

Lagebild 2025

Cybercrime



POLIZEI Brandenburg

Trend

	2024	2025	Veränderung in Prozent	
Cybercrime	2.240	1.990	↘	-11,2 %
Ausspähen von Daten	65	53	↘	-18,5 %
Abfangen von Daten	3	0	↘	-100,0 %
Vorbereiten des Ausspähens und Abfangens von Daten	2	0	↘	-100,0 %
Datenhehlerei	2	1	↘	-50,0 %
Fälschung beweiserheblicher Daten	131	115	↘	-12,2 %
Täuschung im Rechtsverkehr bei der Datenverarbeitung	5	8	↗	+60,0 %
Datenveränderung	49	37	↘	-24,5 %
Computersabotage	17	11	↘	-35,3 %
Computerbetrug	1.966	1.765	↘	-10,2 %
- Betrügerisches Erlangen von Kfz	4	4	=	0 %
- Weitere Arten des Warenkreditbetruges	882	622	↘	-29,5 %
- Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	486	579	↗	+19,1 %
- Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	86	89	↗	+3,5 %
- Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel	147	196	↗	+33,3 %
- Leistungskreditbetrug	94	84	↘	-10,6 %
- Computerbetrug (sonstiger)	164	148	↘	-9,8 %
- Missbräuchliche Nutzung von Telekommunikationsdiensten	13	3	↘	-76,9 %
- Abrechnungsbetrug im Gesundheitswesen	0	2	↗	-
- Überweisungsbetrug	90	38	↘	-57,8 %
Delikte mit Tatmittel Internet und/oder IT-Geräte (insg.)	9.053	9.804	↗	+8,3 %

Inhaltsverzeichnis

1. Vorbemerkung.....	3
2. Lagedarstellung.....	6
2.1 Polizeiliche Kriminalstatistik (PKS)	6
2.1.1 <i>Cybercrime</i>	6
2.1.2 <i>Tatmittel Internet und/oder IT-Geräte</i>	7
2.1.3 <i>PKS-Phänomene</i>	8
2.2 Phänomene und aktuelle Begehungsweisen	9
2.2.1 <i>Diebstahl digitaler Identitäten und Identitätsmissbrauch</i>	9
2.2.2 <i>Angriffe auf das Online-Banking</i>	11
2.2.3 <i>Digitale Erpressung unter Einsatz sogenannter „Ransomware“</i>	13
2.2.4 <i>Ausnutzen von Hardware- und Softwarelücken</i>	15
2.2.5 <i>Payment Diversion Fraud</i>	16
2.2.6 <i>weitere Betrugsstraftaten im Internet</i>	17
2.3 Herausragende Fälle	18
3. Prävention	20
4. Gesamtbewertung und Ausblick	22
5. Anlagen	24
5.1 Cybercrime im Land BB	24
5.2 Tatmittel Internet und/oder IT-Geräte im Land BB.....	26
5.3 Auslandsstraftaten	27

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.

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

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“.

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. 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.

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 der PKS-Inland oder PKS-Ausland ist, neben dem zumindest teilweise in Deutschland befindlichen Erfolgsort, der Handlungsort der Täter. Ist der Handlungsort innerhalb Deutschlands, dann erfolgt die Erfassung in der PKS-Inland. Ist diese Zuordnung nicht möglich, dann erfolgt die Erfassung in der PKS-Ausland, unabhängig davon, ob die Handlung nachweislich im Ausland stattgefunden hat oder der Handlungsort unbekannt ist. Eine Summierung von Inlands- und Auslandsstaten ist aktuell nicht zulässig. Um eine Vergleichbarkeit 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 Auslandsstaten dargestellt, 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 aufgeklärt 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 2025 erfassten Straftaten, die sich gegen das Internet, weitere Datennetze, IT-Systeme oder deren Daten richten, ist gegenüber dem Vorjahr erneut deutlich um 11,2 % auf 1.990 Fälle (2024: 2.240 Fälle) gefallen.

Hinsichtlich der Gesamtsumme des Computerbetruges (PKS-Summenschlüssel 897100) ergibt sich ein Rückgang um 10,2 % auf 1.765 Fälle (2024: 1.966 Fälle).

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

- Ausspähen und Abfangen von Daten, einschließlich der Vorbereitungshandlungen und Datenhehlerei: 54 Fälle (-25,0 %, -18 Fälle),
- Fälschung beweisbarer Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung: 123 Fälle (-9,6 %, -13 Fälle),
- Datenveränderung, Computersabotage: 48 Fälle (-27,3 %, -18 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 Deliktschlüsseln, 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 2025 ein Anstieg um 28,6 % auf 3.171.559 Euro zu verzeichnen (2024: 2.466.109 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 Verdienstaufwände etc. nicht vollständig abbilden. Die größten Schadenssummen durch Cybercrime ergeben sich regelmäßig durch den Einsatz sogenannter „Ransomware“. Diese Fälle werden innerhalb der PKS im Regelfall jedoch als Erpressungen registriert, weshalb derartige Sachverhalte weder in den Gesamtzahlen zur Cybercrime noch in den

durch Cybercrime bewirkten Schadenssummen vollständige Berücksichtigung finden.

