zuständigen Dienststellen.

Die Tatsache, dass die NCMEC-Verfahren derzeit einen Großteil der polizeilichen Ermittlungen ausmachen, bei denen die angelieferten Daten konkrete Ermittlungsansätze liefern, begünstigt die hohe Aufklärungsquote in diesem Deliktsbereich.

Im Jahr 2023 wurden durch das BKA insgesamt 5.603 Vorgänge an das LKA NI übersandt.



Das bedeutet einen Rückgang zum Vorjahr um 13,91 %. Die Prognose des BKA für das Jahr 2023 hatte einen Anstieg der Fälle vorausgesagt. Die tatsächlich eingegangenen Fallzahlen beim BKA übertrafen diese Prognose sogar. Niedriger als erwartet fiel dahingegen die strafrechtliche Relevanz der Meldungen aus, welche sich im Durchschnitt auf ca. 50 % belief und damit die rückläufigen Zahlen erklärt.

In vielen Fällen handelt es sich bei dem von NCMEC übermittelten Beweismaterial um einzelne Fotos/Videos, die insbesondere durch Jugendliche oder Kinder unbedacht versendet werden. Hierbei gibt es eine Anzahl von sog. „Selbstfilmern“, Kinder und Jugendliche, die aus eigener Motivation Bilder und Videos von sich erstellen und verbreiten. Gleichwohl ist jedes Versenden / Herstellen eines kinder- oder jugendpornografischen Inhalts eine Straftat. Die Ermittlungen ziehen weitreichende Folgen nach sich, wie unter anderem Durchsuchungsmaßnahmen und die Sicherstellung/Beschlagnahme von persönlichen Gegenständen.

Am 25.08.2023 trat der Digital Services Act (DSA) der Europäischen Union in Kraft. Für

Hostingdienstanbieter[5] der EU besteht gem. Art. 18 DSA seither eine Meldepflicht gegenüber den Strafverfolgungs- und/oder Justizbehörden für Inhalte, „die einer Gefahr für Leib oder Leben oder die Sicherheit einer Person oder von Personen" darstellen. Dies beinhaltet u.a. Hasskriminalität und Sexualdelikte zum Nachteil von Kindern und Jugendlichen.

Eine zu verzeichnende Steigerung der Fallzahlen in Folge des DSA ist bisher nicht eingetreten, da europäische Hostingdienstanbieter dieser Verpflichtung noch nicht konsequent nachkommen.

3.3 Phänomene

3.3.1 Inhalte mit fehlgeleitetem Humor

Im ersten Quartal des Jahres 2023 erschien ein neues Phänomen. Dabei handelt es sich um Ermittlungsverfahren, die ein bestimmtes Meme[6] zum Gegenstand haben. Das Bild wurde in erster Konsequenz als kinderpornografisch bewertet. Gleichwohl wurde es in der Regel nicht durch klassisch pädosexuelle Täterinnen und Täter verschickt, sondern eher im Kontext eines fehlgeleiteten Sinns für Humor versandt. Besonders in der Altersklasse der Jugendlichen und jungen Erwachsenen entwickelte sich ein Trend, dieses Bild zu verschicken, um die Empfängeraccounts durch Provider wie Meta sperren zu lassen.

Dieses Phänomen führte zu einem massiven Anstieg der Meldungen.

3.3.2 Sextortion

Bei dem Begriff handelt es sich um eine Verfremdung des englischen Wortes Extortion (=Erpressung). Vor allem Kinder und Jugendliche werden zuerst durch Täuschung dazu animiert, von sich selbst Nacktbild- oder Videodateien zu übermitteln. In der Folge werden diese Bild-/Videodateien als Druckmittel für Geldforderungen genutzt.

