Polizeipräsidium
Land Brandenburg

Landeskriminalamt

Lagebild
Cybercrime
im Land Brandenburg
Jahr 2024

Impressum

Polizeipräsidium
Landeskriminalamt
Cyber-Competence-Center
LKA 121
Tramper Chaussee 1
16225 Eberswalde

cybercrime.lka@polizei.brandenburg.de

Trend

	2023	2024		Veränderung in Prozent
Cybercrime	**2.744**	**2.240**	↘	**-18,4 %**
Ausspähen von Daten	80	65	↘	-18,8 %
Abfangen von Daten	1	3	↗	+200,0 %
Vorbereiten des Ausspähens und Abfangens von Daten	5	2	↘	-60,0 %
Datenhehlerei	3	2	↘	-33,3 %
Fälschung beweiserheblicher Daten	129	131	↗	+1,6 %
Täuschung im Rechtsverkehr bei der Datenverarbeitung	6	5	↘	-16,7 %
Datenveränderung	62	49	↘	-21,0 %
Computersabotage	17	17	=	0 %
Computerbetrug	2.441	1.966	↘	-19,5 %
- Betrügerisches Erlangen von Kfz	1	4	↗	+300,0 %
- Weitere Arten des Warenkreditbetruges	1.193	882	↘	-26,1 %
- Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	547	486	↘	-11,2 %
- Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	126	86	↘	-31,8 %
- Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel	223	147	↘	-34,1 %
- Leistungskreditbetrug	112	94	↘	-16,1 %
- Computerbetrug (sonstiger)	137	164	↗	+19,7 %
- Missbräuchliche Nutzung von Telekommunikationsdiensten	14	13	↘	-7,1 %
- Abrechnungsbetrug im Gesundheitswesen	0	0	=	0 %
- Überweisungsbetrug	88	90	↗	+2,3 %
Delikte mit Tatmittel Internet und/oder IT-Geräte (insg.)	**8.788**	**9.053**	↗	**+3,0 %**

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. 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 und der Erfolg der Handlung (Erfolgseintritt) in Deutschland eingetreten ist. Seit 2024 erfolgt diese Darstellung von sogenannten Auslandsstraftaten auf Basis eines bundeseinheitlichen Straftatenkatalogs. So wurden unter anderem Fälle ausgeschlossen, die auf Grund der Deliktsbeschaffenheit bei einem Handlungsort im Ausland zwingend den Erfolgsort auch im Ausland haben müssen und folglich weder in der PKS-Inland noch in der PKS-Ausland auftauchen. Entscheidend für die Erfassung eines Falls in die PKS-Inland oder PKS-Ausland ist, neben dem zumindest teilweise in Deutschland befindlichen Erfolgsort, der Handlungsort der Täter. Ist der Handlungsort der Täter innerhalb Deutschlands, dann erfolgt die Erfassung in der PKS-Inland. Ist es hingegen nicht möglich den Handlungsort der Täter in Deutschland zuzuordnen, dann erfolgt die Erfassung in der PKS-Ausland. Dies ist dabei unabhängig, ob die Handlung nachweislich im Ausland stattgefunden hat oder der Handlungsort unbekannt ist. Eine Summierung von Inlands- und Auslandstaten ist aktuell nicht zulässig. Um jedoch eine Vergleichbarkeit dieses Lagebild hinsichtlich der Auslandsstraftaten mit den vergangenen Berichtsjahren gewährleisten zu können, wurden auch für die vergangenen Vergleichsjahre nur die Delikte dargestellt, die dem Katalog entsprachen. In der Vergangenheit wurden in den Lagebildern sämtlichen Auslandstaten darstellt, weshalb es zu leichten Abweichungen gegenüber den Lagebildern der letzten Berichtsjahre kommt.

Die Unabhängigkeit des Erfolgsortes einer Tat vom Handlungsort der Täter ist vor allem beim Cybercrime-Delikten gegeben.

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-Inland für das Jahr 2024 erfassten Straftaten, die sich gegen das Internet, weitere Datennetze, IT-Systeme oder deren Daten richten, ist gegenüber dem Vorjahr deutlich um 18,4 % auf 2.240 Fälle (2023: 2.744 Fälle) gefallen.

Hinsichtlich der Gesamtsumme des Computerbetruges (PKS-Summenschlüssel 897100) ergibt sich ein Rückgang um 19,5 % auf 1.966 Fälle (2023: 2.441 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: 72 Fälle (-19,1 %, -17 Fälle),
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung: 136 Fälle (+0,7 %, +1 Fall),
- Datenveränderung, Computersabotage: 66 Fälle (-16,5 %, -13 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 und/oder IT-Geräte enthalten.

Bei den registrierten Schäden der Cybercrime ist im Jahr 2024 ein Rückgang um 19,6 % auf 2.466.109 Euro zu verzeichnen (2023: 3.066.628 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.

Die Zahl der bei den erfassten Fällen von Cybercrime ermittelten Tatverdächtigen (TV) fiel von 1.327 TV (Vorjahr) auf 1.134 TV. Personen über 21 Jahre stellen mit einem Anteil von 86,7 % bzw. 984 TV (2023:

90,0 %, 1.194 TV) trotz leichtem Rückgang weiterhin die anteilig größte Gruppe unter den TV dar. Der Anteil nichtdeutscher TV beträgt 17,0 % bzw. insgesamt 193 TV (Vorjahr 12,5 % bzw. 166 TV).

