Polizeipräsidium
Land Brandenburg

Landeskriminalamt

Lagebild
Cybercrime
im Land Brandenburg
Jahr 2022

Impressum

Polizeipräsidium
Landeskriminalamt
Cyber-Competence-Center
LKA 121
Tramper Chaussee 1
16225 Eberswalde
Tel. 03334 388 8620

cybercrime.lka@polizei.brandenburg.de

Trend

	2021	2022		Veränderung
Cybercrime	**2.678**	**2.640**	↘	**-1,4 %**
Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei	63	65	↗	+3,2 %
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung	99	96	↘	-3,0 %
Datenveränderung, Computersabotage	69	78	↗	+13,0 %
Computerbetrug	2.447	2.401	↘	-1,9 %
- Betrügerisches Erlangen von Kfz	2	2	=	0,0 %
- Weitere Arten des Warenkreditbetruges	1.182	1.209	↗	+2,3 %
- Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	542	540	↘	-0,4 %
- Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	118	86	↘	-27,1 %
- Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel	229	170	↘	-25,8 %
- Leistungskreditbetrug	101	107	↗	+5,9 %
- Computerbetrug (sonstiger)	194	175	↘	-9,8 %
- Missbräuchliche Nutzung von Telekommunikationsdiensten	10	18	↗	+80,0 %
- Abrechnungsbetrug im Gesundheitswesen	0	0	=	0
- Überweisungsbetrug	69	94	↗	+36,2 %
Delikte mit Tatmittel Internet und/oder IT-Geräte (insg.)	**8.528**	**8.350**	↘	**-2,1 %**

Inhaltsverzeichnis

1. Vorbemerkung

Das Landeslagebild informiert über Entwicklungen und aktuelle Phänomene im Bereich Cybercrime. Erfasst sind dabei die Straftaten, die sich gegen das Internet, weitere Datennetze (z. B. Intranet, Mobilfunknetze), informationstechnische Systeme (z. B. USB-Sticks, Stand-Alone-PC, Server, Cloud usw.) oder deren Daten richten sowie auch die Straftaten, die mittels dieser Informationstechnik begangen werden[1].

Die Grundlage für das Lagebild bilden die Fallzahlen der Polizeilichen Kriminalstatistik (PKS).

Am 26.08.2020 beschloss die AG Kripo u. a., dass zum 01.01.2021 der **PKS-Summenschlüssel „Computerkriminalität" (897000)** in „Cybercrime" umbenannt wird und zur Beschreibung der Kriminalitätsbelastung im Phänomenbereich „Cybercrime" zu verwenden ist. Dieser Summenschlüssel wurde darüber hinaus wie folgt angepasst und besteht nunmehr aus den Delikten:

- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB
- Datenveränderung, Computersabotage §§ 303a, 303b StGB
- Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB sowie
- dem Computerbetrug § 263a StGB.

Weiter existiert ein gleichnamiger **PKS-Summenschlüssel 897100 „Computerbetrug"**. Dieser setzt sich wie folgt zusammen:

- Betrügerisches Erlangen von Kfz
- Weitere Arten des Warenkreditbetruges
- Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN
- Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten
- Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel
- Leistungsbetrug
- Computerbetrug (sonstiger)
- Missbräuchliche Nutzung von Telekommunikationsdiensten
- Abrechnungsbetrug im Gesundheitswesen
- Überweisungsbetrug.

Außerdem beschloss die AG Kripo, dass lediglich noch ein Sonderkenner „Tatmittel Internet" zu verwenden ist. Dieser wird umbenannt in „Tatmittel Internet und/oder IT-Geräte". Alle weiteren dem Phänomenbereich „Cybercrime" zugeordneten Sonderkenner (Cybercrime, Cybercrime im engeren Sinne, Cybercrime - Tatmittel, Tatmittel weitere Datennetze sowie Tatmittel sonstige IT-Systeme) wurden abgeschafft: Die Erfassung dieser Delikte erfolgt seit dem 01.01.2021 unter dem einzigen Sonderkenner „Tatmittel Internet und/oder IT-Geräte". Auf Grund der Veränderung/Erweiterung der Sonderkenners

[1] 171. Tagung der AG Kripo am 12./13.09.2012 in Wörlitz/ST - TOP 2.3 Definition „Cybercrime"

„Tatmittel Internet“ (vor 2021) und nun „Tatmittel Internet und/oder IT-Geräte“ ist eine Vergleichbarkeit mit den Vorjahren nur eingeschränkt möglich.

Darüber hinaus handelt es sich beim Sonderkenner „Tatmittel Internet und/oder IT-Geräte“ nicht um eine Qualifizierung bezüglich besonderer Fähig- und Fertigkeiten des Tatverdächtigen oder der Tatbegehungsweise. Entscheidend ist lediglich, ob das Internet als „Tatmittel und/oder IT-Geräte“ verwendet wurden.
Unter den Zusatz „IT-Geräte“ fallen alle Netze, die nicht Teil des Internets sind, z. B. Intranet, Mobilfunknetz, Bluetooth, etc. und sonstige informationstechnische Systeme. Bei diesen sonstigen informationstechnischen Systemen handelt es sich um ein in sich geschlossenes, keinem Netzwerk angehöriges IT-Gerät, wie z.B. ein Stand-Alone-PC, USB-Stick, Speicherkarte etc.

Erfasst werden grundsätzlich alle Delikte, zu deren Tatbestandsverwirklichung das Medium Internet und/oder IT-Geräte als Tatmittel verwendet werden. Dabei kommen sowohl Straftaten in Betracht, bei denen das Einstellen von Informationen in das Internet/andere Netze bereits Tatbestände erfüllt als auch solche Straftaten, bei denen das Internet und/oder IT-Geräte als Kommunikationsmedium bei der Tatbestandsverwirklichung verwendet werden.

Seit 2013 werden zur Verbesserung der Darstellungsbreite und -tiefe des Phänomens Cybercrime auch die Straftaten statistisch erfasst, bei denen die jeweiligen Orte der Tathandlungen im Ausland liegen bzw. unbekannt sind oder die Tathandlungen unter Nutzung im Ausland befindlicher Server begangen wurden und der Erfolg der Handlung (Erfolgseintritt) in Deutschland eingetreten ist. Eine Summierung von Inlands- und Auslandstaten ist aktuell nicht zulässig.

In Anbetracht der Tatsache, dass eine Vielzahl von Cybercrime-Straftaten nicht aufgehellt werden können und somit polizeilich nicht bekannt werden, sind bei der Erstellung des Lagebildes auch Erkenntnisse aus nichtpolizeilichen Informationsquellen (z. B. des Bundesamtes für Sicherheit in der Informationstechnik oder von Antivirensoftware-Herstellern) einbezogen worden. Maßgeblich für die phänomenologischen Aussagen des Lagebildes sind daher sowohl Erkenntnisse aus dem Sondermeldedienst Cybercrime als auch aus polizeiexternen Quellen.