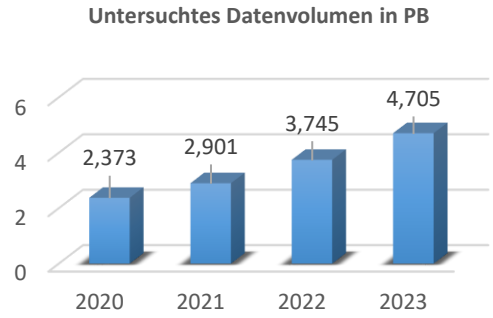
Sextortion entwickelte eine gewisse Brisanz, als es im Januar 2023 in diesem Zusammenhang in Aschaffenburg zu einem Suizid-Versuch eines 17-jährigen Opfers kam.

Um derartige Vorkommnisse in der Zukunft zu verhindern, werden in solchen Fällen, die über den Vorgangseingang der NCMEC-Mitteilungen eingehen, unverzüglich Opferschutzmaßnahmen veranlasst.

Das können Sie tun:

3.4 Sichergestellte Datenmengen

Im Jahr 2023 wurden durch die Fachkommissariate Forensik in Niedersachsen ca. 8,46 Petabyte (PB) an Gesamtdatenvolumen ausgewertet. Davon bezogen sich 4,7 PB Daten auf die Ermittlungsverfahren im Bereich Kinder- und Jugendpornografie. Im Jahresvergleich ist es erneut zu einer deutlichen Steigerung des auszuwertenden Datenbestandes gekommen.[7]



Die Größenordnung PB wird im Alltag bei der Wiedergabe der Leistungsfähigkeit von Großrechnern und Service-Zentren genutzt. Zum Vergleich: 1 PB entspricht 1.073.741.824 MB.

Anschaulicher sind diese bildlichen Vergleiche:

- 1 MB entspricht etwa einem Buch mit 400 Seiten
- 1 PB entspricht etwa 500 Milliarden voll beschriebener Textseiten

Die Gesamtanzahl der untersuchten Asservate beläuft sich im Jahr 2023 auf 34.218, davon 13.118 Datenträger aus dem Bereich Kinderpornografie. Im Jahr 2022 war die Zahl der Asservate nahezu gleich (33.382 gesamt), jedoch die Anzahl der Kinderpornografie-Datenträger (11.306) geringer.

[5] Betraf zu diesem Zeitpunkt Hostinganbieter, die mehr als 45 Millionen aktiv nutzende Personen pro Monat aufweisen.

[6] Inhalt humorvoller oder sarkastischer Natur

[7] Aufgrund eines Datenbankproblems liegen in der IT-Forensik einer Polizeiinspektion für 2023 keine statistischen Daten vor. Das Datenvolumen müsste daher geringfügig höher sein.

3.5 Herausragende Ermittlungsverfahren

3.5.1 Verbreitung von Kinderpornografie und Massendaten

Durch eine NCMEC-Mitteilung wurde im Bereich der Polizeidirektion Osnabrück bekannt, dass ein Snapchat-Nutzer verdächtig ist, kinderpornografische Inhalte hochgeladen zu haben. Weitere Ermittlungen erhärteten den Verdacht gegen den Beschuldigten. Durch das Amtsgericht Hannover wurde ein Durchsuchungsbeschluss erlassen.

Da der Beschuldigte bereits wegen sexuellen Missbrauchs seiner zwei Töchter im August 2021 zu einer Freiheitsstrafe auf Bewährung verurteilt wurde, erfolgte die zeitnahe Umsetzung des Durchsuchungsbeschlusses Ende Juli 2023. Es wurden mehr als 50 Datenträger sichergestellt und priorisiert durch die Sachbearbeitung ausgewertet.

Die Auswertung der Datenträger ergab:

254.268	Kinderpornografie-Dateien
8.881	Jugendpornografie-Dateien
17.181	Präferenz-Dateien[8]
36.790	Pornografische Dateien

Zudem stellte sich heraus, dass der Beschuldigte über Snapchat Kontakt zu minderjährigen Personen suchte und in fünf Fällen von diesen entsprechenden Dateien übermittelt bekommen hat. Im Rahmen der Auswertung können Hinweise auf weitere Taten des schweren sexuellen Missbrauchs zum Nachteil seiner Töchter in den Jahren 2015-2018 erlangt werden. Es erfolgten entsprechende Vernehmungen der Opfer, die dies belegten.