Im Phänomenbereich Cybercrime wurden im Berichtsjahr 10.465 Auslandsstraftaten und somit 714 Straftaten (7,3 %) mehr als im Vorjahr (9.751) polizeilich registriert. Somit haben etwa 82,4 % (2023: 78,0 %) 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-Erfassungsbeleg-Straftat innerhalb des Vorgangsbearbeitungssystems durch die jeweilige kriminalpolizeiliche Sachbearbeitung 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 2024 wurden in der PKS-Inland insgesamt 9.053 Fälle erfasst, die unter Nutzung des „Tatmittels Internet und/oder IT-Geräte“ begangen wurden. Im Vergleich zum Vorjahr stellt dies einen Anstieg um 265 Fälle bzw. 3,0 % dar. Überwiegend handelte es sich dabei trotz deutlichen Rückgangs um Fälle des Waren-/Warenkreditbetruges (2.598 Fälle, -576 Fälle oder -18,2 %) sowie des Computerbetruges[2] (1.302 Fälle, -371 Fälle oder -22,2 %).

Die polizeilich erfasste Gesamtschadenssumme (Schaden gemäß PKS-Inland) hat sich von 5.273.136 Euro auf 8.608.554 Euro bzw. um 63,3 % gesteigert.

Im Berichtszeitraum wurden zu den Straftaten mit dem „Tatmittel Internet und/oder IT-Geräte“ 6.735 TV und somit 544 TV (+8,8 %) mehr als in 2023 ermittelt. Knapp die Hälfte dieses Anstiegs fällt auf die erwachsenen TV, welche um 271 auf nunmehr 5.056 TV angestiegen sind. Die Zahl der Heranwachsenden bleibt mit 507 (Vorjahr: 490) nahezu identisch. Die Anzahl der tatverdächtigen Kinder und Jugendlichen hingegen stieg deutlich auf 414 TV (+123 TV) bzw. 758 TV (+133 TV) an. Insgesamt bilden die Erwachsenen mit 75,1 % (5.056 TV) weiterhin die anteilig größte Gruppe unter den TV, wenn auch der Anteil der Kinder und Jugendlichen stark zugenommen hat.

Zu den Straftaten mit dem „Tatmittel Internet und/oder IT-Geräte“ wurden im Jahr 2024 insgesamt 790 nichtdeutsche TV und damit 233 mehr als im Vorjahr erfasst.

Im Berichtsjahr wurden in der PKS-Ausland 19.831 Straftaten mit dem „Tatmittel Internet und/oder IT-Geräte“ registriert. Damit ist das Fallaufkommen gegenüber dem Vorjahr (2023: 20.331 Fälle[3]) um 500

[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 1.966 Fälle (Punkte 2.1.1).

[3] Die Darstellung von sogenannten Auslandsstraftaten erfolgt ab dem Jahr 2024 aus Basis eines bundeseinheitlichen Katalogs. Um eine Vergleichbarkeit dieser Statistik mit den vergangenen Jahren gewährleisten zu können, erfolgt hier auch die

Fälle (-2,5 %) gesunken. Insgesamt entspricht dies einem Anteil von 68,7 % (Vorjahr 69,8 %) 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 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, wofür ein Phänomenkatalog inklusive entsprechender Definitionen eingeführt wurde:

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

Voraussetzung für eine Erfassung ist, dass diese durch die Sachbearbeitung erkannt und entsprechend markiert werden. Die Zuordnung erfolgt im POLAS-Beleg und ist unabhängig vom jeweiligen Delikt.

Im Berichtsjahr wurden fünf Fälle dem Phänomen (D)DoS-Attacke, 7.259 Fälle dem Phänomen „digitaler Identitätsdiebstahl/ Accountübernahme“, 153 Fälle als „Eindringen in Datennetze/Datenveränderung/Datendiebstahl bei nichtnatürlichen Personen“, 1.648 Fälle dem Phänomen „Angriff auf das Online-Banking“ sowie 114 Fälle als „Ransomware“ zugeordnet.

2.2 Aktuelle Begehungsweisen und Phänomene

2.2.1 Diebstahl digitaler Identitäten und Identitätsmissbrauch

Die digitale Identität[4] 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 durch Datenabfluss nach einem Angriff auf Online-Plattformen statt. Der Identitätsdiebstahl stellt regelmäßig die vorbereitende Einstiegshandlung für die Begehung weiterer Straftaten der Cybercrime und

Darstellung der Auslandsstraftaten für die Jahre davor gemäß diesem Katalog. In der Vergangenheit wurden in den Lagebildern sämtlichen Auslandstaten darstellt, weshalb es zu leichten Abweichungen gegenüber den Lagebildern der letzten Berichtsjahre kommt.

[4] 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.

anderer Delikte dar (z. B. betrügerische Warenbestellungen, missbräuchliche Verwendung von Kreditkartendaten, Versendung von Schadsoftware, DDoS-Attacken zum Nachteil von Unternehmen, Behörden und Einrichtungen etc.). Neben der digitalen Identität einer natürlichen Person, werden auch die „Identitäten“ von juristischen Personen, wie Unternehmen, Vereinen oder anderen Institutionen, missbräuchlich verwendet.

Weiterhin auf hohen Niveau sind Warenkreditbetrugshandlungen nach vorherigem Ausspähen von Zugangskennungen. Insbesondere bei E-Mail-Dienstleistern und Onlinehändlern bzw. Zahlungsdienstleistern werden die Accounts von Geschädigten durch Dritte übernommen oder deren komplette Identität verwendet, um neue Accounts bei Verkaufs- und Finanzdienstleistungsplattformen anzulegen.