2. Lagedarstellung

2.1 Polizeiliche Kriminalstatistik (PKS)

2.1.1 Cybercrime

Die Anzahl der unter Cybercrime (als Haupttat) in der PKS für das Jahr 2022 erfassten Straftaten, die sich gegen das Internet, weitere Datennetze, IT-Systeme oder deren Daten richten, ist gegenüber dem Vorjahr um 1,4 % auf 2.640 Fälle (2021: 2.678 Fälle) gefallen.

Hinsichtlich der Gesamtsumme des Computerbetruges (PKS-Summenschlüssel 897100) ergibt sich eine leichte Senkung um 1,9 % auf 2.401 Fälle von 2.447 Fällen.

Die Entwicklung der weiteren Fallzahlen der Cybercrime zuzuordnenden Deliktsgruppen stellt sich heterogen dar:

- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (- 3,0 %, - 3 Fälle),
- Datenveränderung 57 Fälle (+16,3 %, +8 Fälle),
- Computersabotage 21 Fälle (+5,0 %, +1 Fall),
- Ausspähen und Abfangen von Daten einschließlich der Vorbereitungshandlungen und Datenhehlerei 65 Fälle (+3,2 %, +2 Fälle)

Herausragende Phänomene (Mischsachverhalte Cybercrime und Internetkriminalität), wie z. B. Erscheinungsformen der digitalen Erpressung auf sexueller Grundlage oder im Zusammenhang mit Daten-Verschlüsselungsschadsoftware (Ransomware), Angriffe auf das Onlinebanking, das betrügerische Erlangen von Zahlungskartendaten oder Erscheinungsformen des Tech-Support-Scam werden in der PKS nicht vollständig unter den der Cybercrime zugeordneten Deliktsschlüsseln, sondern u. a. unter den tatsächlich verwirklichten Straftatbeständen erfasst. Insofern findet ein Großteil von Fällen, die z. B. als Betrugsdelikte statistisch abgeschlossen worden sind, hier keine Berücksichtigung und sind in den Fallzahlen zum Tatmittel Internet enthalten.

Bei den durch Cybercrime registrierten Schäden ist im Jahr 2022 ein Rückgang um 7,4 % auf 2.386.503 EUR zu verzeichnen (2021: 2.578.011 EUR). Die Schadenssumme entspricht jedoch ausschließlich den kumulierten Schadenssummen des PKS-Summenschlüssels Computerbetrug (897100). Es gilt zu beachten, dass es sich hierbei lediglich um in der PKS registrierte Schadenssummen für die genannten Cybercrimedelikte handelt, die zum Teil durch die bearbeitenden Polizeibeamten geschätzt werden und Schäden wie Verdienstausfälle etc. nicht vollständig abbilden. Die größten Schadenssummen ergeben sich aus der Schädigung mittels „Ransomware“, welche bereits als Fallzahlen nicht vollständig im Bereich Cybercrime/PKS subsumiert werden, sondern innerhalb der PKS im Regelfall als Erpressungen zu werten ist. Daher sind „Ransomware-Fälle“ auch in vielen Fällen nicht in der genannten Gesamtschadensumme enthalten (vgl. Sonderauswertung Ransomware in diesem Lagebild).

Die Zahl der bei den erfassten Fällen von Cybercrime ermittelten Tatverdächtigen (TV) fiel auf 1.097 TV (2021: 1.151 TV). Personen über 21 Jahre stellen mit einem Anteil von 88,7 % bzw. 973 TV weiterhin

die anteilig größte Gruppe unter den TV dar (2021: 88,8 %, 1.022 TV). Der Anteil nichtdeutscher Tatverdächtiger beträgt 13,4 % bzw. insgesamt 147 Tatverdächtige (Vorjahr 12,0 bzw. 120 TV).

Im Phänomenbereich Cybercrime wurden im Berichtsjahr 8.128 Auslandsstraftaten registriert (2021: 6.933Fälle) Die entspricht einem Anstieg um 1.195 Fälle (+17,2 %). Somit haben im Berichtszeitraum etwa 75,5 % der hierzulande polizeilich bekannt gewordenen Fälle Cybercrime ihren, soweit nachvollziehbaren Ursprung im Ausland (2021: 44,2 %). Die Nachvollziehbarkeit richtet sich u. a. nach im Verfahren festgestellten IP-Adressen der Täterseite mit nachvollziehbarem Ursprung im Ausland.

2.1.2 Tatmittel Internet und/oder IT-Geräte

Fälle, die mit dem Tatmittel Internet und/oder IT-Geräte subsumiert werden, setzen immer das Erfassen eines entsprechenden Sonderkenners im POLAS-Beleg-Straftat innerhalb des Vorgangsbearbeitungssystems durch den jeweiligen kriminalpolizeilichen Sachbearbeiter voraus. Unterbleibt das individuelle Setzen des Kenners, werden Fälle nicht in dieser Rubrik erfasst, obwohl sie phänomenologisch hier zuzuordnen wären. Ständige Kommunikation zum Umgang- und der korrekten Erfassung von Fällen mit dem Tatmittel soll die Differenzen schrittweise verringern.

Im Jahr 2022 wurden in der PKS insgesamt 8.350 Fälle erfasst, die unter der Nutzung des Tatmittels Internet und/oder IT-Geräte begangen wurden (2021: 8.528 Fälle. Dies entspricht einem Rückgang um 178 Fälle (-2,1%). Überwiegend handelte es sich dabei um 3.314 Fälle des Waren-/ Warenkreditbetruges (2021: 2.929 Fälle; Rückgang um -385 Fälle bzw. -10,4 %) sowie um 1.652 Fälle des Computerbetruges (2021: 1.597 Fälle, Rückgang um -55 Fälle bzw. -3,2 %).

Die vorgenannten Zahlen des Computerbetruges stellen wie eingangs festgestellt, lediglich diejenigen Fälle dar, welche von den kriminalpolizeilichen Sachbearbeitern auch mit dem entsprechenden Sonderkenner versehen wurden. Die Gesamtzahl der Fälle des Computerbetrugs betragen wie zu Beginn benannt 2.401 Fälle.

Die polizeilich erfasste Gesamtschadenssumme (Schaden gemäß PKS) betrug 5.355.108 EUR (2021: 4.813.940 EUR; +10,1 %).

Im Berichtszeitraum wurden zu den Straftaten mit dem Tatmittel Internet und/oder IT-Geräte 5.614 TV ermittelt (2021: 5.574; +40 TV). Der Anstieg ist marginal. Unabhängig davon ist ein Rückgang bei den Erwachsenen auf 4.219 TV (2021: 4.255 TV) und Heranwachsenden auf 490 TV (2021: 528 TV) zu verzeichnen. Die Anzahl der tatverdächtigen Kinder und Jugendliche hingegen stieg auf 317 TV (2021: 236 TV) bzw. 588 TV (2021: 555 TV) an.
Insgesamt bilden die Erwachsenen mit 75,2 % (4.219 TV) weiterhin die anteilig größte Gruppe unter den Tatverdächtigen.