Die Zahl der bei den erfassten Fällen von Cybercrime ermittelten Tatverdächtigen (TV) fiel von 1.134 TV (Vorjahr) auf 1.096 TV. Personen über 21 Jahre stellen mit einem Anteil von 86,6 % bzw. 949 TV (2024: 86,7 %, 984 TV) weiterhin die anteilig größte Gruppe unter den TV dar. Der Anteil nichtdeutscher TV beträgt 18,8 % bzw. insgesamt 206 TV (Vorjahr 17,0 % bzw. 193 TV).

Im Phänomenbereich Cybercrime wurden im Berichtsjahr 9.471 Auslandsstraftaten und somit 994 Straftaten (9,5 %) weniger als im Vorjahr (10.465) polizeilich registriert. Somit haben etwa 82,6 % (2024: 82,4 %) 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 dem „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 2025 wurden in der PKS-Inland insgesamt 9.804 Fälle erfasst, die unter Nutzung des „Tatmittels Internet und/oder IT-Geräte“ begangen wurden. Im Vergleich zum Vorjahr stellt dies einen Anstieg um 751 Fälle bzw. 8,3 % dar. Überwiegend handelte es sich dabei um Fälle des Waren-/Warenkreditbetruges (2.155 Fälle, -443 Fälle oder -17,1 %) sowie des Computerbetruges² (1.026 Fälle, -276 Fälle oder -21,2 %).

Die polizeilich erfasste Gesamtschadenssumme (Schaden gemäß PKS-Inland) hat sich von 8.608.554 Euro auf 13.757.970 Euro bzw. um 59,8 % gesteigert. Der Anstieg ist auf einzelne Delikte aus dem Bereich der sonstigen Untreue zurückzuführen.

Im Berichtszeitraum wurden zu den Straftaten mit dem „Tatmittel Internet und/oder IT-Geräte“ 7.359 TV und somit 624 TV (+9,3 %) mehr als im Jahr 2024 ermittelt. Etwas mehr als die Hälfte dieses Anstiegs fällt auf die erwachsenen TV, welche um 332 auf nunmehr 5.388 TV angestiegen sind. Die Zahl der

² Die benannten Zahlen des Computerbetruges stellen lediglich diejenigen Fälle dar, welche von den kriminalpolizeilichen Sachbearbeitern auch mit dem entsprechenden Sonderkennern versehen wurden. Die Gesamtzahl der Fälle des Computerbetrugs betragen 1.765 Fälle (Punkte 2.1.1).

Heranwachsenden bleibt mit 499 TV (Vorjahr: 507) nahezu identisch. Die Anzahl der tatverdächtigen Kinder und Jugendlichen hingegen stieg deutlich auf 555 TV (+141 TV) bzw. 917 TV (+159 TV) an. Insgesamt bilden die Erwachsenen mit 73,2 % (5.388 TV) weiterhin die anteilig größte Gruppe, 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 2025 insgesamt 891 nichtdeutsche TV und damit 101 TV mehr als im Vorjahr erfasst.

Im Berichtsjahr wurden in der PKS-Ausland 18.567 Straftaten mit dem „Tatmittel Internet und/oder IT-Geräte“ registriert. Somit ist das Fallaufkommen gegenüber dem Vorjahr (2024: 19.831 Fälle) um 1.264 Fälle (-6,4 %) gesunken. Insgesamt entspricht dies einem Anteil von 65,4 % (Vorjahr 68,7 %) 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 anhand 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 Phänomene durch die Sachbearbeitung erkannt und entsprechend markiert werden. Die Zuordnung erfolgt im POLAS-Beleg und ist unabhängig vom jeweiligen Delikt.

Im Berichtsjahr wurden drei Fälle dem Phänomen „(D)DoS-Attacke“, 6.415 Fälle dem Phänomen „digitaler Identitätsdiebstahl/ Accountübernahme“, 162 Fälle als „Eindringen in Datennetze/Datenveränderung/Datendiebstahl bei nichtnatürlichen Personen“, 827 Fälle dem Phänomen „Angriff auf das Online-Banking“ sowie 70 Fälle als „Ransomware“ zugeordnet.

2.2 Phänomene und aktuelle Begehungsweisen

2.2.1 *Diebstahl digitaler Identitäten und Identitätsmissbrauch*

Die digitale Identität³ 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 anderer Delikte (z. B. betrügerische Warenbestellungen, missbräuchliche Verwendung von Kreditkartendaten, Versendung von Schadsoftware, DDoS-Attacken zum Nachteil von Unternehmen, Behörden und Einrichtungen etc.) dar. Neben der digitalen Identität einer natürlichen Person, werden auch die „Identitäten“ von juristischen Personen, wie Unternehmen, Vereinen oder anderen Institutionen, missbräuchlich verwendet.

Weiterhin auf hohem 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 Modi Operandi wird die Verwendung von eigenen Zahlungsprozessen von Online-Verkaufsplattformen zur 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 sogenannte 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.

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.

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). Dabei gehen die Täter immer professioneller vor, um ihre Identität zu verbergen. 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 nur durch einen Anruf beim entsprechenden Betriebssystem-Hersteller, einen Support zum Entfernen dieser Schadsoftware erhalten können (sog. Tech-Support-Scam). 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 sie 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 im Anschluss durch die Täter unberechtigt bei der Ausübung weiterer Straftaten eingesetzt.