Bei einem anderen vermehrt auftretenden Phänomen wird die Verwendung von eigenen Zahlungsprozessen von Online-Verkaufsplattformen für die Bezahlung von Gütern, welche über diese Plattform verkauft wurden, ausgenutzt. Dabei wird den Geschädigten suggeriert, dass diese zur Bezahlung der erworbenen Güter Ihre Kreditkartendaten eingeben müssen. Tatsächlich übersenden die Täter jedoch einen Link zu einer täuschend ähnlich gestalteten Webseite und die Geschädigten geben die entsprechenden Daten im Glauben, damit die Güter zu bezahlen, ein. Die Daten verwenden die Täter ihrerseits um Güter im Internet zu erwerben und diese an so genannte Warenagenten liefern zu lassen.

Ferner werden die erlangten Daten auch über illegale „Marktplätze“ und Foren der sogenannten Underground Economy mit 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 weiterer Modus Operandi ist die Darstellung einer vermeintlichen Warnmeldung auf dem Computer, bei welchem dem Anwender suggeriert wird, dass sich eine Schadsoftware auf dessen IT-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. Diese Zugangsdaten werden in der Folge durch die Täter unberechtigt bei der Ausübung weiterer Straftaten eingesetzt.

Vermehrt wurden im Berichtsjahr Sachverhalte festgestellt, bei denen Unternehmensdaten mutmaßlich aus dem Handelsregister entnommen wurden und diese dann auf so genannten „Fake-Webseiten", in der Regel Online-Shops, angegeben wurden, um eine gewisse Legitimität zu suggerieren. Die Namen der Webseiten ähnelten in vielen Fällen den tatsächlichen Unternehmensnamen oder wurden exakt gewählt, sofern das Unternehmen keine eigene Domain unter der Bezeichnung betrieb. Zusätzlich wurden diese Online-Shops teilweise mit der deutschen Top-Level-Domain-Endung „.de" betrieben, um eine höhere Vertrauenswürdigkeit zu erwecken.

Wie auch im Jahr 2023 wurden zunehmend Fälle registriert, bei denen Täter bereits gestellte Rechnungen durch „neue" Bankdaten[5] abänderten (sog. Payment-Diversion-Fraud). Die Täter erlangen dabei Zugriff auf die interne Kommunikation der Geschädigten, indem sie z. B. einen E-Mail-Account „übernehmen" oder sie nutzen marginal veränderte E-Mail-Adressen, um die Geschädigten zu kontaktieren und dabei eine Kommunikation mit dem eigentlichen Geschäftspartner vorzutäuschen.

Beispielfall
Am 02.01.2024 erstattete die geschädigte Firma Strafanzeige gegen unbekannte Täter. Demnach führte das Unternehmen längerfristige Geschäftsbeziehungen mit einem Unternehmen aus Saudi-Arabien. In diesem Zusammenhang stellte das Brandenburger Unternehmen auch digitale Rechnungen an den ausländischen Geschäftspartner aus. Dieser wandte sich an das hiesige Unternehmen, als dort eine E-Mail einging, in welcher die Änderung der Bankverbindung des Unternehmens bekannt gegeben wurde. Die E-Mail wurde von einer E-Mail-Adresse versandt, die bis auf einen Buchstaben der Domain des geschädigten Unternehmens glich. Das saudi-arabische Partnerunternehmen erkannte dies zunächst nicht, erkundigte sich aber beim hier ansässigen Unternehmen nach der Korrektheit diese Änderung, wodurch der Sachverhalt bekannt wurde. Ein finanzieller Schaden ist nicht entstanden.

Beispielfall:
Ein Brandenburger Unternehmen meldete sich bei der ZAC und gab an, dass diese durch ein anwaltliches Schreiben darauf aufmerksam gemacht wurden, dass augenscheinlich ein Online-Shop unter dem Firmennamen betrieben werde. Zusätzlich war im Impressum des Shops die Anschrift des Unternehmens, die Erreichbarkeiten und der Name des Geschäftsführers angegeben. Das Unternehmen selbst betrieb jedoch keine eigene Webseite und war auch in einer anderen Branche tätig. Das Unternehmen erstattete daraufhin Anzeige. Die Ermittlungen ergaben, dass Kunden auf der Webseite Waren erworben und bezahlt hatten, diese jedoch tatsächlich nie erhielten. In der Folge schaltete einer der offensichtlich betrogenen Kunden einen Rechtsbeistand ein, welcher die hier geschädigte Firma informierte. Die Ermittlungen zur in Deutschland registrierten „.de"-Domain ergaben, dass diese auf eine augenscheinlich im osteuropäischen Raum agierende Person registriert war.

[5] Diese „neuen" Bankverbindungen, zu inländischen und ausländischen Banken, sind in der Regel Finanzagentinnen und -agenten zuzuordnen.

2.2.2 Angriffe auf das Online-Banking

Im Berichtszeitraum war eine überwiegend gleichbleibende Anzahl von Angriffen auf das Online-Banking zu verzeichnen. Dies kann u. a. mit der Zunahme und besseren Ausgestaltung von Sicherungssystemen der Banken zusammenhängen.

Auf ähnlich hohem Niveau gegenüber dem Vorjahr sind die Fälle der Betrugsmasche „Support eines Betriebssystemherstellers“ geblieben. Die Geschädigten erhielten Anrufe von Tätern oder wurden durch Einblendungen von sog. „Pop-Up“-Fenstern auf dem Computerbildschirm dazu animiert, eine telefonische Verbindung aufzubauen. Die jeweiligen „Gesprächspartner“ stellten sich als „Support-Mitarbeiter“ vor, die bei der Behebung der angeblichen Störung oder des “Schadsoftwarebefalls“ behilflich wären. 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, um unautorisierte Überweisungen vorzunehmen.