Zu den Straftaten mit dem Tatmittel Internet und/oder IT-Geräte wurden im Jahr 2022 insgesamt 484 nichtdeutsche TV erfasst (2021: 475 TV). Den 484 TV konnten Staatsangehörigkeiten aus insgesamt 68 Staaten zugeordnet werden. Die meisten der nichtdeutschen TV stammen aus Syrien (65 TV), Polen (61 TV), der Russischen Föderation (34 TV), Türkei (28 TV), Afghanistan (27 TV) und Kamerun (20 TV).

In der Kategorie „Auslandsstraftaten“ wurden bei den Straftaten mit dem Tatmittel Internet und/oder IT-Geräte im Berichtsjahr 16.701 Fälle registriert (2021: 14.009 Fälle; + 2.692 Fälle bzw. +19,2 %). Insgesamt entspricht dies einem Anteil von 66,7 % (2021: 62,2 %) der polizeilich registrierten Straftaten mit dem Tatmittel Internet und/oder IT-Geräte, die durch Tathandlungen aus dem Ausland heraus begangen worden sind.

2.2 Aktuelle Begehungsweisen und Phänomene

2.2.1 Diebstahl digitaler Identitäten und Identitätsmissbrauch

Die digitale Identität[2] einer Person besteht in der Regel aus Identifikations- und Authentisierungsdaten, wie etwa der Kombination von Benutzername und Passwort, Bank- oder Kreditkarteninformationen oder E-Mail-Adressen. Das Verschaffen des unberechtigten Zugangs zu derartigen Daten, der Identitätsdiebstahl, findet vor allem mittels Social Engineering, Schadprogrammen auf infizierten Endsystemen (z. B. Einsatz von Keyloggern[3] und Spyware[4]) oder durch Datenabfluss nach dem Angriff auf Online-Plattformen oder auf Servern statt. Der Identitätsdiebstahl stellt regelmäßig die vorbereitende Einstiegshandlung für die Begehung weiterer Straftaten der Cybercrime und anderer Delikte dar (z. B. betrügerische Warenbestellungen, Missbrauch von Kreditkartendaten, Versendung von Schadsoftware, DDoS – Attacken zum Nachteil von Unternehmen und Einrichtungen).

Ferner werden die erlangten Daten über illegale „Marktplätze“ der Underground Economy mit monetärem Gewinn veräußert. Neu in Erscheinung getreten sind zudem Plattformen, auf denen Daten auch frei erhältlich sind, wie z. B. die mittlerweile durch die Sicherheitsbehörden gesperrte Seite *www.We-leak.info.*

Warenkreditbetrugshandlungen nach vorherigem Ausspähen von Zugangskennungen, insbesondere zu E-Mail-Diensten und Onlinehändlern bzw. komplettem „Identitätsdiebstahl“ (mit Neuanlage von Accounts bei Verkaufs- und Finanzdienstleistungsplattformen im Namen Dritter) werden weiterhin auf hohem Niveau festgestellt. Hierunter fällt auch der Einsatz sog. Phishing-E-Mails zum Ausspähen, Verändern und Sperren privater Zugangsaccounts, u. a. bei E-Mail-Diensten, Online-Shops, Internet-Zahlungsdienstleistern sowie in sozialen Netzwerken.

Gerade in Bezug auf einen Finanzdienstleister ist festzustellen, dass die Täter regelmäßig Ausweisdokumente Dritter missbräuchlich nutzen, um ihre eigene Identität zu verschleiern (zum Teil Dokumente von Geschädigten aus anderen Betrugsstraftaten). Es konnte festgestellt werden, dass die Täter stets

[2] Die digitale Identität ist die Summe aller Möglichkeiten und Rechte des einzelnen Nutzers sowie seiner Aktivitäten innerhalb der Gesamtstruktur des Internets. Konkret handelt es sich um sämtliche Arten von Nutzerdaten, also z. B. Zugangsdaten in den Bereichen Kommunikation, E-Commerce, berufsspezifische Informationen, E-Government, Cloud-Computing sowie auch alle anderen zahlungsrelevanten Informationen.

[3] Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern, filtern. (Quelle: www.bsi.bund.de, Glossar)

[4] Als Spyware werden Programme bezeichnet, die heimlich Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. (Quelle: www.bsi.bund.de, Glossar)

professioneller vorgehen, um ihre Identität zu verbergen. Hierfür wurden IP-Adressen verschleiert, erhaltene Gelder mehrmals an weitere Accounts dieses Finanzdienstleisters mit unterschiedlichsten Aliaspersonalien weitertransferiert bzw. Einkäufe bei Unternehmen getätigt, bei denen Auskunftsersuchen der Polizei nicht beantwortet werden (insbesondere Firmen aus dem Ausland) oder eine Auskunft nicht zum Täter führt (Bsp.: Gutscheine, Guthabenkarten). Oftmals werden hierbei längere Zeit nicht genutzte Accounts von Verkaufs- und Finanzdienstleisterplattformen genutzt, um in weiterer Folge Warenkreditbetrugstaten zu begehen.

Wie auch im Jahr 2021 wurden zunehmend Fälle registriert, bei denen sich unbekannte Täter mehrfach unberechtigt in den E-Mail-Verkehr von Firmen einloggten und bereits gestellte Rechnungen durch „neue“ Bankdaten abänderten (sog. Payment-Diversion-Fraud). Der Rechnungsbetrag sollte sodann auf das veränderte Konto überwiesen werden. Diese befanden sich in der Regel im Ausland.

Beispielfall Land Brandenburg 2022
Ein Brandenburger Unternehmen teilte mit, dass der Account einer Rechnungsserviceanwendung eines Lieferanten in China im Februar 2022 übernommen und missbraucht wurde, um falsche Zahlungsinformationen zu übermitteln und damit Zahlungen auf ein fremdes Konto umzuleiten. Damit sei auch eine Zahlung des hier anzeigenden Unternehmens i. H. v. 13.000 EUR in betrügerischer Absicht auf ein mexikanisches Konto geleitet worden. Der Fall einer Übernahme eines Accounts bei einem Rechnungslegungsservice stellt aktuell eine sehr seltene Begehungsweise dar. Bislang sind der ZAC Brandenburg lediglich Fälle bekannt geworden, in denen E-Mail-Accounts durch die Täter übernommen wurden bzw. die Rechnungen mit veränderten Kontodaten auf anderem Wege an die Geschädigten gelangt sind.

Beispielfall Land Brandenburg 2022
Der Geschäftsführer eines Klinikbetriebes in Brandenburg teilte der ZAC Brandenburg mit, dass die Buchhaltung Rechnungen über 336.000 EUR von einem Geschäftspartner erhalten habe und diese wie üblich beglichen habe. Hierbei gelang es den unbekannten Tätern, bisherige Rechnungen abzufangen und mit einer neuen Bankverbindung (nunmehr nach Portugal) zu versehen.