Das Gerichtsverfahren ist für August 2024 terminiert.

3.5.2 Gemeinsamer Aktionstag Kinderpornografie

Am 14.06.2023 beteiligten sich die Bundesländer Niedersachsen, Bremen, Hamburg, Schleswig-Holstein, Mecklenburg-Vorpommern, Berlin und Brandenburg am gemeinsamen Aktionstag. Koordiniert wurde dieser Tag durch das LKA NI. Die einzelnen LKÄ organisierten die Durchführung im jeweiligen Bundesland eigenständig. Ca. 300 Einsatzkräfte aller niedersächsischen Polizeidirektionen setzten in Niedersachsen über 280 Durchsuchungsbeschlüsse um. Es konnten diverse Datenträger wie Laptops, PCs und Smartphones sichergestellt werden.

Eine gemeinsame Presseerklärung hatte u. a. zum Ziel, die Bevölkerung hinsichtlich einer unbedachten Weiterleitung inkriminierter Dateien zu sensibilisieren.

3.5.3 BKA-Öffentlichkeitsfahndung

Das Bundeskriminalamt veröffentlich auf seiner Homepage Öffentlichkeitsfahndungen und bittet damit die Bevölkerung um Unterstützung.
Öffentlichkeitsfahndungen für den Bereich Kinder- und Jugendpornografie, wie auch andere Deliktsbereiche finden Sie hier:

3.6 Informationen zur Prävention

Im Bereich Cybercrime haben wir Ihnen unter Punkt 2.6.1 bereits die Seite

WWW.POLIZEI-BERATUNG.DE

als Informationsquelle für Sicherheitstipps vorgestellt. Hier finden Sie auch Informationen zu den Bereichen Kinder- und Jugendpornografie.

SOUNDSWRONG ist eine Kampagne des Programms Polizeiliche Kriminalprävention (ProPK), die sich mit verschiedenen Videoclips gegen die Verbreitung von Kinderpornografie einsetzt.
Das Ziel besteht darin, Kinder/Jugendliche, Eltern, als auch Fachleute zu sensibilisieren und über die Handlungsmöglichkeiten aufzuklären.

[8] Darstellungen von Kindern und Jugendlichen, bei denen die Kriterien „Kinderpornografie“ und „Jugendpornografie“ nicht zutreffen, die aber aufgrund kriminalistischer Erfahrung eine deliktspezifische sexuelle Neigung indizieren (z.B. Model- und FKK-Bilder von Kindern).

4 Blick in die Zukunft

4.1 Cybercrime

4.1.1 Beweismittelcloud

Digitale Beweismittel durchziehen mittlerweile nahezu sämtliche Deliktsbereiche in unterschiedlicher Qualität und Quantität. Insbesondere in den Phänomenbereichen der Kinder- und Jugendpornografie, der Organisierten Kriminalität und der Wirtschafts- und Internetkriminalität fallen regelmäßig sehr große Datenmengen mit erheblicher Beweisbedeutung an. Es ist mit großer Sicherheit davon auszugehen, dass die auszuwertenden Datenmengen aufgrund der immer weiter fortschreitenden Digitalisierung sämtlicher Lebens- und Kriminalitätsbereiche in Zukunft deliktsfeldübergreifend noch schneller anwachsen werden. Um den Erfordernissen der Digitalisierung Rechnung zu tragen und polizeilich handlungsfähig zu bleiben, sollen digitale Beweismittel zukünftig in einer Cloud-Struktur vorgehalten werden, um dort für den gesamten Gang des Strafverfahrens sicher aufbewahrt zu werden, für Analysezwecke ortsunabhängig zur Verfügung zu stehen und für Polizei und Justiz verfügbar zu bleiben.