Weiterhin trat das Phänomen des unautorisierten Stromanbieterwechsels auf. Hierbei waren die Täter vorgeblich als „Subunternehmer für Stromanbieter“ tätig und gelangten über Gemeinschaftsstromzähler an die Daten der Geschädigten. In der Folge wurden widerrechtlich neue Stromverträge im Namen der Geschädigten online abgeschlossen. Die (Wechsel)Provisionen dafür ließen sich die Täter selber auszahlen. Die Geschädigten stellten erst anhand 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.

Die Anzahl der Fälle, bei denen Kryptowährungen zumeist als Auszahlungsmedium nach Fremdkontennutzung verwendet wurden, hat sich nach hiesiger Einschätzung erhöht. Dies ist auf Wahrnehmungen im Rahmen des täglichen Dienstgeschäftes und bei Erfahrungsaustauschen mit den bearbeitenden Dienststellen zu stützten, kann aber anhand der polizeilichen Auskunftssysteme nicht valide nachvollzogen werden[6].

[6] Dies liegt vornehmlich in fehlenden Katalogwerten zu Kryptowährungen und in der Erfassungspraxis begründet.

Weiter gelang es den Tätern auch zusätzliche Sicherungsmethoden, wie die Zwei-Faktor-Authentifizierung, zu umgehen. So wurden Fälle bearbeitet, bei denen es den Tätern zunächst gelang, die Zugangsdaten für das Online-Banking auszuspähen. In der Folge beantragten die Täter dann einen Wechsel vom TAN-Generator zu einer TAN-App. Die App wurde dann auf einem von den Tätern verwendeten Endgerät installiert, mit dem Banking-Account verknüpft und schließlich zur Autorisierung von unberechtigten Transaktionen verwendet.

2.2.3 Digitale Erpressung unter Einsatz sogenannter „Ransomware“

Die digitale Erpressung unter Einsatz sogenannter „Ransomware“[7] 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.

Neben der Verschlüsselung von Daten werden diese bei einer Vielzahl an Ransomware-Varianten vor der Verschlüsselung zunächst auf Server ausgeleitet und mit der Veröffentlichung dieser gedroht. Für die Veröffentlichung dieser Daten betreiben die meisten Ransomware-Gruppierung so genannte „Dedicated Leak Site“ (DLS) im Darknet und/oder Clearnet.

[7] 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. Zur Entschlüsselung oder Freigabe des Computersystems wird der Betroffene aufgefordert, einen bestimmten Betrag in einer vorgegebenen Kryptowährung (z. B. Bitcoin) zu bezahlen. In vielen Fällen wurden durch die Schadsoftware auch (Firmen-)Daten an die Täter übertragen. Bei Nichtbezahlung wird zusätzlich mit deren Veröffentlichung gedroht.

Im Bereich der Privatpersonen wurde diese Art der digitalen Erpressung im Land Brandenburg bisher 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 fehlerhafter Interpretationen der Definition zum Phänomen „Ransomware“ zugeordnet.

Es ist weiterhin davon auszugehen, dass das Dunkelfeld in diesem Bereich sehr groß ist, weil Unternehmen zunächst an der Wiederherstellung der Arbeitsfähigkeit interessiert sind und eine möglichen Rufschädigung durch Bekanntwerden des Vorfalls vermeiden wollen[8].

Beispielfall:
Am 23.02.2024 meldete sich der Geschäftsführer eines Brandenburger Unternehmens und gab an, dass dessen IT-Infrastruktur verschlüsselt sei. Weiterhin hatte das Unternehmen bereits vor der Kontaktaufnahme mit der Polizei Kontakt mit den Tätern aufgenommen. Gegen eine Zahlung von ca. 3.000 Euro in der Kryptowährung Bitcoin übersandten die Täter dem geschädigten Unternehmen das entsprechende Entschlüsselungstool. Darüber hinaus teilten die Täter mit, dass diese über eine offene RDP-Verbindung (Remote-Desktop-Protokoll) sowie der Verwendung eines „unsicheren“ Passwortes Zugriff auf die IT-Infrastruktur erhielten. Die Ermittlungen führten zur Identifizierung einer Person, deren Aufenthaltsort unbekannt und die auch bereits durch andere Staaten zur Fahndung ausgeschrieben ist.

Beispielfall
Im Rahmen des polizeilichen Informationsaustausches am 29.07.2024 wurde bekannt, dass ein Brandenburger Unternehmen möglicherweise Opfer eine Ransomware-Gruppierung geworden sei. Die unmittelbare Kontaktaufnahme mit dem geschädigten Unternehmen bestätigt dies. Demnach wurden am 18.07.2024 mehrere interne Server verschlüsselt und darüber hinaus ca. 200 GB an Daten extrahiert. In der Folge wurde das Unternehmen erpresst, ein Lösegeld von 100.000 US-Dollar zu zahlen, andernfalls würden die extrahierten Daten veröffentlicht werden. Das Unternehmen entschloss sich dieser Forderung nicht nachzukommen, da es sich u. a. bei den verschlüsselten Daten um Testdatensätze handelte, welche zu dem auch aus Backups wiederhergestellt werden konnten. Darüber hinaus gab das Unternehmen bekannt, dass der Einfallsvektor auf zwei bekannte Sicherheitslücken zurückgeführt wurde.

