Polizeipräsidium
Land Brandenburg

Landeskriminalamt

Lagebild
Cybercrime
im Land Brandenburg
Jahr 2023

Impressum

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

cybercrime.lka@polizei.brandenburg.de

Trend

	2022	2023		Veränderung in Prozent
Cybercrime	**2.640**	**2.744**	↗	**+3,9 %**
Ausspähen von Daten	56	80	↗	+42,9 %
Abfangen von Daten	3	1	↘	-66,7 %
Vorbereiten des Ausspähens und Abfangens von Daten	4	5	↗	+25,0 %
Datenhehlerei	2	3	↗	+50,0 %
Fälschung beweiserheblicher Daten	94	129	↗	+37,2 %
Täuschung im Rechtsverkehr bei der Datenverarbeitung	2	6	↗	+200,0 %
Datenveränderung	57	62	↗	+8,8 %
Computersabotage	21	17	↘	-19,0 %
Computerbetrug	2.401	2.441	↗	+1,7 %
- Betrügerisches Erlangen von Kfz	2	1	↘	-50,0 %
- Weitere Arten des Warenkreditbetruges	1.209	1.193	↘	-1,3 %
- Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	540	547	↗	+1,3 %
- Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	86	126	↗	+46,5 %
- Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel	170	223	↗	+31,2 %
- Leistungskreditbetrug	107	112	↗	+4,7 %
- Computerbetrug (sonstiger)	175	137	↘	-21,7 %
- Missbräuchliche Nutzung von Telekommunikationsdiensten	18	14	↘	-22,2 %
- Abrechnungsbetrug im Gesundheitswesen	0	0	=	0
- Überweisungsbetrug	94	88	↘	-6,4 %
Delikte mit Tatmittel Internet und/oder IT-Geräte (insg.)	**8.350**	**8.788**	↗	**+5,2 %**

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 gemäß §§ 269, 270 StGB
- Datenveränderung, Computersabotage gemäß §§ 303a, 303b StGB
- Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei gemäß §§ 202a, 202b, 202c, 202d StGB
- Computerbetrug gemäß § 263a StGB.

Weiter existiert ein gleichnamiger PKS-Summenschlüssel 897100 „Computerbetrug" gemäß § 263a StGB. 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 wurde in „Tatmittel Internet und/oder IT-Geräte" umbenannt. 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 des 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 und/oder IT-Geräte als Tatmittel 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 erfüllen 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 den polizeilichen Informationsquellen 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 2023 erfassten Straftaten, die sich gegen das Internet, weitere Datennetze, IT-Systeme oder deren Daten richten, ist gegenüber dem Vorjahr um 3,9 % auf 2.744 Fälle (2022: 2.640 Fälle) gestiegen.

Hinsichtlich der Gesamtsumme des Computerbetruges (PKS-Summenschlüssel 897100) ergibt sich ein leichter Anstieg um 1,7 % auf 2.441 Fälle (2022: 2.401 Fälle).

Die Entwicklung der weiteren Fallzahlen der zu Cybercrime zuzuordnenden Deliktsgruppen stellt sich wie folgt dar:

- Ausspähen und Abfangen von Daten, einschließlich der Vorbereitungshandlungen und Datenhehlerei 89 Fälle (+36,9 %, +24 Fälle),
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung 135 Fälle (+40,6 %, +39 Fälle),
- Datenveränderung, Computersabotage 79 Fälle (+1,3 %, +1 Fall).

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 und/oder IT-Geräte enthalten.

Bei den registrierten Schäden der Cybercrime ist im Jahr 2023 ein Anstieg um 28,5 % auf 3.066.628 EUR zu verzeichnen (2022: 2.386.503 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 Cybercrime-Delikte 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 sind. 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) stieg von 1.097 TV (Vorjahr) auf 1.327 TV. Personen über 21 Jahre stellen mit einem Anteil von 90,0 % bzw. 1.194 TV

(2022: 88,7 %, 973 TV) weiterhin die anteilig größte Gruppe unter den TV dar. Der Anteil nichtdeutscher TV beträgt 12,9 % bzw. insgesamt 166 TV (Vorjahr 13,4 % bzw. 147 TV).

Im Phänomenbereich Cybercrime wurden im Berichtsjahr 9.751 Auslandsstraftaten und somit 1.623 Straftaten (20,0 %) mehr als im Vorjahr (8.128) polizeilich registriert. Somit haben etwa 78,0 % (2022: 75,5 %) der in Brandenburg polizeilich bekannt gewordenen Cybercrime-Straftaten ihren Ursprung im Ausland oder sind unbekannten Ursprungs.

2.1.2 Tatmittel Internet und/oder IT-Geräte

Fälle, die unter das „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 2023 wurden in der PKS insgesamt 8.788 Fälle erfasst, die unter Nutzung des „Tatmittels Internet und/oder IT-Geräte“ begangen wurden. Im Vergleich zum Vorjahr stellt dies einen Anstieg um 388 Fälle bzw. 5,2 % dar. Überwiegend handelte es sich dabei um Fälle des Waren-/Warenkreditbetruges (3.174 Fälle, -140 Fälle oder -4,2 %) sowie des Computerbetruges[2] (1.673 Fälle, +21 Fälle oder +1,3 %).

Die polizeilich erfasste Gesamtschadenssumme (Schaden gemäß PKS) hat sich von 5.355.108 EUR auf 5.273.136 EUR bzw. um 1,5 % verringert.

Im Berichtszeitraum wurden zu den Straftaten mit dem „Tatmittel Internet und/oder IT-Geräte“ 6.191 TV und somit 577 TV mehr als in 2022 ermittelt. Der Anstieg beträgt somit 10,3 %. Dieser entfällt nahezu vollständig auf die erwachsenen TV, welche um 566 auf nunmehr 4.785 TV angestiegen sind. Die Zahl der Heranwachsenden bleibt mit 490 unabhängig von der angestiegenen Anzahl an Straftaten gleich. Die Anzahl der tatverdächtigen Kinder und Jugendlichen hingegen fiel auf 291 TV (-26 TV) bzw. stieg auf 625 TV (+37 TV) an. Insgesamt bilden die Erwachsenen mit 77,3 % (4.785 TV) weiterhin die anteilig größte Gruppe unter den TV.