Wie auch im Jahr 2024 wurden zunehmend Fälle registriert, bei denen Täter bereits gestellte Rechnungen durch „neue“ Bankdaten⁴ abänderten (sog. Payment-Diversion-Fraud). Die Täter erlangen somit 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.

Abweichend zu den letzten Berichtsjahren ist auch eine weitere Begehungsweise vermehrt festzustellen, bei welcher den Opfern die erfolgreiche Teilnahme an einem Gewinnspiel bescheinigt und diese zum Aufruf von Webseiten verlasst werden, die denen bekannter Gewinnspiel-Anbieter nachempfunden sind. Die Geschädigten werden dann dazu aufgefordert weitere Daten von sich Preis zu geben, um den vorgeblichen Gewinn zu erhalten.

⁴ Diese „neuen“ Bankverbindungen, zu inländischen und ausländischen Banken, sind in der Regel Finanzagentinnen und -agenten zuzuordnen.

Beispielfall

Die Leitung einer großen internationalen Bildungseinrichtung meldete am 09.05.2025, dass massenhaft E-Mails an Eltern von Schülerinnen und Schüler versandt worden sind. Diese beinhalteten mit einem Nachlass versehene Zahlungsaufforderungen für die Schulgebühren. Als E-Mail-Adresse verwendeten die Täter eine Domain, die der tatsächlichen Domain der Schule sehr ähnlichsah (sog. „Typosquatting“). In einem Fall führte diese Vorgehensweise zum Erfolg und die Angeschriebenen überwiesen im guten Glauben knapp 48.000 Euro an die vorgegebliche Kontonummer der Schule. Ermittlungen ergaben, dass die E-Mail-Adresse einer Mitarbeitenden der Schule zuvor kompromittiert wurde und die Täter so die E-Mail-Adressen der Eltern ausgespäht hatten.

Beispielfall

Am 12.06.2025 teilte eine Brandenburger Hochschule mit, dass über eine dort verwaltete E-Mail-Adresse ca. 230.000 Phishing-E-Mails versandt worden sind. Ermittlungen ergaben, dass zuvor die aussendende E-Mail-Adresse ihrerseits eine Phishing-E-Mail erhalten hatte, der Nutzer den dort enthaltenden Link aufrief und in der Folge seine Zugangsdaten auf der sich öffnenden Webseite eingab. Diese initiale Phishing-E-Mail wurde von einem Server versandt. Der Link, welcher in den ca. 230.000 versandten Phishing-E-Mails eingetragen war, führte zu einem anderen Server.

2.2.2 Angriffe auf das Online-Banking

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

Auf ähnlich hohem Niveau gegenüber dem Vorjahr sind die Fälle der Betrugsmasche „Support eines Betriebssystemherstellers“ geblieben. Im Zusammenhang mit dieser Betrugsmasche erhielten die Geschädigten Anrufe von Tätern oder wurden durch Einblendungen von sog. „Pop-Up“-Fenstern auf dem Computerbildschirm dazu aufgefordert, 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 der Modus Operandi 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 selbst auszahlen. Die Geschädigten stellten erst anhand der Bank-Abbuchungen fest, dass sie ihren Stromanbieter „gewechselt“ hatten.

Das Phänomen des sog. „falschen Bankmitarbeiters“ ist weiterhin präsent. Kennzeichnend ist, dass die Geschädigten mittels einer vorgetäuschten Rufnummer der tatsächlichen Bank (sog. „Call-ID-Spoofing“) kontaktiert.

Am häufigsten erhielten die Geschädigten in 2025 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 Zugriff auf ihr Online-Banking sowie unberechtigte Überweisungen mit hohen Geldbeträgen.

Der Modus Operandi des „falschen Bankmitarbeitenden“ verdeutlicht, dass das Vorgehen der Täter einem ständigen Wandel unterliegt und häufig nicht gänzlich ermittelt werden 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 Dienstgeschäfts und bei Erfahrungsaustauschen mit den bearbeitenden Dienststellen zu stützen, kann aber anhand der polizeilichen Auskunftssysteme nicht valide nachvollzogen werden⁵.

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.

⁵ Dies liegt vornehmlich in fehlenden Katalogwerten zu Kryptowährungen und in der Erfassungspraxis begründet.

2.2.3 Digitale Erpressung unter Einsatz sogenannter „Ransomware“

Die digitale Erpressung unter Einsatz sogenannter „Ransomware“⁶ 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. Demzufolge 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), Mails 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, deren Arbeiten regelmäßig zu einer vollständigen Bereinigung des jeweiligen IT-Systems führt. Neben den durch die Ransomware verursachten Systemschäden und dem Arbeitsausfall entstehen beachtliche Mehrkosten für die Beauftragung von IT-Unternehmen. Das führt wiederum dazu, dass insbesondere kleinere Unternehmen häufiger abwägen den Lösegeldforderungen nachzukommen, da die Kosten im Vergleich zum Systemausfall und der Bereinigung geringfügiger erscheinen.

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

Es ist weiterhin davon auszugehen, dass das Dunkelfeld in diesem Bereich sehr groß ist. Grundsätzlich sind Unternehmen zunächst an der Wiederherstellung

⁶ 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.

der Arbeitsfähigkeit interessiert und wollen eine möglichen Rufschädigung durch Bekanntwerden des Vorfalls vermeiden⁷.