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. Vor allem das Ausnutzen von sog. Zero-Day-Sicherheitslücken[9] birgt dabei ein großes Schadenspotential.

[8] Diese Erkenntnis stammt vor allem aus Erfahrungen im Zusammenhang mit dem Monitoring der oben genannten DLS der Ransomware-Gruppierungen. Nach einer solchen Veröffentlichung trat die ZAC-Dienststelle regelmäßig proaktiv an die Unternehmen heran. Zwar hatten die Unternehmen für gewöhnlich Kenntnis von diesem IT-Sicherheitsvorfall, aber (noch) keinen Kontakt zu den Strafverfolgungsorganen aufgenommen.
[9] 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.

Beispielfall
Am 25.01.2024 meldete sich ein Verantwortlicher einer städtischen Wohnungsgesellschaft bei der ZAC Brandenburg und gab an, dass diese Opfer einer Bot-Attacke geworden seien. Demnach wurde das Kontaktformular der Webseite innerhalb von zwei Stunden ca. 90.000 Mal versendet. Im Kontaktformular wurden wechselnde E-Mail-Adressen sowie ein stets gleichlautender Text, inkl. eines Links, eingetragen. Die Handlung erfolgte sehr wahrscheinlich mit Hilfe eines Skriptes mit dem die implementieren SPAM-Schutz-Maßnahmen umgangen werden konnten. Dies erfolgte durch das wiederholte Ausführen des Senden-Befehls (POST-Request). Weiter machten die Täter sich den Umstand zunutze, dass eine Bestätigungs-E-Mail der geschädigten Gesellschaft an die angegebene E-Mail-Adresse versendet wird. So gelang es den Tätern ca. 90.000 E-Mail-Empfängern, eine mutmaßlich unerwünschte E-Mail zukommen zu lassen. Der Aufruf der Webseite erfolgte über eine IP-Adresse. Diese konnte einem VPN-Dienstleister zugeordnet werden, welcher jedoch keinerlei Daten zu seinen Kunden speichert.

Beispielfall:
Am 21.02.2024 meldete sich der IT-Administrator einer Brandenburger Gemeinde bei der ZAC und gab an, dass unbekannte Täter sich Zugriff auf einen E-Mail-Server der Gemeinde verschafften und im Anschluss SPAM-E-Mails versendeten. Die Ermittlungen ergaben, dass es den Tätern gelang, die Zugangsdaten eines Mitarbeitenden auszuspähen und in der Folge zu nutzen. Dies erreichten sie, indem sie von einer ebenfalls übernommenen E-Mail-Adresse eine E-Mail an eine Vielzahl an Mitarbeitenden der Gemeinde sandten. Inhaltlich gaben Sie dabei an, dass eine neue Version des E-Mail-Programms eingeführt werden würde und daher der Mitarbeitende den beigefügten Link aufrufen müsse. Dieser Link führte zu einer Anmeldemaske, welche unter der Kontrolle der Täter stand. Sofern ein Mitarbeitender nun dort seine Zugangsdaten eingab, konnten diese durch die Täter mitgelesen und im Nachgang verwendet werden.

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 Unternehmen, z.B. im Namen des Geschäftsführers, kontaktiert und um Übermittlung der aktuellen Aufträge gebeten. Ausgehend von diesem Grundkonstrukt werden unterschiedliche Modi 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. Weiter wurden Sachverhalte bekannt, bei denen E-Mails im Namen von Mitarbeitenden eines Unternehmens an die jeweiligen Personalverwaltungen mit der Bitte geschrieben wurden, die dort hinterlegten Bankdaten für die Gehaltszahlungen anpassen zu wollen.

Beispielfall
Ein Brandenburger Amt stellte am 05.03.2024 Strafanzeige, nachdem feststellt wurde, dass unbekannte Täter eine veränderte Rechnung übersandten. Demnach erhielt der verantwortliche Sachbearbeitende des Amts digital eine Rechnung, nachdem eine vorher vereinbarte Dienstleistung erbracht wurde. Kurze Zeit später erhielt der Sachbearbeitende vom identischen Absender erneut eine E-Mail mit einer digitalen Rechnung, jedoch mit der veränderten Bankverbindung. Innerhalb der E-Mail wurde die Änderung der Bankverbindung ebenfalls angegeben. In der Folge wurde der Betrag an die neue Bankverbindung durch die zuständige Stelle im Amt zahlbar gemacht. Der Betrug fiel erst auf, als der Dienstleister sich nach der Bezahlung erkundigte. Den Tätern war es offensichtlich gelungen, Zugriff auf das E-Mail-Postfach des Dienstleisters zu erhalten und konnte so die zweite E-Mail mit der veränderten Bankverbindung an das Amt übersenden.

Beispielfall
Die Personalleiterin eines in Brandenburg ansässigen Unternehmens erhielt eine E-Mail vorgeblich vom Betriebsleiter mit der Anfrage, ob vor der nächsten Gehaltsauszahlung noch eine Änderung seiner Bankdaten möglich wäre, da bei diesem ein Bankwechsel stattgefunden habe. Die Personalleiterin teilte darauf den Prozess mit und bemerkte dann, dass die E-Mail-Adresse ungewöhnlich war und kontaktierte den Betriebsleiter direkt. Dieser bestätigte den Betrugsverdacht.

2.2.6 weitere 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[10].