Zu den Straftaten mit dem „Tatmittel Internet und/oder IT-Geräte“ wurden im Jahr 2023 insgesamt 557 nichtdeutsche TV und damit 73 mehr als im Vorjahr erfasst. Den 557 TV konnten Staatsangehörigkeiten aus insgesamt 75 Staaten zugeordnet werden. Die meisten der nichtdeutschen TV stammen aus Syrien (74 TV), Polen (62 TV), der Russischen Föderation (42 TV), der Ukraine (36 TV), Afghanistan (30 TV), Türkei (22 TV) und Nigeria (19 TV).

[2] Die dargestellten Zahlen des Computerbetruges stellen lediglich diejenigen Fälle dar, welche von den kriminalpolizeilichen Sachbearbeitern auch mit dem entsprechenden Sonderkenner versehen wurden. Die Gesamtzahl der Fälle des Computerbetrugs betragen 2.441 Fälle (Punkte 2.1.1).

In der Kategorie „Auslandsstraftaten“ wurden bei den Straftaten mit dem „Tatmittel Internet und/oder IT-Geräte“ im Berichtsjahr 20.465 Fälle registriert. Damit ist das Fallaufkommen gegenüber dem Vorjahr (2022: 16.701 Fälle) signifikant um 3.764 Fälle (+22,5 %) angestiegen. Insgesamt entspricht dies einem Anteil von 67,7 % (Vorjahr 66,7 %) der polizeilich registrierten Straftaten mit dem „Tatmittel Internet und/oder IT-Geräte“, die durch Tathandlungen aus dem Ausland oder ungeklärten Ursprungs heraus begangen worden sind.

2.1.3 PKS-Phänomene

Unter den dem Cybercrimebereich zuzuordnenden Delikten (z. B. Ausspähen von Daten) werden unterschiedliche Phänomene (z. B. Identitätsdiebstahl, Angriff auf das Online-Banking) erfasst. Folglich sind nicht schon an Hand der bloßen Betrachtung der Deliktszahlen entsprechende Entwicklungen erkennbar. Aus diesem Grund ist eine tiefergreifende Differenzierung der jeweiligen Straftaten und eine Zuordnung zu Phänomenen nötig, weshalb ein Katalog für bestimmte Phänomene eingeführt wurde:

- (D)DoS-Attacke
- Digitaler Identitätsdiebstahl/Accountübernahme
- Eindringen in Datennetze/Datenveränderung/Datendiebstahl bei nichtnatürlichen Personen
- Angriff auf das Online-Banking
- Ransomware.

Diese sind durch die Sachbearbeitung auszuwählen und unabhängig vom jeweiligen Delikt zu erfassen, wobei jedoch Unterrepräsentativität zu unterstellen ist (vgl. Fallzahl Ransomware Sonderauswertung und Fallzahl Phänomenkenner).

Im Berichtsjahr wurden 74 Fälle als Phänomen „Angriff auf das Online-Banking“, 587 Fälle als Phänomen „digitaler Identitätsdiebstahl/ Accountübernahme“, 50 Fälle als „Eindringen in Datennetze/Datenveränderung/Datendiebstahl bei nichtnatürlichen Personen“ sowie vier Fälle als „Ransomware“ erfasst. Gemäß den PKS-Daten gab es demnach keinen Fall, der dem Phänomen „DDoS“ zugeordnet wurde.

2.2 Aktuelle Begehungsweisen und Phänomene

2.2.1 Diebstahl digitaler Identitäten und Identitätsmissbrauch

Die digitale Identität[3] 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 oder

[3] 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, z. B. Zugangsdaten in den Bereichen Kommunikation, E-Commerce, berufsspezifische Informationen, E-Government, Cloud-Computing sowie alle anderen zahlungsrelevanten Informationen.

durch Datenabfluss nach einem Angriff auf Online-Plattformen statt. Der Identitätsdiebstahl stellt regelmäßig die vorbereitende Einstiegshandlung für die Begehung weiterer Straftaten der Cybercrime und anderer Delikte dar (z. B. betrügerische Warenbestellungen, missbräuchliche Verwendung von Kreditkartendaten, Versendung von Schadsoftware, DDoS-Attacken zum Nachteil von Unternehmen, Behörden und Einrichtungen etc.).

Warenkreditbetrugshandlungen nach vorherigem Ausspähen von Zugangskennungen, insbesondere bei E-Mail-Diensten und Onlinehändlern bzw. kompletter „Identitätsdiebstahl“ (mit Neuanlage von Accounts bei Verkaufs- und Finanzdienstleistungsplattformen im Namen Dritter), wurden im Berichtsjahr weiterhin auf hohem Niveau dokumentiert.

Ferner werden die erlangten Daten auch über illegale „Marktplätze“ und Foren der Underground Economy mit monetärem Gewinn veräußert oder kostenfrei zur Verfügung gestellt.

Gerade in Bezug auf Finanzdienstleister und Exchanger für Kryptowährungen 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 wurde festgestellt, dass die Täter dabei immer professioneller vorgehen, um ihre Identität zu verbergen. Hierfür wurden IP-Adressen verschleiert, erhaltene Gelder mehrmals an Accounts von unterschiedlichen Finanzdienstleistern mit unterschiedlichsten Aliaspersonalien weitertransferiert bzw. Einkäufe bei Unternehmen getätigt, bei denen Auskunftsersuchen der Polizei nicht beantwortet werden (insbesondere Firmen aus dem Ausland) oder eine entsprechende Auskunft nicht zum Täter führt (z. B. Gutscheine, Guthabenkarten). Auch werden Kryptowährungen mit teilweise starken Anonymitäts-Funktionalitäten verwendet sowie bewusst zwischen unterschiedlichen Kryptowährungen gewechselt. Oftmals werden längere Zeit nicht genutzte Accounts von Verkaufs- und Finanzdienstleisterplattformen genutzt, um in weiterer Folge Warenkreditbetrugstaten zu begehen.

Im Zusammenhang mit dem Diebstahl digitaler Identitäten ist auch die Anwerbung von unwissentlichen Finanzagentinnen und Finanzagenten weiterhin ein verbreitetes Mittel.