2.2.2 Angriffe auf das Online-Banking

Im Berichtszeitraum ist eine überwiegend gleichbleibende Anzahl von Angriffen auf das Online-Banking zu verzeichnen, was auf die Zunahme und bessere Ausgestaltung von Sicherungssystemen der Banken zurückzuführen sein könnte.

Am häufigsten erhielten die Geschädigten nach dem Erhalt einer E-Mail, welche den Anruf eines Kundenberaters des Geldinstitutes ankündigte, tatsächlich einen Anruf. Im Gespräch mit dem Kundenberater, der z. B. eine notwendige Sicherheitsüberprüfung suggerierte, übermittelten die Geschädigten TANs und ermöglichten somit Zugriff auf ihr Online-Banking sowie unberechtigte Überweisungen mit hohen Geldbeträgen. Die höchste Schadenssumme betrug 250.000 EUR.

Bezugnehmend auf diesen Modus Operandi wird erkennbar, dass das Vorgehen der Täter ständigem Wandel unterlegen ist und häufig nicht nachvollzogen werden kann, wie die Täter an Kontodaten und weitere sensible Daten der Geschädigten gelangt sind.

Ein neues, jedoch bisher selten aufgetretenes Phänomen ist die Erstellung virtueller EC-Karten, die durch die Täter genutzt werden. Diese Karte wird auf ein mobiles Endgerät mit NFC-Funktionalität (z. B. Smartphone) angelegt und kann wie eine physisch zum Bankkonto zugehörige EC-Karte verwendet werden. Die Täter sind damit in der Lage, Einkäufe zu bezahlen oder das Geld unmittelbar am Geldautomaten direkt vom Bankkonto des Geschädigten abzuheben.

Es wurden darüber hinaus wiederholt Fälle bearbeitet, bei denen die Zahlungsmöglichkeiten mittels Smartphone missbraucht wurden. Die Anzahl der Fälle, in denen Kryptowährungen zumeist als Auszahlungsmedium nach Fremdkontennutzung genutzt werden, hat sich nach hiesiger Einschätzung erhöht. Leider spiegeln die polizeilichen Auskunftssysteme keine valide Datenbasis in diesem Kontext wieder. Es handelt sich bei der Einschätzung lediglich um eine Wahrnehmung im Rahmen des täglichen Dienstgeschäftes und Erfahrungsaustausches im Arbeitskreis Cybercrime des Polizeipräsidiums.

2.2.3 Digitale Erpressung unter Einsatz sogenannter „Ransomware“

Die digitale Erpressung unter Einsatz sogenannter „Ransomware“[5] hat sich in Deutschland zu einer weit verbreiteten Begehungsweise entwickelt und ist für einen erheblichen Teil festgestellter Schäden bzw. Schadenssummen im Bereich von Unternehmen und Behörden verantwortlich. Entsprechende Schadsoftware bzw. die gesamte „Dienstleistung“ kann in einschlägigen Foren der Underground Economy als „Ransomware-Kits“ erworben werden. Hierdurch ist bei den Tätern kein besonderer IT-Sachverstand für die Durchführung einer digitalen Erpressung erforderlich. Die häufigsten Infizierungswege für die Verbreitung von Ransomware sind Anhänge von Spam-E-Mails (z. B. getarnt als Bewerbungen) mit Verlinkungen auf fremde Webserver oder mit präparierten Dateianhängen (Makro, Javascript) bzw. Drive-by-Angriffe mittels Exploit Kits, die Sicherheitslücken u. a. im Browser und dessen Plug-Ins ausnutzen. Auch das Ausspähen offener Ports bzw. das Überwinden von Administratorenzugängen für die Fernwartung in Unternehmensnetzwerken führten häufig zur Infektion mit Ransomware.

Insbesondere bei Unternehmen und Behörden sorgt der Befall mit Ransomware für größere Beeinträchtigungen im Dienstbetrieb. Notwendige Onlineanwendungen von Unternehmen und Behörden müssen oftmals über längere Zeit vom Netz genommen werden und es werden externe IT-Unternehmen beauftragt, den Vorfall zu bereinigen, was häufig zu einer vollständigen Systembereinigung führt. Neben den durch die Ransomware verursachten Systemschäden und dem Arbeitsausfall sind die Mehrkosten für die Beauftragung von IT-Unternehmen beachtlich. Dies führt wiederum dazu, dass insbesondere kleinere Unternehmen häufiger abwägen, inwieweit eine mögliche Lösegeldzahlung einen geringeren monetären Einfluss gegenüber dem Systemausfall und der Bereinigung hat.

In Kombination der verschiedenartigen Recherchewerkzeuge der Polizei (eFBS, POLAS, PKS) ergibt sich für das Jahr 2022 (2021) folgendes Mengengerüst an Fällen, die dem Phänomen „Ransomware“ zugeordnet werden können:

[5] „Ransomware“ sind Computerprogramme, mit deren Hilfe ein Eindringling (Trojaner) den Zugriff auf einen fremden Computer sperren kann, um für die Entsperrung ein „Lösegeld“ zu fordern. Die Bezeichnung „Ransomware“ setzt sich aus der englischen Bezeichnung für Lösegeld „Ransom“ sowie dem für Schadsoftware gebräuchlichen Wort „Malware“ zusammen.

- Vorgänge 2022 insgesamt: 31 Vorgänge (davon 26 x betroffene Unternehmen, 2 x betroffene Institution, 3 x betroffene Privatpersonen)
- Vorgänge 2021 insgesamt: 35 Vorgänge (davon 29 x betroffene Unternehmen, 1 x betroffene Institutionen, 5 x betroffene Privatpersonen)

Auf weiterhin existierende Unschärfen der Fallzahlendarstellung aufgrund nicht einheitlich umgesetzter Erfassungsregeln wird hingewiesen. Darüber hinaus wird auch hier von einem beachtlichen Dunkelfeld ausgegangen, da gerade Unternehmen nicht jeden „IT-Sicherheitsvorfall“ der Polizei melden, sondern eher darauf bedacht sind, die Arbeitsfähigkeit schnellstmöglich wiederherzustellen und eine Rufschädigung zu vermeiden.

Beispielfall Land Brandenburg 2022

Am 28.11.2022 ging bei der ZAC des LKA Brandenburg per E-Mail der Hinweis ein, dass unbekannte Täter die IT-Infrastruktur eines kommunalen Busbetriebes angegriffen hätten und große Teile des Unternehmens, u. a. der Verwaltungs- und Werkstattbereich, betroffen seien.