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

Darüber hinaus ist vor allem im Bereich der Erpressung von Privatpersonen das Phänomen der sog. „Sextortion“ weiterhin präsent. Dabei erhalten E-Mail-Empfänger eine Drohung, dass angeblich von ihnen gefertigte intime Videoaufzeichnungen veröffentlicht werden, es sei denn die Geschädigten würden eine entsprechende Summe in einer Kryptowährung zahlen. Teilweise wird dieser Drohung mehr Nachdruck verliehen, indem persönliche Daten, Passwörter oder Anschriften mitgeteilt werden.

Als Variante dieser Begehungsweise wird nicht mit der Veröffentlichung intimer Bildaufzeichnungen gedroht, sondern mit körperlicher Gewalt durch Dritte.

Beispielfall

Am 30.09.2025 meldete ein Brandenburger Amt, dass dort die IT-Infrastruktur verschlüsselt wurde. Zunächst ergab sich zum Cyberangriff eine untypische Informationslage, da keinerlei Ransomnote (Erpresserschreiben) einer Ransomware-Gruppierung festgestellt wurde. Auch ein Datenabfluss konnte nicht festgestellt werden. Da das Backup-System vom Angriff nicht betroffen war, konnten die IT-Verantwortlichen die Systeme zeitnah wiederherstellen. Am 20.10.2025 erfolgte dann eine Kontaktaufnahme durch eine Polizeidienststelle eines anderen Bundeslandes. Im Rahmen eines dort geführten Ermittlungsverfahrens wurde ein Server sichergestellt, auf dem sich augenscheinlich auch Daten des hier betroffenen Amtes befanden. Folglich war es doch zu einem Datenabfluss gekommen. Ungewöhnlich scheint, dass nach derzeitigem Ermittlungsstand zwar eine Verschlüsselung mittels der Ransomware „Locky“ festgestellt, aber noch immer kein Erpresserschreiben aufgefunden wurde. Somit bleibt unklar, ob eine finanzielle oder lediglich destruktive Absicht beim Angriff vorlag.

⁷ 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.

Beispielfall

Am 19.03.2025 zeigte der Geschäftsführende eines Brandenburger Unternehmens an, dass in seinem Unternehmen insgesamt vier Server und das Backup verschlüsselt wurden. Betroffen war die Office Umgebung, sodass die Buchhaltung nicht mehr funktionierte und demnach keine Löhne gezahlt oder Angebote erstellt werden konnten. Der finanzielle Schaden belief sich auf 83.500 Euro. Die Kunden des Unternehmens waren nicht direkt betroffen, jedoch wurde ein Datenabfluss festgestellt. Das geschädigte Unternehmen blieb weiterhin betriebsfähig. Ermittlungen ergaben, dass das Unternehmen durch die Ransomware-Gruppierung „Akira“ angegriffen wurde und auf der Leak-Site der Gruppierung mit der Veröffentlichung von mehr als 13 GB an Unternehmensdaten gedroht wurde, welche Informationen über Angestellte und Kunden sowie über Finanzen und Projekte des Unternehmens enthalten sollten. Obwohl das Unternehmen der Lösegeldforderung nicht nachkam, wurden keine Daten des Unternehmens veröffentlicht. Die im Zusammenhang mit der Gruppierung geführten zentralen Ermittlungen sind noch nicht abgeschlossen.

2.2.4 Ausnutzen von Hardware- und Softwarelücken

Wie in den vergangenen Berichtsjahren wurden durch Täter auch in 2025 immer wieder Sicherheitslücken in Hard- und Software ausgenutzt, um sich unberechtigt Zugang zu Daten oder Zugriff auf IT-Systeme zu verschaffen. Vor allem das Ausnutzen von sog. Zero-Day-Sicherheitslücken⁸ birgt dabei ein großes Schadenspotential.

Beispielfall

Am 15.01.2025 wurde bekannt, dass eine Tätergruppierung unter Ausnutzung einer Software-Sicherheitslücke die IT-Infrastruktur im Land Brandenburg ansässiger zunächst unbekannter Personen oder Institutionen kompromittiert haben könnte und durch die Tätergruppierung „Belsen Group“ Daten im Internet veröffentlicht worden sind. Eine Sichtung der veröffentlichten Daten ergab, dass umfangreiche Firewall-Konfigurationsdaten und Fernwartungszugänge (VPN-Zugangsdaten) betroffen waren. Weiterhin wurden Dateisystem-Screenshots eines Landkreises veröffentlicht. Auf Grund dieser Erkenntnisse wurde die Amtsleitung für Digitales der betroffenen Stadt kontaktiert und über den Vorfall sowie eine damit möglicherweise im Zusammenhang stehende, die Firewall der Stadtverwaltung betreffende, Sicherheitslücke aufgeklärt. Die betreffende Sicherheitslücke war der Amtsleitung nach eigener Aussage bereits bekannt und wurde behoben, da das CERT Brandenburg die Stadt bereits darüber informiert hatte. Weitere Ermittlungen ergaben, dass die ausgespähten Daten bereits aus dem Jahr 2022 stammten. Somit wurde wahrscheinlich bereits damals eine entsprechende Sicherheitslücke ausgenutzt und die Daten lediglich erst jetzt durch die

⁸ 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.