2.3 Herausragende Fälle

Vorbereiten des Ausspähens von Daten bei einem Krankenhaus-Verbund

Am 26.02.2024 meldete sich der IT-Verantwortliche eines Krankenhaus-Verbundes und teilte mit, dass es an zwei Firewall-Standorten zu ungewöhnlichen Anmeldeversuchen bei den dort betriebenen VPN-Portalen gekommen sei. Bei den Versuchen werden sowohl die Namen von ehemaligen, als auch derzeitigen Mitarbeitenden verwendet. Jedoch verwenden die Angreifer die falsche Syntax, sodass bereits aus diesem Grund eine Anmeldung erfolglos war. Ermittlungen hinsichtlich der Täter ergaben, dass der überwiegende Anteil der Zugriffsversuche aus dem TOR-Netzwerk stammte. Darüber hinaus gab es Zugriffsversuche über IP-Adressen, die VPN-Dienstleistern zugeordnet werden konnten. Im engen Austausch mit dem IT-Verantwortlichen wurden weitere Härtungsmaßnahmen, wie die Unzulässigkeit der Anmeldung aus dem TOR-Netzwerk, besprochen und durch den IT-Verantwortlichen konfiguriert.

Computersabotage bei einem Landkreis

Seit dem 19.07.2024 wurden Teile der IT-Infrastruktur eines Landkreises mittels einer DDoS-Attacke angegriffen. In der Folge ist es dann zu einem Funktionsausfall eines Web-Servers gekommen. Weiter wurde bekannt, dass der in Rede stehende Web-Server für Anhörungsbögen von Verkehrsordnungswidrigkeiten verwendet wird. Die Ermittlungen ergaben, dass der DDoS-Angriff höchstwahrscheinlich von einem so genannten Botnet ausgeführt wurde. Darüber hinaus wurde ein Angriffsmuster eines so genannten Brute-Force-Angriffs festgestellt, bei dem systematisch Zugangsdaten ausprobiert werden. Der Angriff richtete sich gegen die Zugänge für die Anhörungsbögen. Nach Auswertung der Protokolldateien und Rücksprache mit den Verantwortlichen wurde bekannt, dass die Syntax der Anmeldeversuche nicht korrekt war und darüber hinaus, die Zugänge immer nur für einen kurzen Zeitraum aktiv sind. Da die Zugriffsversuche konstant hochblieben, wurden in Absprache mit der Sachbearbeitung weitere Härtungsmaßnahmen an dem Server sowie der Firewall durchgeführt und dadurch die unerwünschten Zugriffsversuche minimiert. Anfang August teilte der Landkreis dann mit, dass die Zugriffsversuche sich nunmehr auch auf zwei weitere Server erstrecken, diese aber auf Grund der veränderten Firewall-Konfigurationen nicht beeinflusst wurden. Die weiteren Ermittlungen zu den anfragenden IP-Adressen ergaben, dass diese sehr wahrscheinlich durch einen entsprechenden Dienstleister verwendet werden, der seinen Dienst (Aufruf einer Webseite durch eine Vielzahl an Endgeräten) gegen Bezahlung im Internet anbietet. Der genaue Hintergrund des Angriffs konnte mangels vorhandener Forderung nicht ermittelt werden.

Datenveränderung und Betrug bei einem Bau-Unternehmen

Ein in Brandenburg ansässiges Bau-Unternehmen war mit Teilaufträgen bei einer größeren Baustelle in Berlin betraut. In diesem Zusammenhang hat das geschädigte Unternehmen eine Rechnung an das für die Buchungen zuständige Unternehmen bei dem in Rede stehenden Projekt versendet. Nach dem

[10] Für eine dezidierte Darstellung dieses Phänomens wird auf das Lagebild Wirtschaftskriminalität 2024 verwiesen.

beim geschädigten Unternehmen keine Zahlung einging, erkundigte sich das Unternehmen bei den Verantwortlichen. Dabei stellte sich heraus, dass dort eine zweite aktualisierte Rechnung eingegangen sowie die Zahlung bereits ausgelöst sei. Es entstand ein finanzieller Schaden von ca. 850.000 Euro. Die Ermittlungen ergaben, dass beim Buchungsunternehmen drei Tage nach dem Erhalt der korrekten Rechnung eine verfälschte Rechnung einging. Diese wurde augenscheinlich von einer ebenfalls dem Unternehmen zugeordneten E-Mail-Adresse versandt. Etwaige unautorisierte Zugriffe konnten jedoch nicht festgestellt werden. Ob es tatsächlich einen unberechtigten Zugriff auf die in Rede stehende E-Mail-Adresse gab, konnte nicht abschließend geklärt werden. Die Gelder wurden auf ein deutsches Bankkonto transferiert. Der Inhaber ist amtlich in Deutschland gemeldet und bereits mehrfach polizeilich bekannt.

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 2024 insgesamt 837 (2023: 999) Präventionsveranstaltungen zum Thema „Cybercrime/Neue Medien“ durch, mit denen rund 20.554 (2021: 23.807) Teilnehmerinnen und Teilnehmer erreicht wurden. Die Veranstaltungen wurden als Projekt, als 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 wurde 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[11].

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.

[11] Siehe auch www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

Die ZAC Brandenburg hat im Jahr 2024 insgesamt 15 Veranstaltungen (2023: 16, mit 1.284 TN) mit 1.259 Teilnehmerinnen und Teilnehmern mittels Vorträgen zu aktuellen Aspekten der Cybersicherheit und Verhaltensempfehlungen begleitet durch 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.