Ein Modus Operandi stellt dabei die Darstellung einer vermeintlichen Warnmeldung auf dem Computer dar, bei der dem Anwender suggeriert wird, dass sich eine Schadsoftware auf dessen Endgerät befände und diese durch einen Anruf beim entsprechenden Betriebssystem-Hersteller einen Support zum Entfernen dieser Schadsoftware erhalten können. In der Regel werden diese dann durch den vermeintlichen Supportmitarbeiter dazu animiert, eine Fernwartungs-Software auf ihren Computer zu installieren und dadurch Fremdzugriff auf das eigene IT-System zu gewähren. In der Folge werden die Geschädigten kommunikativ derart beeinflusst oder unter Druck gesetzt, dass diese mitunter Bankkonten und/oder Accounts bei Exchangern für Kryptowährungen eröffnen bzw. die entsprechenden Zugangsdaten für bereits existierende Accounts herausgeben, ohne es im Detail konkret wahrzunehmen.

Wie auch im Jahr 2022 wurden zunehmend Fälle registriert, bei denen Täter unberechtigt auf den E-Mail-Verkehr von Firmen zugriffen und bereits gestellte Rechnungen durch „neue“ Bankdaten abänderten (sog. Payment-Diversion-Fraud). Diese „neuen“ Bankverbindungen sind sowohl inländischen als auch ausländischen Banken und in der Regel Finanzagentinnen und -agenten zuzuordnen. Die Täter

erlangen dabei Zugriff auf interne Konversationen der Geschädigten, indem es ihnen z. B. gelingt, auf einen der entsprechenden E-Mail-Accounts Zugriff zu erlangen oder die Konversation mit einer nur marginal veränderten E-Mail-Adresse zu „übernehmen".

Beispielfall
Am 28.06.2023 erstattete die geschädigte Firma Strafanzeige gegen unbekannte Täter. Demnach arbeitet die geschädigte Firma für ihre Auslandsgeschäfte in Spanien mit einer selbstständigen Handelsvertretung in diesem Land zusammen. Diese leitet Rechnungen von der geschädigten Firma an die Kunden in Spanien weiter. Einer der spanischen Kunden hatte Produkte im Wert von 116.401,45 Euro erhalten. Die entsprechenden Rechnungen wurden vom geschädigten Unternehmen an die Handelsvertretung in Spanien per E-Mail versendet. Diese E-Mails, inklusive der jeweiligen Anhänge, wurden durch die Täter offensichtlich „abgefangen", die Rechnungen verändert und sodann an die Handelsvertretung gesendet und in der Folge durch diese an die spanischen Kunden der geschädigten Firma weitergeleitet. Da die Kunden die Rechnungen von der bekannten Handelsvertretung erhielten, wurden die Rechnungen entsprechend beglichen. Als die jeweiligen Beträge nicht bei der geschädigten Firma aus Deutschland eingingen, ergaben interne Überprüfungen, das die Handelsvertretung die in Rede stehende E-Mail mit den angefügten Rechnungen von einer E-Mail-Adresse erhielt, die der originalen E-Mail-Adresse täuschend ähnlich aussah. Es wurde lediglich ein Buchstabe in der Domain ausgetauscht.

Beispielfall
Zwei in Brandenburg ansässige Unternehmen aus der Solaranlagen-Branche stehen in geschäftlichen Beziehungen zueinander. In der Folge wurde von einem der Unternehmen eine Rechnung in einer E-Mail an das andere Unternehmen übersandt. Diese E-Mail ging dort offensichtlich nie ein. Stattdessen fingen unbekannte Täter die E-Mail offensichtlich ab, veränderten die Rechnung und übersandten diese erneut im Namen der Rechnung stellenden Firma mit dem Hinweis, dass die Kontoverbindung sich gegenüber vorherigen Handelsgeschäften geändert habe. Der Kunde ging von der Echtheit der Rechnung aus und überwies den offenen Betrag in Höhe von 1.076.575,42 Euro an die „neue" Bankverbindung. Diese gehörte zu einer deutschen Bank. Die dortigen internen Prüfmechanismen kamen zu dem Ergebnis, dass die IBAN nicht zum Empfänger passt und es sich um eine geschäftliche Überweisung handelt, die Bank aber keine Geschäftskonten unterhalte. Die Summe wurde daher an das überweisende Unternehmen zurücküberwiesen. Wie es den Tätern gelang, auf den E-Mail-Verkehr der geschädigten Firma zuzugreifen, wurde nicht zweifelsfrei festgestellt.

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. Auffällig ist hierbei, dass die Nutzung der Bankdaten der Geschädigten im nicht europäischem Ausland (Asien, Russland) zugenommen hat.

Auf ähnlich hohem Niveau gegenüber dem Vorjahr sind die Fälle der Betrugsmasche „Support eines Betriebssystemherstellers" geblieben. Die Geschädigten erhalten Anrufe von Tätern oder werden durch Einblendungen von sog. „Pop-Up"-Fenstern auf dem Computerbildschirm dazu animiert, eine telefonische

Verbindung aufzubauen. Die jeweiligen „Gesprächspartner“ stellen sich als „Support-Mitarbeiter“ vor, die bei der Behebung der angeblichen Störung oder des “Schadsoftwarebefalls“ behilflich wären. Vereinzelt wurden Ermittlungsverfahren geführt, bei denen die Geschädigten über sechs Stunden mit den Tätern telefonierten und diesen bis zu 25 TANs übermittelten. Sofern nicht schon telefonisch eine Abfrage der Zugangsdaten für das Online-Banking erfolgte, wurden die Geschädigten wiederum dazu animiert, eine „Fernwartungssoftware“ auf dem IT-System zu installieren und dem vorgeblichen Support-Mitarbeiter dadurch Fernzugriff auf ihren Computer zu ermöglichen. In der Folge wurden die Geschädigten dazu veranlasst, Zahlungen, z. B. für diese „Dienstleistungen“, per Online-Banking durchzuführen oder die Täter installierten aus der Ferne Software, mit welcher im nächsten Schritt die jeweiligen Zugangsdaten etc. ausgespäht wurden.

Ergänzend wurde in der Polizeidirektion Ost festgestellt, dass es dort vermehrt zu Stromanbieterwechseln ohne Zustimmung der Geschädigten gekommen ist. Demnach waren die Täter als „Subunternehmer für Stromanbieter“ tätig und gelangten über Gemeinschaftsstromzähler an die Daten der Geschädigten. In der Folge wurden neue Stromverträge im Namen der Geschädigten online abgeschlossen. Durch die neuen Stromunternehmen wurden Provisionen an die Täter ausgezahlt. Die Geschädigten stellten erst auf Grund der Bank-Abbuchungen fest, dass sie ihren Stromanbieter „gewechselt“ haben.