Gruppierung veröffentlicht. Hinweise auf eine nachhaltige Kompromittierung der Systeme lagen nicht vor. Die Ermittlungen ergaben weiterhin, dass die „Belsen Group“ in diesem Zusammenhang insgesamt etwa 15.000 Firewall und VPN-Konfigurationen veröffentlichte. Diese stammen alle von der entsprechenden Sicherheitslücke aus dem Jahr 2022. Die Reaktionsgeschwindigkeit des Herstellers bis zur Bereitstellung eines Sicherheitsupdates nach Bekanntwerden der Sicherheitslücke betrug vier Tage im Jahr 2022.

Beispielfall

Am 19.09.2025 wurde öffentlich bekannt, dass Angreifer Zugriff auf etwa 5% aller Cloud-Konten eines Firewall-Herstellers erlangten und in diesem Zusammenhang Firewall-Backups ausspähten, welche Konfigurationsdateien und verschlüsselte Passwörter enthielten. Am 10.10.2025 wurde dann bekannt, dass mittlerweile sämtliche Cloud-Backups aller Firewall-Kunden dieses Herstellers kompromittiert wurden. Dies hatte gravierende Folgen, da Angreifer über diese Backup-Daten direkten Zugriff auf Firewall-Konfigurationsdateien (wie bspw. VPN-Konfigurationen) erlangten, die dann ggf. für weiterführende Angriffe (wie Ransomware-Angriffe) genutzt werden können. In diesem Zusammenhang wurden in Brandenburg auch zwei Ransomware-Angriffe zum Nachteil zweier Gemeinden bekannt, die diese Firewall nutzten. In einem Fall wurden sämtliche virtuelle Server verschlüsselt, folglich standen Bürgerservices weitgehend nicht mehr zur Verfügung. Wie für erfolgreiche Ransomware-Angriffe üblich, mussten die Systeme aufwändig wiederhergestellt werden. Am 02.12.2025 meldete das Amt schließlich, dass alle Dienstleistungen wieder wie gewohnt angeboten werden. In den auf den Angriff folgenden Monaten wurden auch Phishing-Versuche gemeldet, bei denen zumindest naheliegend erscheint, dass Einwohnermeldedaten der Gemeinden genutzt worden sein könnten. Die Angriffe auf die Gemeinden wurden der Ransomware-Gruppierung „Lynx“ zugeordnet.

2.2.5 Payment Diversion Fraud

Ein weiteres weit verbreitetes (Betrugs-)Phänomen ist der so genannte „Payment Diversion Fraud“. Im Allgemeinen erhält 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 potenziellen Opfer. Ferner wurden der ZAC der Polizei des Landes Brandenburg Fälle bekannt, bei denen im Vorfeld von einem der Geschäftspartner der E-Mail-Account oder das ganze Netzwerk kompromittiert wurde.

Auch die Verwendung von ausländischen Bankverbindungen führt nicht immer dazu, dass die Täuschungshandlung auffällt, da bei Geschäftsbeziehungen über Ländergrenzen hinweg z. B. Bankkonten und Firmensitz nicht immer im gleichen Land verortet sind. Weiter wurden Sachverhalte bekannt, in 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

Am 07.08.2025 wurde durch einen Mitarbeitenden einer Stadt Anzeige erstattet, nachdem bekannt wurde, dass es dort zu Überweisungen auf falsche Bankkonten gekommen war. Ermittlungen ergaben, dass dem 03.06.2025 in einem zentralen Postfach der Stadt eine E-Mail vorgeblich von einem Unternehmen, welches Vertragspartner der Stadt ist, einging in der eine geänderte Kontoverbindung bekannt gegeben wurde. Die E-Mail wurde von einer nicht zum Unternehmen passenden E-Mail-Adresse versendet, jedoch mit der Signatur des Unternehmens. Die neue Bankverbindung wurde in der Folge durch den Sachbearbeitenden der Stadt im System angepasst und ab diesem Zeitpunkt wurden sämtliche Zahlungen an die neue, von den Tätern genutzte Bankverbindung, transferiert. Am 17.06.2025 wurde erneut eine E-Mail an das zentrale Postfach gesandt und durch den Mitarbeitenden der Stadt eine weitere Änderung der Bankverbindung veranlasst. Am 06.08.2025 wurde dann durch die Bank die Zahlungsanweisung abgewiesen und dadurch bekannt, dass sämtliche Zahlungen nicht an die richtige Bankverbindung gegangen waren. Auf einem der Zielkonten wurden ca. 150.000 Euro durch die Bank eingefroren. Etwa 80.000 Euro davon wurden der hier geschädigten Stadt zugeordnet. Ermittlungen zu den Kontoinhabenden ergaben, dass diese aus einem finanziell benachteiligten Personenkreis, teilweise ohne festen Wohnsitz, aus dem Ruhrgebiet stammten. Im Rahmen des polizeilichen Informationsaustausches wurde bekannt, dass dort eine Tätergruppierung agiert, die o. g. Personen gezielt anspricht und diese gegen Bezahlung etc. anwirbt Bankkonten auf deren Namen zu eröffnen, wobei diese Personen tatsächlich nie Zugriff auf die Konten erhalten.

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“ bekannt gemacht worden. Dabei treten die Täter über soziale Plattformen mit den Opfern in Kontakt, in vielen Fällen erfolgt der Wechsel zu einem Instant-Messenger, um zunächst ein Vertrauensverhältnis aufzubauen.