Wie schon im Jahr zuvor stellen vor allem Ransomware-Angriffe ein erhebliches Risiko für Unternehmen und Behörden dar. Besonders im Bereich Klein- und Mittelständischen Unternehmen (KMU) stellen diese Angriffe die Betroffenen vor große Herausforderungen. Hintergrund hierbei sind oftmals gar nicht oder nur unzureichend abgesicherte oder gewartete Hard- und Softwarelösungen. Dazu kommen in vielen Fällen nur unzureichend geschulte Administratoren bzw. Mitarbeitende im Umgang mit IT-Endgeräten. Wenngleich ein Trend der nachlassenden Zahlungsbereitschaft zu erkennen ist, muss hier weiterhin auf Aufklärung und Prävention gesetzt werden, um vor allem die besonders gefährdeten Unternehmen besser auf solche Angriffe vorzubereiten bzw. zu schützen. Auch zeigten Exekutivmaßnahmen der Strafverfolgungsbehörden durchaus ihre Wirkung, da im Nachgang zumindest vorübergehend die Aktivitäten der betroffenen Ransomware-Gruppierungen minimiert wurden und in einigen Fällen auch nicht mehr auftraten.

Im privaten Bereich ist das Phänomen des sogenannten „Cybertrading“ relevant. Hier werden vor allem technisch eher weniger versierte und meist ältere Bürgerinnen und Bürger durch Werbe-Anzeigen oder gezieltes Ansprechen in Sozialen Medien dazu gebracht, zunächst kleinere in der Folge immer größere Summen in Kryptowährungen zu investieren. Diesem Phänomen ist nach hiesiger Einschätzung besonders präventiv zu entgegnen.

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. Dieser soll fortgeführt und bezogen auf die Phänomendarstellung stetig weiterentwickelt werden.

Zukünftig wird vor allem die Umsetzung der NIS-2-Richtlinie für Unternehmen relevant werden. Welche konkreten Auswirkungen dies auf die alltägliche Polizeiarbeit haben wird, bleibt abzuwarten.

Weiter wird das Support-Ende von einem der weitverbreitetsten Betriebssystem-Versionen im Oktober 2025 mutmaßlich zu einer gesteigerten Ausnutzung von dann möglicherweise auftretenden Schwachstellen führen.

5 Anlagen

5.1 Cybercrime

- Fallzahlenentwicklung 2020 bis 2024 (Quelle: PKS)

	2021	2022	2023	2024		Veränderung
Erfasste Fälle	**2.678**	**2.640**	**2.744**	**2.240**	↘	***-18,4 %***
Aufklärungsquote (AQ) in %	61,8	58,2	58,9	58,2	↘	*-0,7 %-Punkte*

- Delikte im Detail:

▸ Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr b. der Datenverarbeitung (§§ 269, 270 StGB)	99	96	135	136	↗	*+0,7 %*
▸ Datenveränderung, Computersabotage (§§ 303a, 303b StGB)	69	78	79	66	↘	*-16,5 %*
▸ Ausspähen, Abfangen von Daten, einschl. Vorbereitungshandlungen und Datenhehlerei (§§ 202a-d StGB)	63	65	89	72	↘	*-19,1 %*
▸ Computerbetrug (§ 263a StGB)	2.447	2.401	2.441	1.966	↘	*-19,5 %*
▸ Betrügerisches Erlangen von Kfz	2	2	1	4	↗	*+300,0 %*
▸ Weitere Arten des Warenkreditbetruges	1.182	1.209	1.193	882	↘	*-26,1 %*
▸ Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	542	540	547	486	↘	*-11,2 %*
▸ Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	118	86	126	86	↘	*-31,8 %*
▸ Computerbetrug mittels rechtswidrig erlangter sonst. unbarer Zahlungsmittel	229	170	223	147	↘	*-34,1 %*
▸ Leistungskreditbetrug	101	107	112	94	↘	*-16,1 %*
▸ Computerbetrug (sonstiger)	194	175	137	164	↗	*+19,7 %*
▸ Missbräuchliche Nutzung von Telekommunikationsdiensten	10	18	14	13	↘	*-7,1 %*
▸ Abrechnungsbetrug im Gesundheitswesen	0	0	0	0		*0*
▸ Überweisungsbetrug	69	94	88	90	↗	*+2,3 %*

- Schadenssummen 2020 bis 2024 (Quelle: PKS)[12]

Jahr	Schadensfälle insgesamt	Schaden in EUR	durchschnittlicher Schaden in EUR pro Fall
2021	2.447	2.578.011	1.054
2022	2.401	2.386.503	994
2023	2.441	3.066.628	1.256
2024	1.966	2.466.109	1.254

- Tatverdächtige 2021 bis 2024 (Quelle: PKS)

	2021	2022	2023	2024		Veränderung
Tatverdächtige (insgesamt)	**1.151**	**1.097**	**1.327**	**1.134**	↘	***-14,5 %***
männlich	740	714	825	713	↘	*-13,6 %*
weiblich	411	383	502	421	↘	*-16,1 %*
Erwachsene	1.022	973	1.194	987	↘	*-17,3 %*
Heranwachsende	75	67	79	85	↗	*+7,6 %*
Jugendliche	43	42	50	55	↗	*+10,0 %*
Kinder	11	15	4	10	↗	*+150,0 %*
Nichtdeutsche TV	138	147	166	193	↗	*+16,3 %*
Anteil nichtdeutscher TV in %	12,0	13,4	12,5	17,0	↗	*+4,5 %-Punkte*