Das Phänomen des sog. „falschen Bankmitarbeiters“ ist weiterhin präsent. Dabei werden die Geschädigten mittels einer veränderten Rufnummer der tatsächlichen Bank (sog. „Call-ID-Spoofing) kontaktiert. Am häufigsten erhielten die Geschädigten nach dem Erhalt einer E-Mail, welche den Telefonanruf eines Kundenberaters des Geldinstitutes ankündigte, tatsächlich einen solchen Anruf. Im Gespräch mit dem vorgeblichen 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.

Bezugnehmend auf diesen Modus Operandi wird erkennbar, dass das Vorgehen der Täter einem ständigen Wandel unterliegt und häufig nicht nachvollzogen kann, wie die Täter an Kontodaten und weitere sensible Daten der Geschädigten gelangt sind.
Es wurden darüber hinaus wiederholt Fälle bearbeitet, bei denen die Zahlungsmöglichkeiten mittels Smartphone missbräuchlich verwendet wurden. Die Anzahl der Fälle, bei denen Kryptowährungen zumeist als Auszahlungsmedium nach Fremdkontennutzung verwendet wurden, hat sich nach hiesiger Einschätzung erhöht. Leider spiegeln die polizeilichen Auskunftssysteme keine valide Datenbasis in diesem Kontext wider. 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“[4] hat sich in Deutschland zu einer weit verbreiteten Begehungsweise entwickelt und ist maßgeblich für die festgestellten 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-as-a-Service (R-a-a-S)“ erworben werden. Hierdurch ist bei den Tätern kein besonderer IT-Sachverstand mehr 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 u. a. Sicherheitslücken 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. Darüber hinaus müssen häufig externe IT-Unternehmen mit dem Vorfall beauftragt werden, was regelmäßig zu einer vollständigen Bereinigung des jeweiligen IT-Systems 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.

Im Bereich der Privatpersonen wurde diese Art der digitalen Erpressung nicht festgestellt. Bei dieser Zielgruppe wird auf deren IT-System oftmals lediglich ein Sperrbildschirm eingeblendet, um dem potenziellen Opfer zu suggerieren, deren Daten wären verschlüsselt/gesperrt. Eine Entsperrung dieser Daten soll dann durch die Zahlung einer Summe in der Regel in Kryptowährungen möglich sein. Auch wenn hier im Allgemeinen keine Verschlüsselungen von Daten stattfinden, werden diese Fälle teilweise auf Grund der nicht einheitlichen Definition von „Ransomware“ dem entsprechenden Phänomen zugeordnet.

Entscheidend für die Zuordnung zum Phänomen „Ransomware“ ist, dass dies im Einzelfall durch die Sachbearbeitung erkannt und mit dem entsprechenden PKS-Kenner versehen wird. Für das Jahr 2023 wurden demnach lediglich vier in Brandenburg bearbeitete Verfahren mit dem PKS-Kenner „Ransomware“ markiert.

[4] Die Bezeichnung Ransomware wird für Schadsoftware-Varianten verwendet, die es Tätern ermöglichen, Daten auf fremden Computern zu verschlüsseln oder die Benutzung des Computers auf andere Art und Weise zu verhindern (z. B. Sperrbildschirm). Zur Entschlüsselung oder Freigabe des Computersystems wird der Betroffene aufgefordert, einen bestimmten Betrag in einer vorgegebenen Währung, zumeist Krypto-Währung (z. B. Bitcoin), zu bezahlen. In einigen Fällen wurden durch die Schadsoftware auch (Firmen-)Daten an die Täter übertragen. Bei Nichtbezahlung wird mit der Veröffentlichung gedroht.

Um einen konkreteren Überblick zur Thematik „Ransomware“ zu erlangen, wurde im Rahmen der Lagebilderstellung mittels Kombination verschiedenartiger Recherchewerkzeuge der Polizei (POLAS, PKS, in der ZAC-Dienststelle des LKA bekannt gewordene Fälle) eine Sonderauswertung durchgeführt. Demnach sind dem Phänomen „Ransomware“ folgende Vorgänge zuzuordnen:

- Vorgänge 2023 insgesamt: 23 Vorgänge (davon 14 x betroffene Unternehmen, 9 x betroffene Privatpersonen)
- Vorgänge 2022 insgesamt: 31 Vorgänge (davon 26 x betroffene Unternehmen, 2 x betroffene Institution, 3 x betroffene Privatpersonen).

Auf „Unschärfen“ der Fallzahlendarstellung auf Grund nicht einheitlich umgesetzter Erfassungsregeln wird hingewiesen. Darüber hinaus ist hierbei von einem beachtlichen Dunkelfeld auszugehen, da gerade Unternehmen nicht jeden „IT-Sicherheitsvorfall“ der Polizei melden, sondern eher darauf bedacht sind, die Arbeitsfähigkeit schnellstmöglich wiederherzustellen und eine entsprechende Rufschädigung zu vermeiden.

Eine spezielle „Version“ einer Ransomware trat nicht in den Vordergrund.

Beispielfall
Ein IT-Dienstleister eines Landkreises teilte der Zentralen Ansprechstelle Cybercrime (ZAC) des LKA am 14.12.2023 telefonisch mit, dass eine Schadsoftware in den eingesetzten IT-Systemen aufgefunden wurde. Die als Systemtreiber getarnte Software sei nach ersten Informationen dazu bestimmt gewesen, Daten der IT-Systeme auszuspähen. Weiterhin wurde mitgeteilt, dass diese Schadsoftware bemerkt und bereinigt worden sei. Am gleichen Tag gingen dann bei der ZAC weitere Informationen ein, welche auf ein Ausspähen von Daten bei dem in Rede stehenden Dienstleister hindeuteten. Demnach sei es bereits zu einem Ausspähen von Daten gekommen und deren unberechtigte Verwendung zur Verschlüsselung der IT-Systeme stünde möglicherweise unmittelbar bevor. Mit diesen Informationen wurde erneut Kontakt mit dem Dienstleister aufgenommen, worauf dieser entschied, sämtliche IT-Systeme sofort vom Internet zu trennen und zu isolieren. In der Folge wurden die exemplarisch bereitgestellten Daten überprüft und es bestätigte sich, dass diese tatsächlich aus den IT-Systemen des Dienstleisters stammten. Mit diesen Daten wäre es „Angreifern“ möglich gewesen, Zugang zu sämtlichen eingesetzten IT-Systemen zu erlangen, um diese zu verschlüsseln und in der Folge den Dienstleister zu erpressen. Weiterführende Ermittlungen des LKA 121 führen in den osteuropäischen Raum.