Nach Kontaktaufnahme mit dem Unternehmen konnte in Erfahrung gebracht werden, dass es unbekannten Dritten in der Nacht vom 25. zum 26.11.2022 gelang, sich mittels Schadsoftware Zugang zu den Servern des Unternehmens zu verschaffen und diese derart zu beeinträchtigen, dass Anmeldvorgänge für Berechtigte nicht mehr möglich waren. In den Arbeitsdruckern befanden sich anonyme Ausdrucke in englischer Sprache, in denen die mutmaßlichen Täter angeben, die IT-Systeme des Unternehmens verschlüsselt zu haben und mit der Veröffentlichung von Unternehmensdaten drohten. Bei der im Täterschreiben aufgeführten Kontaktmöglichkeit handelt es sich um eine URL aus dem sog. TOR-Netzwerk.

Für den regulären Linienbetrieb und den Busverkehr ergaben sich nach Auskunft des Unternehmens durch den IT-Ausfall keine Einschränkungen.

Beispielfall Land Brandenburg 2022

Am 16.02.2022 erstattete eine Behörde der Wasserstraßen- und Schifffahrtsverwaltung beim BSI Meldung über einen vermeintlichen IT-Sicherheitsvorfall.

Gegen 06:50 Uhr am 16.02.2022 soll von einem technischen Mitarbeiter auf Grund einer Phishing-E-Mail eine ZIP-Datei (Link: hxxxs://popular-bd[.]com/idomaeot/mi-anienqrurnsrationie-spuunorasm) heruntergeladen und entpackt worden sein. Das Archiv enthielt eine schadhafte Datei eines Tabellenverarbeitungsprogramms. Diese sei durch den Mitarbeiter geöffnet wurden und er habe die Aktivierung des Makros bestätigt.

Das BSI übernahm eine umfangreiche Analyse des Vorfalls und stellte diese den hier ermittelnden Behörden zu Verfügung nachdem die geschädigte Behörde Anzeige erstattet hatte.

Die Analyse des BSI ergab, dass das kompromittierte System zwar den Schadcode aus der Datei ausgeführt hatte, aber keine Maleware (vermutlich QakBot) nachgeladen wurde.

Beispielfall Land Brandenburg 2022

Am 23.05.2022 zeigte die Geschäftsführerin eines geschädigten Unternehmens an, dass wichtige IT-Systeme am 18.05.2022 mit einer Ransomware verschlüsselt worden seien. Zuvor sei eine E-Mail an verschiedene E-Mail-Adressen von Mitarbeitern verschickt worden, in der 26 verschiedene Verlinkungen zur Domain „ibb.co/[…)]“ enthalten sind. Die in Englisch verfassten E-Mail wurde über die Verschlüsselung informiert und eine Datenveröffentlichung bei Nichtzahlung angedroht. Weiter enthielt sie eine TOR-Verlinkung, über die das Unternehmen mit den Tätern Kontakt per Chat aufnehmen sollte. Die Verlinkungen verwiesen auf Screenshots geöffneter Dateien, wie z. B. Rechnungen. Die TOR-Webseite enthielt ebenfalls die o. g. veröffentlichten Bilder, eine Forderung in Höhe von 120.000 Euro und einen Text, in dem auf die Verschlüsselung sowie angedrohter Konsequenzen bei Nichtzahlung hingewiesen wurde. Die Domain „ibb.co“ war einem Anonymisierungsdienst zugeordnet, der erfahrungsgemäß nicht auf polizeiliche Auskunftsersuchen antwortet.

Bereits zur Anzeigenaufnahme war der Wiederherstellungsprozess eingeleitet worden. Vorab gesicherte Dateien wurden von der geschädigten Firma auf einem USB-Stick übersendet. Darauf enthalten waren u. a. verschlüsselte Dateien mit der Dateiendung „.lockbit“, eine Ransomnote sowie als Schadsoftware eingestufte Programme. Die Webseite „id-ransomware.malwarehunterteam.com“ ordnet den verschlüsselten Dateien die Ransomware Lockbit zu.

Im Zusammenhang mit der Ransomware LockBit 2.0 bzw. 3.0 führt das LKA Schleswig-Holstein zentrale Ermittlungen. Die hiesigen Erkenntnisse wurden im Rahmen des polizeilichen Informationsaustausches an diese Dienststelle übermittelt. Die dort getätigten Ermittlungen dauern weiterhin an.

2.2.4 Ausnutzen von Hardware- und Softwarelücken

Beispielfall Land Brandenburg 2022

Seit dem 28.12.2022, lagen dem LKA Brandenburg konkrete Hinweise vor, dass Verwaltungen bzw. sensible Infrastrukturen der Stadt Potsdam im Fokus von Gruppierungen stehen, die Cyberangriffe durchführen oder bereits durch Gruppierungen kompromittiert wurden. Das Einbringen bereits aktiver Backdoors (Software, die es den Tätern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zu einem System zu erhalten) von Täterseite konnte nicht ausgeschlossen werden.

Im Rahmen der ersten Ermittlungen wurde in Erfahrung gebracht, dass durch den IT-Bereich bislang keine offensichtliche Kompromittierung festgestellt wurde. Dennoch wurden zunächst interne (IT-Bereich der Stadt Potsdam sowie beim zuständigen Provider) Prüfhandlungen initiiert.

Am 29.12.2022 um 19:00 Uhr wurde durch einen Dienstleister der Stadtverwaltung Potsdam festgestellt, dass ein sogenannter „Brute-Force“-Angriff (systematisches Ausprobieren von Passwörtern) gegen eine der Stadtverwaltung zugehörigen Domäne gestartet wurde. Daraufhin entschied die Stadtverwaltung Potsdam, die eigene sowie die Internetkommunikation einiger kommunaler Töchterunternehmen bis auf Weiteres zu unterbrechen. Damit waren sämtliche externe datenbankbasierte Dienstleistungen der Stadt Potsdam nicht erreichbar. Einen Zusammenhang zwischen der „Brute-Force-Attacke“ und der Gefährdungslage wurde nicht festgestellt.

Weiter wurde am 26.01.2023 bekannt, dass im Rahmen einer durch mehrere Staaten (z. B. USA und Deutschland) koordinierten Exekutivmaßnahme, die IT-Infrastruktur einer international agierenden Hackergruppierung abgeschaltet werden konnte. Es kam dabei jedoch zu keinerlei Festnahmen. Bei dieser Hackergruppierung handelt es sich um diejenige, vor der durch den ursprünglichen Hinweis gewarnt wurde.

Mit Stand 31.01.2023 ist hier keine erfolgreiche Kompromittierung der IT-Systeme der Stadtverwaltung Potsdam und deren kommunalen Töchterunternehmen, die mit der in Rede stehenden Hacker-Gruppierung im Zusammenhang stehen, bekannt.