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.

Beim Phänomen „Cybertrading“ werden Opfer gezielt angeschrieben oder durch Werbeversprechen dazu animiert, in Kryptowährungen zu investieren. Das 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., gefordert⁹.

2.3 Herausragende Fälle

DDoS-Angriff auf die Internetwache

Spätestens seit dem Frühjahr 2023 ist die pro-russische Gruppierung „No-Name057(16)“ vielen ein Begriff. Es handelt sich dabei um eine Tätergruppierung aus dem Bereich Cybercrime, die DDoS-Angriffe ankündigt, plant und durchführt. Die Gruppierung formierte sich im Zuge des russischen Angriffskrieges auf die Ukraine und führt seitdem auch auf deutsche Behörden und Organisationen Angriffe durch. Die Angriffe fokussieren sich insgesamt gesehen auf Behörden und Unternehmen der Länder, die sich solidarisch mit der Ukraine zeigen. Oft sind entsprechende DDoS-Angriffe als direkte Antwort auf entsprechende solidarische Akte zu verstehen. Charakteristisch für die Gruppierung ist, dass sie sich durch intensive Nutzung des Telegram-Messengers organisiert und insbesondere in zwei Kanälen je deutscher und englischer Sprache durchgeführte Angriffe für sich reklamiert. Die Telegram-Kanäle und Gruppen werden auch dazu genutzt, eine möglichst breite Masse an Personen für die Durchführung von Angriffen zu rekrutieren, inkl. entsprechender Tutorials. Im Land Brandenburg wurde im Jahr 2023 die Internetwache der Polizei Brandenburg erfolgreich angegriffen und stand kurzzeitig nicht zur Verfügung. Aufgrund dieser Ereignisse ergriff der Zentrale IT-Dienstleister des Landes Brandenburg (ZIT-BB) DDoS-Schutzmaßnahmen. Auch im ersten Quartal 2025 erging im Rahmen des polizeilichen Informationsaustauschs eine Warnmeldung darüber, dass am 12.02.2025 erneut ein Angriff auf deutsche Behördendomains stattgefunden habe, darunter laut der Gruppierung wiederum die Internetwache der Polizei Brandenburg. Erste Ermittlungen ergaben, dass die 2023 implementierten Schutzmechanismen den Angriff wirksam abwehrten. Auch nachfolgend gelang bisher kein erfolgreicher Angriff mehr.

⁹ Für eine dezidierte Darstellung dieses Phänomens wird auf das Lagebild Wirtschaftskriminalität 2025 verwiesen.

Darknet- Händler „Zugang zu deutscher Behörde“

Am 17.01.2025 erging durch das LKA Nordrhein-Westphalen eine Meldung an die ZAC LKA BB, in welcher mitgeteilt wurde, dass bereits am 07.01.2025 auf einer Darknet-Verkaufsplattform Zugangsdaten zu einer „Behörde in Deutschland“ zum Kauf angeboten wurden. Es konnte zunächst anhand des Verkaufsangebots nicht direkt festgestellt werden, um welche Behörde es sich handelte. Das LKA NRW erlangte allerdings im Rahmen der Gefahrenabwehr durch einen sog. Scheinankauf die angebotenen Zugangsdaten. Eine Sichtung des Zugangs ergab, dass es sich bei den angebotenen Daten um den Zugang zu einem in osteuropäischem Ausland befindlichen Server handelte. Dieser hatte wiederum Zugriff auf einen Server, der einem Landkreis im Land Brandenburg zugeordnet wurde. Genauer ergaben die weiterführenden Ermittlungen, dass es sich um einen Server zur Zwischenspeicherung von Entwicklungsständen eines Kreisarchivs handelte. Dieser war nach Aussage des Landkreises kein Teil des Landesverwaltungsnetzes, weiterhin wurde diesem keinerlei Kritikalität zugemessen. Der betroffene Server des Landkreises wurde in Zusammenarbeit mit dem betreibenden IT-Dienstleister abgeschaltet und bereinigt. Weiterführende Auswirkungen blieben aus. Der Verkäufer der Zugangsdaten wurde im Rahmen erster OSINT-Recherchen mit einem X-Account in Verbindung gebracht. Weiterhin konnten in diesem Rahmen Bezüge zur Ransomware-Gruppierung „Hellcat“ hergestellt werden. Auch wenn im konkreten Fall kein kritisches System des Landkreises betroffen war, zeigt dieser Vorfall die stetige Gefahr durch entsprechende Tätergruppierungen, auch für Behörden.