Beispielfall
Im Rahmen des Monitorings von einschlägigen Leak-Seiten und durch das BKA gesteuerte Hinweise wurde der ZAC des LKA am 27.11.2023 bekannt, dass die Ransomwaregruppierung „INC“ ein deutschlandweit agierendes Unternehmen mit Hauptsitz in Brandenburg als verschlüsselt angab. Daraufhin nahm die ZAC mit dem Unternehmen Kontakt auf. Im Rahmen der bilateralen Zusammenarbeit konnte durch die IT-Abteilung des Unternehmens auch nach mehrwöchigen Nachforschungen allerdings keine Verschlüsselung oder ein Abfluss von Daten festgestellt werden. Kurz vor Jahresende waren auf der Leak-Seite der Gruppierung vorgebliche Daten vom in Rede stehenden Unternehmen herunterladbar. Im Rahmen einer Sichtung der Daten durch die ZAC konnte eine Betroffenheit des brandenburgischen

Unternehmens falsifiziert werden. Weitere Ermittlungen ergaben, dass tatsächlich ein im Gesundheitswesen tätiges Unternehmen aus NRW geschädigt worden war. Durch eine Kontaktaufnahme mit dem Unternehmen wurde weiterhin in Erfahrung gebracht, dass der Vorfall bereits angezeigt und durch Kollegen des LKA NRW bearbeitet worden war. Letztendlich hatte die Tätergruppierung sich im Namen des Unternehmens „geirrt" und somit wohl nicht das eigentlich geschädigte Unternehmen erpressen können.

2.2.4 Ausnutzen von Hardware- und Softwarelücken

Wie in den letzten Berichtsjahren wurden auch im vergangenen Jahr immer wieder Sicherheitslücken in Hard- und Software durch Täter ausgenutzt, um sich unberechtigt Zugang zu Daten oder Zugriff auf IT-Systeme zu verschaffen. Dabei haben vor allem das Ausnutzen von sog. Zero-Day-Sicherheitslücken[5] ein großes Schadenspotential.

Beispielfall
Im Februar wandte sich der Prokurist eines WLAN-Hotspotbetreibers an die ZAC des LKA und teilte mit, dass ein Server vom Unternehmen vermutlich teilweise verschlüsselt worden sei. Über den IT-Verantwortlichen wurde bekannt, dass der in Rede stehende Server einen veralteten Versionsstand hatte. Der exakte Schaden konnte nicht ermittelt werden, wurde aber durch das Unternehmen auf ca. 70.000 Euro geschätzt. Die Ermittlungen ergaben u. a., dass die Täter eine Schwachstelle in der auf dem Server betriebenen Virtualisierungssoftware ausnutzten. Bemerkenswert in diesem Zusammenhang ist, dass der Hersteller der Software bereits im Februar 2021 einen Patch veröffentlichte, der die ausgenutzte Sicherheitslücke schließt.

Beispielfall
Am 19.05.2023 meldete die Feuerwehr einer Stadt in Brandenburg der ZAC des LKA, dass Rettungsdienstalarmierungen einer Regionalleitstelle online einsehbar seien. Hierbei war zunächst unklar, wer die Funkübertragungen abfängt, dekodiert und sie auf einer Website öffentlich einsehbar bereitstellt. Im Zuge erster Ermittlungen konnte verifiziert werden, dass die in Rede stehenden Daten tatsächlich auf einer Website öffentlich aufrufbar sind. Im Rahmen polizeilicher Ermittlungen und Maßnahmen wurden Erkenntnisse gewonnen, die darauf hindeuten, dass der Tatverdächtige über Kenntnisse im Bereich Funktechnik verfügt und bei einer Freiwilligen Feuerwehr tätig ist. Zudem wurde eine Empfangsanlage für Digitalfunk-Übertragungen betrieben.

2.2.5 Payment Diversion Fraud

Ein weiteres bereits in den letzten Jahren weit verbreitetes (Betrugs-)Phänomen ist der so genannte „Payment Diversion Fraud". Dabei erhält im Allgemeinen der Käufer eine Zahlungsaufforderung/Rechnung von den Tätern, die vorgeben, der tatsächliche Verkäufer zu sein. Die Täter erfahren dabei auf unterschiedlichen Wegen von den Geschäftsbeziehungen zwischen zwei Unternehmen. So erhalten diese, z. B. über soziale Plattformen, Kenntnis von Geschäftshandlungen. Auch werden gezielt Personen in

[5] Zero-Day-Sicherheitslücken sind Schwachstellen in Hard- oder Softwareprodukten, die den Herstellern noch nicht bekannt sind oder zu denen noch keine Nachbesserungen (Patches) zum Schließen dieser Lücke veröffentlicht wurden.

Unternehmen, z.B. im Namen des Geschäftsführers, kontaktiert und um Übermittlung der aktuellen Aufträge gebeten. Ausgehend von diesem Grundkonstrukt werden unterschiedliche Modus Operandi angewendet, um die gefälschte Rechnung glaubhaft dem potenziellen Opfer zu übermitteln. In vielen Fällen erstellen dabei die Täter ähnliche E-Mail-Adressen und kontaktieren dann die potentiellen Opfer. Auch wurden der ZAC des LKA Fälle bekannt, bei denen im Vorfeld von einem der Geschäftspartner der E-Mail-Account oder das ganze Netzwerk kompromittiert wurde. Vor allem bei Geschäftsbeziehungen über Ländergrenzen hinweg sind z. B. Bankkonten und Firmensitz nicht immer im gleichen Land verortet.