Beispielfall Land Brandenburg 2022

Ab dem 26.11.2022 erfolgte ein DDoS-Angriff auf die Webseite des Flughafens BER. Dabei wurde der Webseitenbereich für die Flugauskunft zielgerichtet überlastet. Dies gelang den Tätern, indem sie eine Vielzahl von manipulierten Suchanfragen sendeten, welche zu keinem plausiblen Ergebnis (bekannten Flug) führen konnten. Dadurch war von Tatbeginn bis zum 27.11.2022 die Erreichbarkeit der Flugauskunft beeinträchtigt. Auffällig viele Verbindungen für den Angriff stammten von einem VPN-Dienst. Eine Überarbeitung des Programmcodes auf der Webseite des Geschädigten führte dazu, dass der an den Folgetagen fortgesetzte Angriff nicht weiter zum Erfolg führte. Es ließen sich keine Täter ermitteln.

3. Prävention

Die polizeiliche Präventionsarbeit im Zusammenhang mit Cybercrime/Neue Medien richtet sich insbesondere an Kinder und Jugendliche mit dem Ziel, die Teilnehmer zu einer sachgerechten und umsichtigen Mediennutzung zu befähigen und so entsprechende Medienkompetenzen aufzubauen. Die Kinder und Jugendlichen sollen über potentielle Gefahren im Umgang mit dem Internet und Neuen Medien sowie zu den ordnungs- und strafrechtlichen Rahmenbedingungen (z. B. Urheberrecht) informiert sein und entsprechende Verhaltensweisen zur Vermeidung von Opferwerdung kennen. Zudem sollen sie darin unterstützt werden, sich mit den Angeboten und Möglichkeiten des Internets und der Neuen Medien kritisch und verantwortungsbewusst auseinanderzusetzen.

Die Polizeiinspektionen führten im Jahr 2022 insgesamt 568 (2021: 297) Präventionsveranstaltungen zum Thema „Cybercrime/Neue Medien“ durch, mit denen rund 12.778 (2021: 6.260) Teilnehmer erreicht wurden. Diese Themenfelder sowie die damit verbundenen Risiken und Gefahren sind zudem im Rahmen weiterer Präventionsmaßnahmen, wie z. B. innerhalb der Gewaltprävention, angesprochen worden.

Der Digital-Kompass ist ein Projekt der Bundesarbeitsgemeinschaft der Senioren-Organisationen (BAGSO) und Deutschland sicher im Netz e.V. in Partnerschaft mit der Verbraucher-Initiative mit Förderung des Bundesministeriums der Justiz und für Verbraucherschutz, welcher deutschlandweit kostenfreie Angebote für Senioren rund um das Thema „Internet“ bereitstellt. Durch diese Angebote werden mittels sogenannter Internetlotsen ältere Menschen dabei unterstützt, digitale Angebote selber auszuprobieren. In Königs Wusterhausen kümmern sich ehrenamtlich tätige Senioren um die Ausgestaltung und Vermittlung derartiger Informationen und werden dabei durch das Sachgebiet Prävention der PI DS unterstützt. Im Berichtsjahr fand eine gemeinsame Veranstaltung in Königs-Wusterhausen statt.

Unterstützend kommen bei den polizeilichen Veranstaltungen u. a. Informationsmaterialien des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) zur Anwendung.

Des Weiteren finden Veranstaltungen mit Erwachsenen (wie Eltern oder Lehrer/-innen) statt, um diese mit den Themen Internet und Neue Medien vertraut zu machen, sie zu einem sicherheits- und verantwortungsbewussten Umgang mit dem Internet und den Neuen Medien zu befähigen und als Multiplikatoren zu gewinnen.

Die im LKA Brandenburg eingerichtete „Zentrale Ansprechstelle Cybercrime“ (ZAC) bietet Wirtschaftsunternehmen und Behörden Beratung und Unterstützung zum Thema „Cybersicherheit“ u. a. auch zu den Maßnahmen nach Feststellung eines Angriffs durch Cyberkriminelle an. Hierzu sind für die ZAC in den Bundesländern gesonderte Erreichbarkeiten eingerichtet[6].

Die ZAC kooperiert insbesondere mit Vertretern der Industrie- und Handelskammern (IHK), der Handwerkskammer (HWK), dem Verband für Sicherheit in der Wirtschaft Berlin-Brandenburg (VSW BE-BB), der Arbeitsgemeinschaft Technikunterstützte Informationsverarbeitung im Land Brandenburg (TUIV AG)

[6] siehe auch www.polizei-dein-partner.de - Präventionsportal der Gewerkschaft der Polizei

sowie dem Zentralen IT-Dienstleister für Behörden des Landes Brandenburg (ZIT BB). Neben dem regelmäßigen Erfahrungsaustausch beteiligt sich die ZAC aktiv an der Gestaltung von Informationsveranstaltungen z. B. beim Verband für Sicherheit in der Wirtschaft oder vor Vertretern von Unternehmen sowie Mitarbeitern der öffentlichen Verwaltungen bzw. führt derartige Veranstaltungen auch anlassbezogen nach Anforderung eigenständig durch.

Die ZAC Brandenburg hat im Jahr 2022 insgesamt 19 Veranstaltungen mit 1.800 Teilnehmern (2021: neun Veranstaltungen mit 630 Teilnehmern) mit Vorträgen zu aktuellen Aspekten der Cybersicherheit und Verhaltensempfehlungen bzw. mit Live-Vorführungen zu möglichen Sicherheitsrisiken im täglichen Umgang mit den Medien aktiv unterstützt.

Die in vielen Unternehmen bestehenden technischen Sicherungsmaßnahmen, wie z. B. Backups, IT-Berater, Antivirensoftware, etc. sind keine Garantie für die Vermeidung von schädigenden Cyberangriffen. Einmal bekanntgewordene Schwachstellen in den Systemen der Geschädigten werden auch in der Folge weiterhin durch Tatverdächtige ausgenutzt. Es besteht daher fortwährend Beratungsbedarf, so dass technische Sicherheitsmaßnahmen und Handlungsempfehlungen im erforderlichem Umfang in die allgemeinen Arbeitsabläufe integriert werden können.

4. Gesamtbewertung und Ausblick

Die Möglichkeiten im Rahmen der Digitalisierung der Gesellschaft, sowohl im privaten als auch kommerziellen Bereich, geben regelmäßig auch Manipulations- und Angriffsmöglichkeiten für Cyberkriminelle. Zu den häufigsten Angriffsvektoren gehören weiterhin das Ausnutzen von Schwachstellen in den IT-Systemen sowie die Nutzung strukturiert betriebener Botnetze, um Schadsoftware oder Spam-E-Mails massenhaft zu verteilen. Daher ist in Bezug auf Cybercrime weiterhin von einem hohen bzw. steigenden Gefährdungs- und Schadenspotential auszugehen.