Ehemaliger Mitarbeiter löscht umfangreich Daten

Am 20.03.2025 gab das geschädigte Unternehmen im Rahmen der Anzeigenaufnahme an, dass dieses Daten in einer Cloud eines namenhaften Anbieters speichere und verarbeite. Im weiteren Verlauf wurden umfangreiche Datensätze inklusive Backups von einem unbekannten Täter gelöscht. Ermittlungen ergaben, dass die Löschung über einen Nutzer-Account erfolgte, der so nicht bekannt war. Der Zugriff wurde über eine IP-Adresse, die einem regional agierenden Provider zugeordnet werden konnte, vorgenommen. Dieser konnte die IP-Adresse jedoch keinem konkreten Anschlussinhabenden zuordnen. Ermittlungen zum zunächst unbekannten Nutzer-Account ergaben, dass dieser bereits am 29.11.2024 erstellt worden war. Die Protokolldateien, die dokumentieren, wer diesen Account erstellt hatte, waren jedoch nicht mehr vorhanden. Diese waren offensichtlich gelöscht worden. Im Zuge der Zeugenvernehmung wurde bekannt, dass einem ehemaligen Mitarbeiter des Unternehmens am 28.11.2024 gekündigt worden war und dieser am 19.03.2025 einen Negativbescheid hinsichtlich seiner Abfindung vom Unternehmen erhalten hatte. Außerdem wohnte dieser im Einzugsbereich des Providers und hatte auch bei diesem einen entsprechenden Vertrag. Ergänzend wurde bekannt, dass dieser ehemalige Mitarbeiter sowohl die entsprechenden technischen Fertigkeiten hatte als auch in dem Bereich des Unternehmens tätig war, wo dieser die Nutzer-Accounts hatte erstellen können. Auch war dessen Account einen Tag nach der Kündigung noch nicht gesperrt, sodass dieser auch über die Rechte verfügte, die nötig waren, den Account, zu erstellen.

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 potenzielle 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 einer 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 2025 insgesamt 1.201 (2024: 837) Präventionsveranstaltungen zum Thema „Cybercrime/Neue Medien“ durch, mit denen rund 28.724 (2024: 20.554) Teilnehmende erreicht wurden. Die Veranstaltungen wurden als Projekt, als Vortrag und im Rahmen von Elternabenden durchgeführt. Die Schwerpunkte richteten sich an dem Alter der Teilnehmenden aus und umfassten 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 (z.B. Eltern oder Lehrer/-innen) statt, um diese mit den Themen Internet und Neue Medien vertraut zu machen, sie zu einem sicherheits- und verantwortungsbewussten Umgang mit dem Internet und den Neuen Medien zu befähigen und als Multiplikatoren zu gewinnen.

Die im LKA Brandenburg eingerichtete „Zentrale Ansprechstelle Cybercrime“ (ZAC) bietet Wirtschaftsunternehmen und Behörden Beratung und Unterstützung zum Thema „Cybersicherheit“, u. a. auch zu den Maßnahmen nach der Feststellung eines Angriffs durch Cyberkriminelle, an. Hierzu sind für die ZAC in den Bundesländern gesonderte Erreichbarkeiten eingerichtet¹⁰.

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

¹⁰ Siehe auch www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html



öffentlichen Verwaltungen bzw. führt derartige Veranstaltungen auch anlassbezogen nach Anforderung eigenständig durch.

Die ZAC Brandenburg begleitete im Jahr 2025 insgesamt 40 Veranstaltungen mit 2.362 Teilnehmenden (2024: 15, mit 1.259 TN) durch Vorträge zu aktuellen Aspekten der Cybersicherheit und Verhaltensempfehlungen unterstützt durch Live-Vorführungen zu möglichen Sicherheitsrisiken im täglichen Umgang mit den Medien.

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 erforderlichen 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, insbesondere sog. Zero-Day-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 der 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 und vor allem unzureichende Backup-Konzepte. Dazu kommen in vielen Fällen nur unzureichend geschulte Administratoren bzw. Mitarbeitende im Umgang mit IT-Endgeräten. Wenngleich der Trend der nachlassenden Zahlungsbereitschaft weiter anhält, 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 ihre Wirkung, da im Nachgang zumindest vorübergehend die Aktivitäten der betroffenen Ransomware-Gruppierungen minimiert wurden und in einigen Fällen auch nicht mehr auftraten.

Im Zusammenhang mit der Schnelllebigkeit des Kriminalitätsbereichs „Cybercrime“ erscheint seit dem 1. Quartal 2023 regelmäßig ein entsprechender polizei-interner Monitoring-Bericht, in welchem spezifische Phänomene dargestellt und besondere Ermittlungsmaßnahmen vorgestellt 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.

Die rasante Entwicklung Künstlicher Intelligenz (KI) verändert nicht nur Wirtschaft und Gesellschaft, sondern zunehmend auch die digitale Sicherheitslandschaft. Insbesondere der Fortschritt generativer KI-Systeme ermöglicht es, Texte, Bilder, Softwarecodes und andere digitale Inhalte in kurzer Zeit automatisiert zu erzeugen bzw. zu optimieren. Dies eröffnet unter anderem auch Möglichkeiten sowohl für die Abwehr als auch für die Durchführung von Cyberangriffen. Der Einsatz von KI kann aber auch neue Phänomene begründen. So gibt es Vorgehensweisen oder Straftaten, die sich unmittelbar gegen KI-Modelle richten oder durch deren unautorisierte Nutzung finanzielle Schäden verursacht werden. KI stellt somit einen eigenen Angriffsvektor dar, wirkt vor allem aber als Technologie, die bestehende Methoden der Cybercrime effizienter und skalierbarer macht. Im Bereich



der Cybercrime kann KI unter anderem zur Automatisierung und Personalisierung von Phishing- und Social-Engineering-Angriffen eingesetzt werden. Sprachmodelle können beispielsweise glaubwürdig formulierte Nachrichten in unterschiedlichen Sprachen erzeugen, ohne die bisherigen sprachlichen Auffälligkeiten automatisierter Betrugsversuche. Darüber hinaus kann KI bei der Analyse großer Datenmengen helfen, wodurch Angreifer potenziell schneller geeignete Ziele oder Informationen über diese identifizieren können. Gleichzeitig erleichtert der Zugang zu generativen KI-Systemen auch weniger erfahrenden Personen den Einstieg in bestimmte Formen digitaler Kriminalität und senkt somit die Eintrittsschwelle zu cyberkriminellem Handeln.