Beispielfall

Am 25.05.2023 meldete ein im Land Brandenburg ansässiges Unternehmen der ZAC des LKA, dass ihre Kunden mitgeteilt hätten, verdächtige E-Mails vom Unternehmen erhalten zu haben. Bei den Empfängern der in Rede stehenden E-Mails handle es sich speziell um Kunden des Unternehmens, welche kürzlich eine Rechnung des Unternehmens per E-Mail erhalten hätten. Auf diese E-Mail sei dann direkt eine Zweite gefolgt, welche die Kunden über eine geänderte Bankverbindung zur Begleichung der Rechnung informierte. Unbekannte Täter hatten von einer E-Mail-Adresse, welche der echten E-Mail-Adresse des Unternehmens täuschend ähnelte, Zahlungserinnerungen mit der Mitteilung einer geänderten Kontoverbindung an Kunden versendet. Später übersandten die Täter E-Mails über die tatsächliche E-Mail-Adresse des Geschäftsführers des Unternehmens an die Kunden. In zwei Fällen wurden die Kunden nicht rechtzeitig sensibilisiert, sodass es zu Überweisungen von insgesamt 33.000 Euro kam. Im Rahmen der polizeilichen Maßnahmen konnten eine Rücküberweisung sowie eine Sperrung des Zielkontos erwirkt werden. Darüber hinaus wurde festgestellt, dass das E-Mail-Konto eines Mitarbeiters kompromittiert worden war, während eine Vertretungsregelung für den Geschäftsführer in der Anwendung Outlook bestand.

2.2.6 Betrugsstraftaten im Internet

Neben den fortwährend vorhandenen Betrugsstraftaten im Internet sind im Berichtsjahr vor allem Phänomene des sog. „Lovescaming“ bzw. des „Cybertrading“ aufgetreten. Dabei treten die Täter über soziale Plattformen mit den Opfern in Kontakt, wobei in vielen Fällen der Wechsel zu einem Instant-Messenger erfolgt. In aller Regel wird zunächst ein Vertrauensverhältnis aufgebaut.

Im Zusammenhang mit dem Phänomen „Lovescaming“ gibt der Täter vor, einen gut bezahlten Beruf auszuüben oder anderweitig über finanzielle Ressourcen zu verfügen. In der Folge wird das Opfer unter einen Vorwand gebeten, zunächst einen kleinen Geldbetrag für z. B. kaputte Reifen oder Zollgebühren zu übernehmen. Dann steigern sich die Summen unter Umständen bis auf mehrere 10.000 Euro. Zumeist geben die jeweiligen Täter vor, dass sie Probleme beim Zugriff auf ihre Konten hätten. Schadenssummen sind meist mehrere 10.000 Euro, aber auch ein Schaden bis zu 600.000 Euro wurde bereits bekannt. Die technischen Ermittlungen führen in vielen Fällen in den afrikanischen Raum.

Beim Phänomen „Cybertrading“ werden Opfer gezielt angeschrieben oder durch Werbeversprechen dazu animiert, in Kryptowährungen zu investieren. Dies geschieht auf unterschiedliche Art und Weise. So werden z. B. Webseiten aufgesetzt, die die Neugier/Unwissenheit potenzieller Opfer ausnutzen. Auf

der anderen Seite werden Opfer gezielt von „Brokern“ auf sozialen Plattformen angesprochen und diese von Investitionen auf bestimmten Webseiten „überzeugt“. Dabei werden auch hier zunächst kleinere Beträge durch die Opfer „investiert“. Die Webseiten der vorgeblichen Handelsplattformen täuschen dann eine große Wertsteigerung der „investierten“ Mittel vor. In der Folge werden in vielen Fällen weitere größere Summen durch die Geschädigten „angelegt“. Sofern die Geschädigten in der Folge Auszahlungen wünschen, werden durch die Täter weitere Beträge, wie „Steuern“, „Zollgebühren“ etc., gefordert.

Beispielfall

Anfang 2023 wurde ein IT-affiner Mitarbeiter eines Unternehmens, welcher seine aktuelle Position im Unternehmen, seinen beruflichen Werdegang sowie Interessen auf einer sozialen Plattform bekannt gab, dort von einem ebenfalls angemeldeten Nutzer angeschrieben. Nachdem sich der spätere Geschädigte sowie dieser Nutzer eine gewisse Zeit über diverse Entwicklungen der Informatik austauschten, wurden auch Kryptowährungen thematisiert. Schließlich überzeugte der Täter den Geschädigten auf einer legitimen Plattform einen Account zu erstellen und in der Folge in die Kryptowährung „Bitcoin“ zu investieren. Weiter gab der Täter an, über Informationen zu einer „neuen und noch nicht offiziell herausgegebenen Kryptowährung“ zu verfügen. Diese könne man über die Handelsplattform, bei der der Geschädigte bereits registriert war, auf Nachfrage beim Support erwerben. Dies tat der Geschädigte und teilte dies dem Täter mit. Unmittelbar danach erhielt der Geschädigte eine E-Mail, welche vorgeblich von der Handelsplattform stammte, in der diesem eine Bitcoin-Adresse mitgeteilt wurde, an die Bitcoins transferiert werden sollen und die dann in die neue Kryptowährung getauscht werden würden. Der Geschädigte investierte in der Folge ca. 76.000 Euro in Bitcoin und übersandte diese an eine Bitcoin-Adresse der Täter.

2.3 Herausragende Fälle

Datenveränderung i. V. m. Computerbetrug

Ein Geschäftsführer eines Brandenburger Unternehmens zeigte am 14.12.2023 an, dass das geschädigte Unternehmen seit März 2023 einen Online-Ticket-Shop betreibt. Hersteller und Vertreiber der Software dieses Ticketshops ist ein externer Dienstleister. Die Bezahlung im Onlineshop erfolgt ausschließlich über einen bestimmten Finanzdienstleister, der für seine Transaktionen eine E-Mail-Adresse verwendet. Dazu wurde in die Software eine feststehende E-Mail-Adresse implementiert. Im Rahmen einer Kundenanfrage zur Rückerstattung der gezahlten Beträge wurde festgestellt, dass zu diesem Kunden kein Zahlungseingang bei der E-Mail-Adresse existent war. Bei den internen Recherchen im Zusammenhang mit den Auskünften des Kunden konnte festgestellt werden, dass dieser via den Finanzdienstleister an eine augenscheinlich ähnliche E-Mail-Adresse überwiesen hatte. Es wurde die gleiche Domain mit einer anderen Top-Level-Domain registriert. Offenbar hatten Unbekannte Zugriff auf die Software des Ticketshops erlangt und dort mehrfach und nur temporär die Zahlungs-API ausgetauscht, d.h. von der ursprünglichen E-Mail-Adresse auf die E-Mail-Adresse der Täter und wieder zurück. Die Unbekannten hatten die Domain erworben, sich über diese die ähnliche E-Mail-Adresse eingerichtet und unter Angabe dieser einen Kunden-Account beim Finanzdienstleister registriert. Auf diesen Account wurden Zahlungen von potenziellen Kunden über den manipulierten Ticketshop umgeleitet. Es entstand ein Schaden von ca. 100.000 Euro.