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

5.2 Tatmittel Internet und/oder IT-Geräte[13]

- Fallzahlenentwicklung 2020 bis 2024 (Quelle: PKS)

	2021	2022	2023	2024		Veränderung
erfasste Fälle (insgesamt)	**8.528**	**8.350**	**8.788**	**9.053**	↗	***+3,0 %***
Aufklärungsquote (AQ) in %	87,0	85,2	85,5	87,5	↗	*+2,0 %-Punkte*

- Schadenssummen 2020 bis 2024 (Quelle: PKS)

Jahr	Schadensfälle insgesamt	Schaden in EUR	durchschnittlicher Schaden in EUR pro Fall
2021	5.033	4.813.940	956
2022	4.502	5.355.108	1.189
2023	4.415	5.273.136	1.194
2024	4.040	8.608.554	2.131

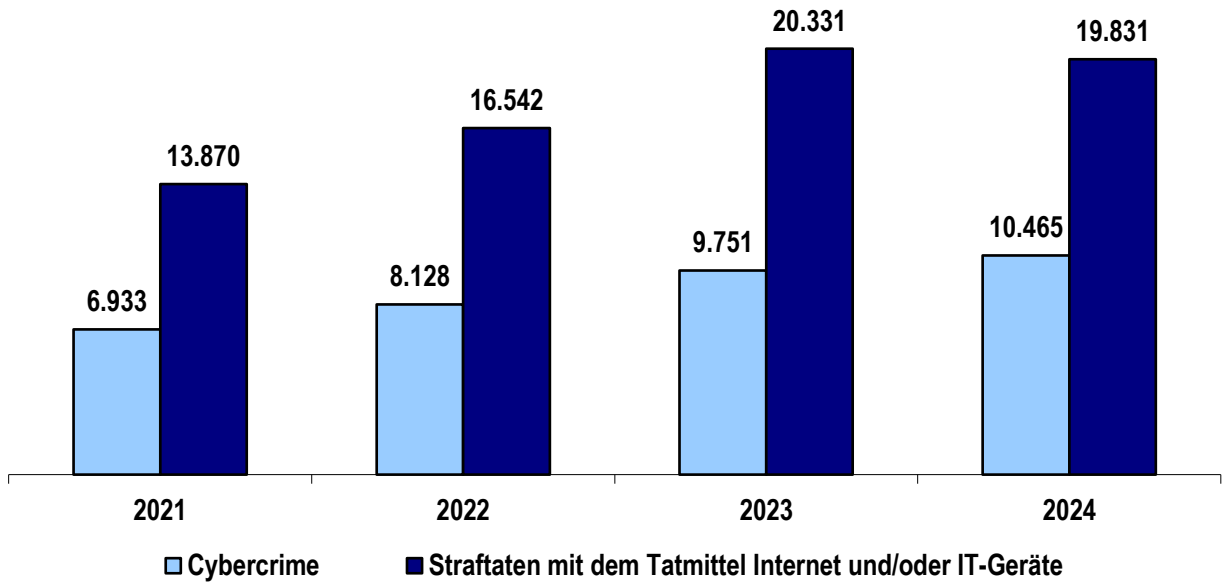
- Tatverdächtige 2020 bis 2024 (Quelle: PKS)

	2021	2022	2023	2024		Veränderung
Tatverdächtige (insgesamt)	**5.574**	**5.614**	**6.191**	**6.735**	↗	***+8,8 %***
männlich	3.911	3.907	4.247	4.691	↗	*+10,5 %*
weiblich	1.663	1.707	1.944	2.044	↗	*+5,1 %*
Erwachsene	4.255	4.219	4.785	5.056	↗	*+5,7 %*
Heranwachsende	528	490	490	507	↗	*+3,5 %*
Jugendliche	555	588	625	758	↗	*+21,3 %*
Kinder	236	317	291	414	↗	*+42,3 %*
Nichtdeutsche TV	475	484	557	790	↗	*+41,8 %*
Anteil nichtdeutscher TV in %	8,5	8,6	9,0	11,7	↗	*+2,7 %-Punkte*

[13] 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 des Jahres 2020 sowie 2021-2024 nur eingeschränkt gegeben.

5.3 Auslandsstraftaten[14]

(Quelle: PKS-Ausland)



- Aufklärungsquoten

	2021	2022	2023	2024
Cybercrime	2,8 %	2,7 %	2,7 %	1,8 %
Straftaten mit dem Tatmittel Internet und/oder IT-Geräte	10,1 %	9,5 %	7,4 %	5,8 %

[14] Die Darstellung von sogenannten Auslandsstraftaten erfolgt ab dem Jahr 2024 auf Basis eines mit dem Ziel einer besseren Auswertequalität angepassten bundeseinheitlichen Katalogs. Um eine Vergleichbarkeit dieser Statistik mit den vergangenen Jahren gewährlisten zu können, erfolgt hier auch die Darstellung der Auslandsstraftaten für die Jahre davor gemäß diesem Katalog- Insofern weichen die hier gegenübergestellten Zahlen zu den Jahren 2021, 2022 und 2023 leicht von den Darstellungen in den vergangenen Lagebildern ab.

L LKA 121: rechnerisch, fachlich richtig, Plausibilität

L LKA 120: fachlich richtig, Plausibilität, strategische Ausrichtung

L LKA 100: fachlich richtig, Plausibilität, strategische Ausrichtung

FüD LKA: Plausibilität und strategische Ausrichtung

L'in FüD LKA: strategische Ausrüstung

L LKA: Schlusszeichnung