Schadprogramme, die gezielt an Internetnutzer bzw. breit an eine undefiniert große Anzahl von Privatpersonen, Unternehmen und Behörden, z. B. per E-Mail oder Drive-by-Exploit verteilt werden, stellen eine der größten Bedrohungen im Bereich Cybercrime dar. Insbesondere die Bedrohungslage durch Ransomware spielt aufgrund der hohen monetären bzw. wirtschaftlichen Schäden eine herausgehobene Rolle. Bei der Durchführung der Cyber-Angriffe werden von den Angreifern häufig psychologische Manipulationstechniken (bekannt als Social Engineering) angewandt bzw. verschiedene Verschlüsselungs- und Anonymisierungstechnologien zur Tatausführung eingesetzt.

In einer Studie (Wirtschaftsschutz 2022) des Branchenverbandes Bitkom vom 31. August 2022 wird von einem Schaden für Unternehmen in Deutschland in Höhe von 202 Mrd. Euro allein durch Diebstahl, Industriespionage und Sabotage (vorrangig durch Ransomware) berichtet. Die durch Cybercrime verursachten Schäden werden in zahlreichen Studien, insbesondere durch Bitkom, seit vielen Jahren verfolgt. Hierbei sind jährliche Steigerungen im Milliardenbereich absehbar.

Ausbau und Nutzung der „Cybertoolbox“ des BKA als Ermittlungsinstrument
Die „Cybertoolbox“ ist eine Webanwendung, in der verschiedene Ermittlungs- und Auswertetools des BKA über Extrapol den Polizeibehörden der Länder und des Bundes zur Verfügung gestellt werden. Ermöglicht wird die Überprüfung verschiedener, polizeilich relevanter Entitäten[7] auf etwaig beim BKA vorliegende Erkenntnisse, sowie die Möglichkeit, im Trefferfall aus den Anwendungen heraus Auskunftsersuchen zu den getroffenen Entitäten an das BKA zu übermitteln. Die „Cybertoolbox“ wurde allen kriminalpolizeilichen Dienststellen im Jahre 2020 vorgestellt und hat sich im Laufe der letzten beiden Jahre als Ermittlungsinstrument etabliert. Eine Besonderheit ergibt sich, sofern zwei Nutzer (Ermittler) dieselbe Suche (auch bundesweit) durchführen, da sie nunmehr über die Suche des jeweils anderen automatisiert benachrichtigt werden. Dadurch kann eine Doppelbearbeitung auch über Ländergrenzen hinweg verhindert und die Erkenntnislage verbessert werden. Die Implementierung des sogenannten „dir3ctory“ in der Cybertoolbox, als Nachfolger der Zentralen Providerdatenbank, wertet die Ermittlungsmöglichkeiten nochmals deutlich auf.

Die sachgerechte Nutzung der „Cybertoolbox“ in den Ermittlungsdienststellen unterstützt die Ermittlungsführung und ist daher weiterhin zu intensivieren.

[7] Eine Entität ist ein Begriff aus der Philosophie, Semantik und Informatik. Eine Entität beschreibt das Wesen bzw. die Identität eines konkreten oder abstrakten Gegenstands des Seins. Entitäten sind eindeutig identifizierbar und damit einzigartig.

Planung weiterer (Cybercrime) -Übungen mit KRITIS-Unternehmen

Nachdem im Jahr 2021 eine Cybercrime-Übung des LKA BB mit BASF Schwarzheide als KRITIS-Unternehmen durchgeführt wurde, sollten weitere Planübungen/Planbesprechungen mit KRITIS-Betreibern im Land Brandenburg im Blick behalten werden. Insbesondere vor dem Hintergrund der allgemein steigenden Bedrohungslage, auch im Kontext des Russland-Ukraine-Krieges 2022 sollte Handlungssicherheit sowohl bei den KRITIS-Betreibern als auch im Polizeibereich bei entsprechenden Angriffsszenarien bestehen. Die Polizei soll dabei proaktiv an KRITIS-Betreiber herantreten und die Durchführung gemeinsamer Übungen vorantreiben.

Durchführung eines landesweiten Monitorings zur Entwicklung des Phänomens Cybercrime und angrenzender Phänomenbereiche sowie einer entsprechenden quartalsweisen Lagedarstellung

Im Zusammenhang mit der Schnelllebigkeit des Kriminalitätsbereichs „Cybercrime“ erscheint ein lediglich jährlich erstelltes Landeslagebild nicht ausreichend, um neue Phänomene und Begehungsweise zu erkennen und auf diese adäquat eingehen zu können. Aus diesem Grund wird beginnend mit dem 1. Quartal 2023 eine entsprechende Ausarbeitung vierteljährlich erfolgen.

5. Anlagen

5.1 Cybercrime

- Fallzahlenentwicklung 2018 bis 2022 (Quelle: PKS)

	2018	2019	2020	2021	2022		Veränderung
Erfasste Fälle	**2.992**	**2.461**	**2.323**	**2.678**	**2.640**	↘	***-1,4 %***
Aufklärungsquote (AQ) in %	73,7	67,9	63,1	61,8	58,2	↘	*-3,6 %*

- Delikte im Detail:

▸ Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr b. der Datenverarbeitung (§§ 269, 270 StGB)	124	100	71	99	96	↘	*-3,0 %*
▸ Datenveränderung, Computersabotage (§§ 303a, 303b StGB)	80	63	68	69	78	↗	*+13,0 %*
▸ Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei (§§ 202a-d StGB)	116	107	74	63	65	↗	*+3,2 %*
▸ Computerbetrug (§ 263a StGB)	2.658	2.186	2.102	2.447	2.401	↘	*-1,9 %*
▸ Betrügerisches Erlangen von Kfz	0	0	3	2	2		*0,0 %*
▸ Weitere Arten des Warenkreditbetruges	1.104	922	899	1.182	1.209	↗	*+2,3 %*
▸ Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	424	449	415	542	540	↘	*-0,4 %*
▸ Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	121	145	115	118	86	↘	*-27,1 %*
▸ Computerbetrug mittels rechtswidrig erlangter sonst. unbarer Zahlungsmittel	614	268	223	229	170	↘	*-25,8 %*
▸ Leistungskreditbetrug	125	100	175	101	107	↗	*+5,9 %*
▸ Computerbetrug (sonstiger)	196	230	223	194	175	↘	*-9,8 %*
▸ Missbräuchliche Nutzung von Telekommunikationsdiensten	41	35	8	10	18	↗	*+80,0 %*
▸ Abrechnungsbetrug im Gesundheitswesen	0	0	1	0	0		
▸ Überweisungsbetrug	33	37	10	69	94	↗	*+36,2 %*

- Schadenssummen 2018 bis 2022 (Quelle: PKS)[8]

Jahr	Schadensfälle insgesamt	Schaden in EUR	durchschnittlicher Schaden in EUR pro Fall
2018	2.658	2.369.627	892
2019	2.186	2.196.569	1.005
2020	2.102	2.105.125	1.002
2021	2.447	2.578.011	1.054
2022	2.401	2.386.503	994

- Tatverdächtige 2018 bis 2022 (Quelle: PKS)

	2018	2019	2020	2021	2022		Veränderung
Tatverdächtige (insgesamt)	**1.265**	**1.114**	**1.108**	**1.151**	**1.097**	↘	***-4,7 %***
männlich	836	736	691	740	714	↘	*-3,5 %*
weiblich	429	378	417	411	383	↘	*-6,8 %*
Erwachsene	1.123	964	974	1.022	973	↘	*-4,8 %*
Heranwachsende	93	94	89	75	67	↘	*-10,7 %*
Jugendliche	41	47	35	43	42	↘	*-2,3 %*
Kinder	8	9	10	11	15	↗	*+36,3 %*
Nichtdeutsche TV	221	128	143	138	147	↗	*+6,5 %*
Anteil nichtdeutscher TV in %	17,5	11,5	12,9	12,0	13,4	↗	*+1,4-Punkte %*

[8] Bei Cybercrime wurden Schäden nur bei den Delikten des Computerbetruges (PKS-Summenschlüssel 897100) registriert.