Ausspähen von Daten i. V. m. Erpressung

Am 19.08.2023 meldete eine große Unternehmensgruppe aus dem Land Brandenburg der ZAC des LKA den Zugang einer erpresserischen E-Mail. In der E-Mail behaupteten die Täter, Daten des Unternehmens erbeutet zu haben und diese an direkte Konkurrenz-Unternehmen versenden zu wollen. Die Unternehmensgruppe bestätigte, dass die ergänzend zur E-Mail zur Verfügung gestellten Daten empfindliche Informationen des Unternehmens sind. Auf Grund der Brisanz der Daten entschied sich das Unternehmen, die geforderte Summe zu zahlen. In der Folge teilten die Täter u. a. Daten eines Endgerätes mit, welches einer Mitarbeiterin des Unternehmens zugeordnet werden konnte. Die weiteren Ermittlungen ergaben, dass diese mit dem Endgerät aus dem Homeoffice auf das Netzwerk des Unternehmens Zugriff erlangten. Zusätzlich wurde das Endgerät aber auch von einem Kind der Mitarbeiterin verwendet, um Computerspiele zu spielen. Auf diesem Computer war allerdings zumindest zeitweise jegliche Anti-Viren-Software deaktiviert worden, um eine sog. „Cheating-Software“ ausführen zu können[6]. So konnte das System mit einer Schadsoftware infiziert werden, welche über den Computer genutzte Login-Daten ausspähte und speicherte, darunter auch Login-Informationen für die Unternehmensumgebung. Dies wurde von den Tätern zur Exfiltration der Daten genutzt.

[6] Diese ermöglicht es zwar, sich in Computerspielen einen Vorteil zu verschaffen, wird aber oftmals als Virus erkannt.

3 Prävention

Die polizeiliche Präventionsarbeit im Zusammenhang mit Cybercrime/Neue Medien richtet sich insbesondere an Kinder und Jugendliche mit dem Ziel, diese 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 2023 insgesamt 999 (2022: 568) Präventionsveranstaltungen zum Thema „Cybercrime/Neue Medien“ durch, mit denen rund 23.807 (2021: 12.778) Teilnehmerinnen und Teilnehmer erreicht wurden. Die Veranstaltungen wurden als Projekt, Vortrag und im Rahmen von Elternabenden durchgeführt. Die Schwerpunkte richteten sich nach dem Alter der Teilnehmerinnen und Teilnehmer. Somit reichten die Themen von Mobbing, Fremdenkontakt, Datendiebstahl, Viren bis hin zum Onlinebanking, gefälschten Internetseiten, Betrugsmaschen und rechtlichen Regelungen im Internet. In der Regel wurden keine Präventionsmaßnahmen durchgeführt, die sich ausschließlich der Cybercrime widmeten.

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.

Zusätzlich wurden in der Polizeiinspektion Dahme-Spree bei Aufführungen des „Seniorentheaters“ die Thematik Cybercrime als präventive Maßnahme aufgegriffen.

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[7].

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) 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.

[7] siehe auch www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

Die ZAC Brandenburg hat im Jahr 2023 insgesamt 16 Veranstaltungen (2022: 19, mit 1.800 TN) mit 1.284 Teilnehmerinnen und 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 Kriminelle 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 Entwicklungen im Rahmen der Digitalisierung der Gesellschaft, sowohl im privaten als auch kommerziellen Bereich, bedingen 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 der Studie „Wirtschaftsschutz 2023“ des Branchenverbandes Bitkom vom 01. September 2023[8] wird von einem Schaden für Unternehmen in Deutschland in Höhe von ca. 223 Mrd. EUR 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. In dieser wie auch anderen Studien ist weiterhin eine Professionalisierung der Täter offensichtlich.

Im Zusammenhang mit der Schnelllebigkeit des Kriminalitätsbereichs „Cybercrime“ erscheint seit dem 1. Quartal 2023 regelmäßig ein entsprechender polizeiinterner Monitoring-Bericht, in welchem spezifische Phänomene dargestellt und besondere Ermittlungsmaßnahmen vorgestellt werden. Dieses soll fortgeführt und bezogen auf die Phänomendarstellung stetig weiterentwickelt werden.

[8] Quelle: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf

5 Anlagen

5.1 Cybercrime

- Fallzahlenentwicklung 2019 bis 2023 (Quelle: PKS)

	2019	2020	2021	2022	2023		Veränderung
Erfasste Fälle	**2.461**	**2.323**	**2.678**	**2.640**	**2.744**	↗	***+3,9 %***
Aufklärungsquote (AQ) in %	67,9	63,1	61,8	58,2	58,9	↗	*+0,7 %-Punkte*

- Delikte im Detail:

▸ Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr b. der Datenverarbeitung (§§ 269, 270 StGB)	100	71	99	96	135	↗	*+40,6 %*
▸ Datenveränderung, Computersabotage (§§ 303a, 303b StGB)	63	68	69	78	79	↗	*+1,3 %*
▸ Ausspähen, Abfangen von Daten, einschl. Vorbereitungshandlungen und Datenhehlerei (§§ 202a-d StGB)	107	74	63	65	89	↗	*+36,9 %*
▸ Computerbetrug (§ 263a StGB)	2.186	2.102	2.447	2.401	2.441	↗	*+1,7 %*
▸ Betrügerisches Erlangen von Kfz	0	3	2	2	1	↘	*-50,0 %*
▸ Weitere Arten des Warenkreditbetruges	922	899	1.182	1.209	1.193	↘	*-1,3 %*
▸ Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	449	415	542	540	547	↗	*+1,3 %*
▸ Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	145	115	118	86	126	↗	*+46,5 %*
▸ Computerbetrug mittels rechtswidrig erlangter sonst. unbarer Zahlungsmittel	268	223	229	170	223	↗	*+31,2 %*
▸ Leistungskreditbetrug	100	175	101	107	112	↗	*+4,7 %*
▸ Computerbetrug (sonstiger)	230	223	194	175	137	↘	*-21,7 %*
▸ Missbräuchliche Nutzung von Telekommunikationsdiensten	35	8	10	18	14	↘	*-22,2 %*
▸ Abrechnungsbetrug im Gesundheitswesen	0	1	0	0	0		*0*
▸ Überweisungsbetrug	37	10	69	94	88	↘	*-6,4 %*