4.1.2 Künstliche Intelligenz und Cybercrime

Seit einer Mitteilung in der Washington Post im März 2023[9] (Täter nutzten angeblich KI für Betrug, um sich am Telefon als Familie auszugeben) sind auch im LKA NI im Bereich der Prävention vermehrt Presseanfragen zur Verwendung von KI bzw. Deepfakes eingegangen.

Insbesondere wurde die Frage gestellt, ob und wie Täter diese Möglichkeiten nutzen können und dieses bereits umsetzen. In diesem Bereich ist eine rasante Weiterentwicklung von KI-Tools sichtbar, die von den Tätern für gewisse Betrugsdelikte grundsätzlich verwendet werden könnte. Denkbar sind hier aufwendig vorbereitete und lohnenswerte Delikte wie CEO-Fraud[10], Romance-Scamming[11], Fakeshops[12], Support-Scam[13] oder vorgetäuschte Entführungen.

Der typische Enkeltrick oder Anruf von falschen Polizeibeamten kommt in Niedersachsen derzeit, trotz diverser anderslautender Medienberichte, ohne KI aus. Die geschulten Täter können die potentiellen Opfer auch ohne geklonte Stimmmuster von Familienangehörigen von einer aktuell bestehenden Gefahr überzeugen und zur Herausgabe von Bargeld und anderen Wertgegenständen bringen.

Hier sind bislang keine Fälle bekannt geworden, bei denen der Einsatz einer KI nachgewiesen werden konnte.

4.2 Kinder- / Jugendpornografie

4.2.1 KI-Einsatz im Bereich der Datenaufbereitung

Die Auswertung dieser beständig wachsenden Datenmengen stellt die Strafverfolgungsbehörden bei der Aufklärung der Straftaten vor eine große Herausforderung. Die forensische Datensicherung und Datenaufbereitung sowie die kriminalistische Datenauswertung in Ermittlungsverfahren wegen des sexuellen Missbrauchs von Kindern und Jugendlichen sowie der Verbreitung, des Erwerbs und Besitzes kinder- und jugendpornografischer Inhalte dauern häufig mehrere Wochen bis Monate. Eine umfassende und detaillierte manuelle Auswertung der Daten jedes einzelnen Ermittlungsverfahrens, insbesondere zur schnellen Detektion andauernder sexueller Missbrauchshandlungen, wird durch die immensen Datenmengen zunehmend erschwert. Ein zunehmender Einsatz technischer Verfahren, darunter die Nutzung sog. Künstlicher Intelligenz (KI) kann ein wichtiger Baustein sein, um die Aus- und Bewertung von Bildmaterial effizienter zu gestalten. Im LKA NI wurde eine KI-Software mittels Methoden sogenannter neuronaler Netze entwickelt und wird stetig weiterentwickelt.

Vom LKA NI wurde eine KI-Software zur „Pornographie-(Szenen-)Erkennung“ entwickelt. Die Software besteht aus zwei Programmen, dem KiPo-Analyzer und dem Tracebook KiPo. Der KiPo-Analyzer wird zur Untersuchung von Bild- und Videodateien auf pornografischen Inhalt eingesetzt und ermöglicht eine automatisierte Separierung von bisher unbekanntem Material in Daten mit „wahrscheinlich pornographischem“ und solche mit „wahrscheinlich nicht pornographischem“

[9] https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/

[10] Betrüger fordert als angeblicher Firmenchef Mitarbeitende auf, Überweisungen zu tätigen oder Informationen mitzuteilen.

[11] Betrüger täuscht Liebesbeziehung vor, um Geld zu erbeuten.

[12] Angebliche Onlineshops, die keine Ware versenden, sondern stattdessen Daten/Gelder betrügerisch erlangen.

[13] Auf einem Heimgerät wird ein Cyber-Angriff vorgetäuscht, welcher vom angeblichen Support gegen Zahlung „behoben“ wird.

Inhalt. Das Programm Tracebook KiPo dient im Nachgang zur Sichtung sowie Aus- und Bewertung der durch den KiPo-Analyzer erzeugten Resultate.