5.2 Tatmittel Internet und/oder IT-Geräte[9]

- Fallzahlenentwicklung 2018 bis 2022 (Quelle: PKS)

	2018	2019	2020	2021	2022		Veränderung
erfasste Fälle (insgesamt)	**7.998**	**7.939**	**7.995**	**8.528**	**8.350**	↘	***- 2,1 %***
Aufklärungsquote (AQ) in %	86,3	86,1	86,7	87,0	85,2	↘	*-1,8 %-Punkte*

- Schadenssummen 2018 bis 2022 (Quelle: PKS)

Jahr	Schadensfälle insgesamt	Schaden in EUR	durchschnittlicher Schaden in EUR pro Fall
2018	5.577	3.773.915	677
2019	5.252	3.792.966	722
2020	4.948	7.804.313	1.577
2021	5.033	4.813.940	956
2022	4.502	5.355.108	1.189

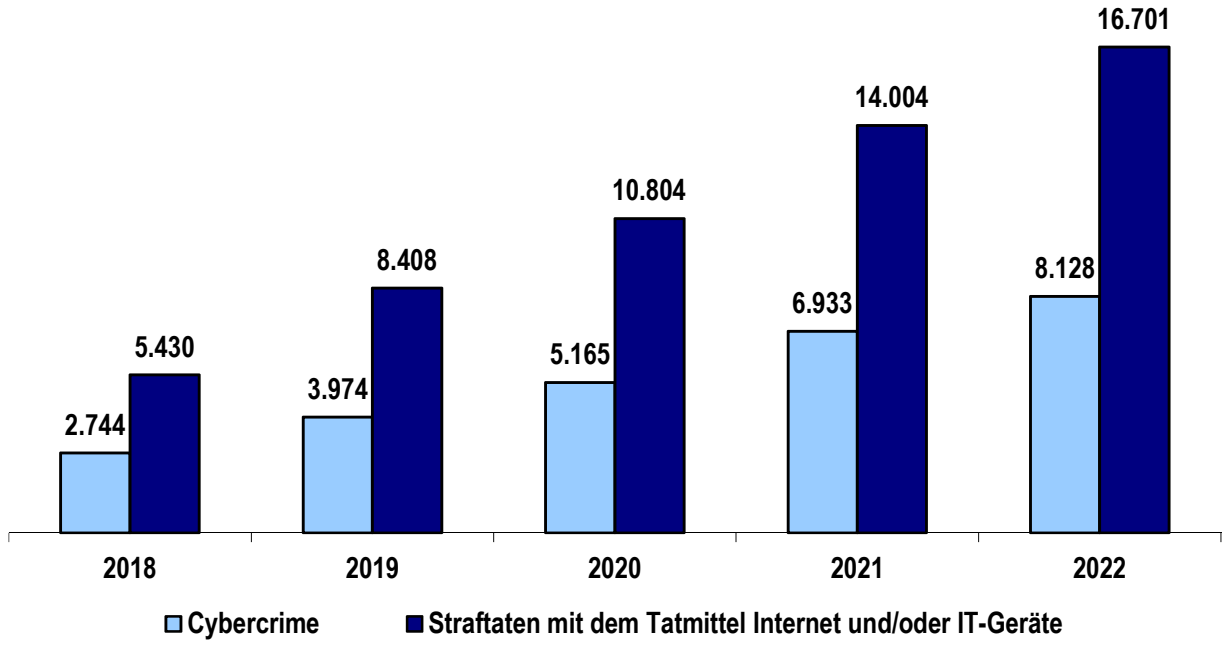
- Tatverdächtige 2018 bis 2022 (Quelle: PKS)

	2018	2019	2020	2021	2022		Veränderung
Tatverdächtige (insgesamt)	**4.381**	**4.646**	**5.065**	**5.574**	**5.614**	↗	***+0,7 %***
männlich	2.949	3.247	3.511	3.911	3.907	↘	*-0,1 %*
weiblich	1.432	1.399	1.554	1.663	1.707	↗	*+2,6 %*
Erwachsene	3.604	3.698	3.964	4.255	4.219	↘	*-0,8 %*
Heranwachsende	361	412	436	528	490	↘	*-7,2 %*
Jugendliche	345	394	464	555	588	↗	*+5,9 %*
Kinder	71	142	201	236	317	↗	*+34,3 %*
Nichtdeutsche TV	308	303	387	475	484	↗	*+1,9 %*
Anteil nichtdeutscher TV in %	7,0	6,5	7,6	8,5	8,6	↗	*+0,1 %-Punkte*

[9] Zum 01.01.2021 erfolgte die Umbenennung des Sonderkenners „Tatmittel Internet“ in „Tatmittel Internet und/oder IT-Geräte“. Weiter wurden die alle bis dahin vorhandenen Sonderkenner aus dem Bereich Cybercrime abgeschafft. Die bis dahin mit diesen Sonderkennern erfassten Delikte werden ab 2021 unter dem einzig verbliebenen Sonderkenner „Tatmittel Internet und/oder IT-Geräte“ erfasst. Aus diesem Grund ist eine Vergleichbarkeit der Jahre 2018-2020 sowie 2021-2022 nur eingeschränkt gegeben.

5.3 Auslandsstraftaten[10]

(Quelle: PKS-Ausland)



- Aufklärungsquoten

	2018	2019	2020	2021	2022
Cybercrime	5,6 %	4,6 %	3,1 %	2,8 %	2,7 %
Straftaten mit dem Tatmittel Internet und/oder IT-Geräte	8,4 %	6,8 %	7,1 %	10,1 %	9,5 %

[10] Auf Grund der veränderten Definition des PKS-Summenschlüssel 897000 Cybercrime (vor 2021 Computerkriminalität) wurden für die Jahre 2018-2020 die einzelnen PKS-Schlüssel für diesen PKS-Summenschlüssel gemäß der Richtlinie 2022 einzeln addiert, um eine Vergleichbarkeit mit den Zahlen der Jahre 2021 und 2022 zu schaffen.