- Schadenssummen 2019 bis 2023 (Quelle: PKS)[9]

Jahr	Schadensfälle insgesamt	Schaden in EUR	durchschnittlicher Schaden in EUR pro Fall
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
2023	2.441	3.066.628	1.256

- Tatverdächtige 2019 bis 2023 (Quelle: PKS)

	2019	2020	2021	2022	2023		Veränderung
Tatverdächtige (insgesamt)	**1.114**	**1.108**	**1.151**	**1.097**	**1.327**	↗	***+21,0 %***
männlich	736	691	740	714	825	↗	*+15,5 %*
weiblich	378	417	411	383	502	↗	*+31,1 %*
Erwachsene	964	974	1.022	973	1.194	↗	*+22,7 %*
Heranwachsende	94	89	75	67	79	↗	*+17,9 %*
Jugendliche	47	35	43	42	50	↗	*+19,0 %*
Kinder	9	10	11	15	4	↘	*-73,3 %*
Nichtdeutsche TV	128	143	138	147	166	↗	*+12,9 %*
Anteil nichtdeutscher TV in %	11,5	12,9	12,0	13,4	12,5	↘	*-0,9 %*

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

5.2 Tatmittel Internet und/oder IT-Geräte[10]

- Fallzahlenentwicklung 2019 bis 2023 (Quelle: PKS)

	2019	2020	2021	2022	2023		Veränderung
erfasste Fälle (insgesamt)	**7.939**	**7.995**	**8.528**	**8.350**	**8.788**	↗	***+5,2 %***
Aufklärungsquote (AQ) in %	86,1	86,7	87,0	85,2	85,5	↗	*+0,3 %-Punkte*

- Schadenssummen 2019 bis 2023 (Quelle: PKS)

Jahr	Schadensfälle insgesamt	Schaden in EUR	durchschnittlicher Schaden in EUR pro Fall
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
2023	4.415	5.273.136	1.194

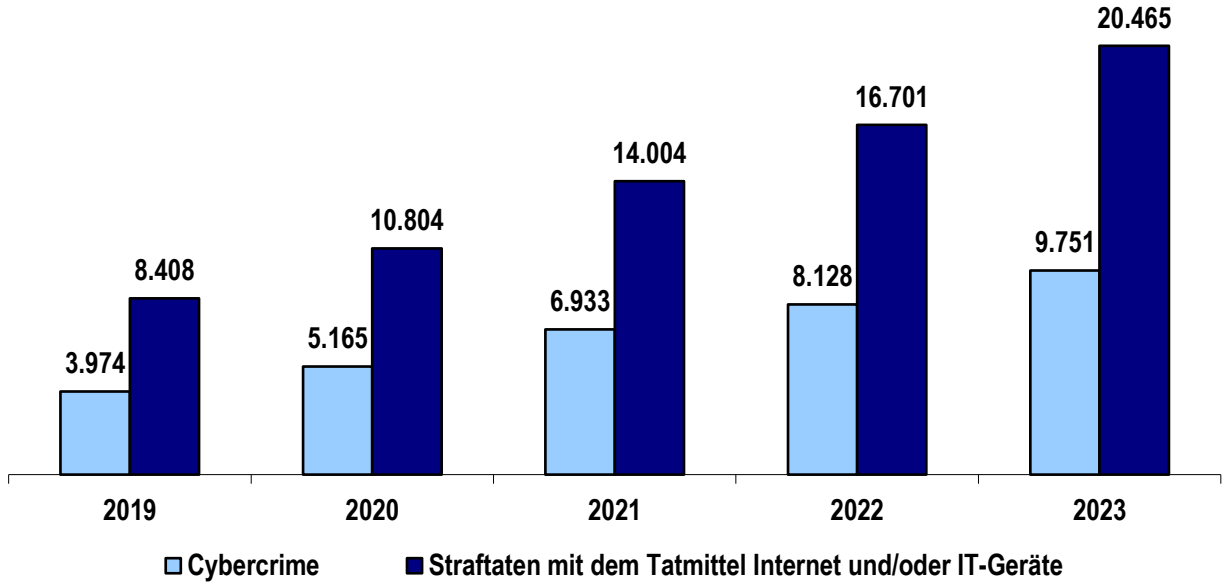
- Tatverdächtige 2019 bis 2023 (Quelle: PKS)

	2019	2020	2021	2022	2023		Veränderung
Tatverdächtige (insgesamt)	**4.646**	**5.065**	**5.574**	**5.614**	**6.191**	↗	***+10,3 %***
männlich	3.247	3.511	3.911	3.907	4.247	↗	*+8,7 %*
weiblich	1.399	1.554	1.663	1.707	1.944	↗	*+13,9 %*
Erwachsene	3.698	3.964	4.255	4.219	4.785	↗	*+13,4 %*
Heranwachsende	412	436	528	490	490	=	*0 %*
Jugendliche	394	464	555	588	625	↗	*+6,3 %*
Kinder	142	201	236	317	291	↘	*-8,2 %*
Nichtdeutsche TV	303	387	475	484	557	↗	*+15,1 %*
Anteil nichtdeutscher TV in %	6,5	7,6	8,5	8,6	9,0	↗	*+0,4 %*

[10] 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 2019/2020 sowie 2021-2023 nur eingeschränkt gegeben.

5.3 Auslandsstraftaten[11]

(Quelle: PKS-Ausland)



- Aufklärungsquoten

	2019	2020	2021	2022	2023
Cybercrime	4,6 %	3,1 %	2,8 %	2,7 %	2,7 %
Straftaten mit dem Tatmittel Internet und/oder IT-Geräte	6,8 %	7,1 %	10,1 %	9,5 %	7,5 %

[11] Auf Grund der veränderten Definition des PKS-Summenschlüssel 897000 Cybercrime (vor 2021 Computerkriminalität) wurden für die Jahre 2019 und 2020 die einzelnen PKS-Schlüssel für diesen PKS-Summenschlüssel gemäß der Richtlinie 2022 einzeln addiert, um eine Vergleichbarkeit mit den Zahlen der Jahre 2021 bis 2023 zu schaffen.