Anfang 2024 wurde eine mehrjährige landesweite Testphase des Kipo-Analyzers sowie von Tracebook Kipo beendet und der Einsatz der Softwareanwendungen in den Regelbetrieb überführt.

Die Mitarbeitenden der Fachkommissariate müssen nun nicht mehr in jedem Fall sämtliche Inhalte manuell auswerten. Dies wird zur Beschleunigung entsprechender Ermittlungsverfahren sowie dem frühzeitigen Erkennen andauernder sexueller Missbrauchshandlungen beitragen. Dadurch werden Täterinnen und Täter noch schneller zu ermitteln sein, zudem wird die Arbeitsbelastung der mit der Auswertung oder Inaugenscheinnahme von kinder- und jugendpornographischen Dokumenten, Dateien oder Medien befassten Mitarbeiterinnen und Mitarbeitern reduziert.

Die Softwareanwendungen dienen ausschließlich als Assistenzsysteme, um die polizeiliche Sachbearbeitung bei der Bewältigung ihrer Aufgaben zu unterstützen. Die finale Auswertung, Analyse, Beurteilung sowie Entscheidung bezüglich der Ergebnisse obliegt ausschließlich der polizeilichen Sachbearbeitung bzw. der zuständigen Staatsanwaltschaft.

4.2.2 Anpassung des Strafrahmens

Im Frühjahr 2021 wurde eine Strafrechtsverschärfung des §184b StGB[14] „Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte“ verabschiedet. Durch die Anhebung des Strafrahmens zum Verbrechenstatbestand wurde es nahezu unmöglich, Verfahren aufgrund von Geringfügigkeit oder gegen Auflagen einzustellen. Dies hatte gravierende Auswirkungen auf die Ermittlungen im Bereich Kinderpornografie. Der Tatbestand eines Verbrechens lässt kaum Ausnahmen zu – somit machen sich z.B. auch Jugendliche eines Verbrechens strafbar, die unbedacht einen inkriminierten Inhalt weiterleiten (siehe Punkt 3.2.2). Ein solcher Fall liegt auch vor, wenn Elternteile inkriminierte Dateien bei ihren Kindern festgestellt und diese an eine zweite Instanz weitergeleitet haben, um über den Missstand zu informieren. Über ein Beispiel eines solchen Sachverhalts, bei dem eine Lehrerin angeklagt wurde, informierten bereits öffentliche Medien.[15]

Umso mehr werden Durchsuchungsbeschlüsse umgesetzt, die zur Folge haben, dass ein massenhaftes Datenvolumen der sichergestellten Datenträger ausgewertet werden muss (siehe Punkt 3.4).

Der Bundestag hat am 16. Mai 2024 beschlossen, dass die Mindeststrafen für Verbreitung, Erwerb und Besitz kinderpornografischer Inhalte erneut angepasst werden.[16] Besitz und Erwerb werden künftig mit einer Mindestfreiheitsstrafe von drei Monaten , die Verbreitung mit einer Mindestfreiheitsstrafe von sechs Monaten bestraft. Durch die Absenkung der Mindestfreiheitsstrafe ist es nun wieder möglich, Verfahren mit einem minderschweren Unrechtsgehalt nach §153 und 154 StPO einzustellen oder nach §407 ff. StPO durch einen Strafbefehl zu erledigen.

Die Anpassung des Strafrahmens hat primär zum Ziel, Menschen vor Strafverfolgung zu schützen, die zur Aufklärung der Taten beitragen wollen. Zusätzlich dürfte die erneute Anpassung einen positiven Effekt bei der Bewältigung des anfallenden Datenvolumens bewirken.

[14] Anhebung des Strafrahmens zum Verbrechen. Das bedeutet eine Mindestfreiheitsstrafe von einem Jahr Freiheitsstrafe.

[15] www.swr.de/swraktuell/rheinland-pfalz/koblenz/lehrerin-kinderpornografischer-inhalte-konfisziert-deswegen-angeklagt-100.html

[16] https://www.tagesschau.de/inland/bundestag-gewalt-kinder-mindeststrafe-100.html