Auch für die Cyberspionage ergeben sich durch KI neue Möglichkeiten. Nachrichtendienste und andere Akteure können KI bspw. bei der Verarbeitung und Auswertung großer Mengen digitaler Informationen einsetzen. Insbesondere bei der Analyse öffentlich zugänglicher Informationen (OSINT) kann eine automatisierte Verarbeitung dabei helfen, relevante Zusammenhänge schneller zu erkennen. Darüber hinaus können derartige Systeme bei der Übersetzung, Klassifizierung und Zusammenfassung umfangreicher Dokumentenbestände eingesetzt werden. Zudem steigt durch KI die Gefahr, dass Desinformationen und manipulierte Inhalte gezielter erstellt und verbreitet werden. Im Bereich der Cybersabotage kann KI insbesondere die Geschwindigkeit und Anpassungsfähigkeit von Angriffen beeinflussen. Mittels automatisierter Systeme können große Mengen technischer Informationen analysiert und potenzielle Schwachstellen gezielt ausgenutzt werden.

5. Anlagen

5.1 Cybercrime im Land BB

- Fallzahlenentwicklung 2021 bis 2025 (Quelle: PKS)

	2021	2022	2023	2024	2025		Veränderung
Erfasste Fälle	2.678	2.640	2.744	2.240	1.990	↘	-11,2 %
Aufklärungsquote (AQ) in %	61,8	58,2	58,9	58,2	59,0	↗	+0,8 %-Punkte

- Delikte im Detail:

▶ Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr b. der Datenverarbeitung (§§ 269, 270 StGB)	99	96	135	136	123	↘	-9,6 %
▶ Datenveränderung, Computersabotage (§§ 303a, 303b StGB)	69	78	79	66	48	↘	-27,3 %
▶ Ausspähen, Abfangen von Daten, einschl. Vorbereitungshandlungen und Datenhehlerei (§§ 202a-d StGB)	63	65	89	72	54	↘	-25,0 %
▶ Computerbetrug (§ 263a StGB)	2.447	2.401	2.441	1.966	1.765	↘	-10,2 %
▶ Betrügerisches Erlangen von Kfz	2	2	1	4	4	=	0 %
▶ Weitere Arten des Warenkreditbetruges	1.182	1.209	1.193	882	622	↘	-29,5 %
▶ Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	542	540	547	486	579	↗	19,1 %
▶ Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	118	86	126	86	89	↗	+3,5 %
▶ Computerbetrug mittels rechtswidrig erlangter sonst. unbarer Zahlungsmittel	229	170	223	147	196	↗	33,3 %
▶ Leistungskreditbetrug	101	107	112	94	84	↘	-10,6 %
▶ Computerbetrug (sonstiger)	194	175	137	164	148	↘	-9,8 %
▶ Missbräuchliche Nutzung von Telekommunikationsdiensten	10	18	14	13	3	↘	-76,9 %
▶ Abrechnungsbetrug im Gesundheitswesen	0	0	0	0	2	↗	-
▶ Überweisungsbetrug	69	94	88	90	38	↘	-57,8 %

- Schadenssummen 2021 bis 2025 (Quelle: PKS)¹¹

Jahr	Schadensfälle ¹² 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
2025	1.765	3.171.559	1.797

- Tatverdächtige 2021 bis 2025 (Quelle: PKS)

	2021	2022	2023	2024	2025	Veränderung	
Tatverdächtige (insgesamt)	1.151	1.097	1.327	1.134	1.096	↘	-3,4 %
männlich	740	714	825	713	704	↘	-1,3 %
weiblich	411	383	502	421	392	↘	-6,9 %
Erwachsene	1.022	973	1.194	987	949	↘	-3,9 %
Heranwachsende	75	67	79	85	82	↘	-3,5 %
Jugendliche	43	42	50	55	56	↗	+1,8 %
Kinder	11	15	4	10	9	↘	-10,0 %
Nichtdeutsche TV	138	147	166	193	206	↗	+6,7 %
Anteil nichtdeutscher TV in %	12,0	13,4	12,5	17,0	18,8	↗	+1,8 %-Punkte

¹¹ Bei Cybercrime wurden Schäden nur bei den Delikten des Computerbetruges (PKS-Summenschlüssel 897100) registriert.

¹² vollendete und versuchte Taten

5.2 Tatmittel Internet und/oder IT-Geräte im Land BB

- Fallzahlenentwicklung 2021 bis 2025 (Quelle: PKS)

	2021	2022	2023	2024	2025	Veränderung	
erfasste Fälle (insgesamt)	8.528	8.350	8.788	9.053	9.804	↗	+8,3 %
Aufklärungsquote (AQ) in %	87,0	85,2	85,5	87,5	89,0	↗	+1,5 %-Punkte

- Schadenssummen 2021 bis 2025 (Quelle: PKS)

Jahr	Schadensfälle insgesamt ¹³	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
2025	3.397	13.757.970	4.050

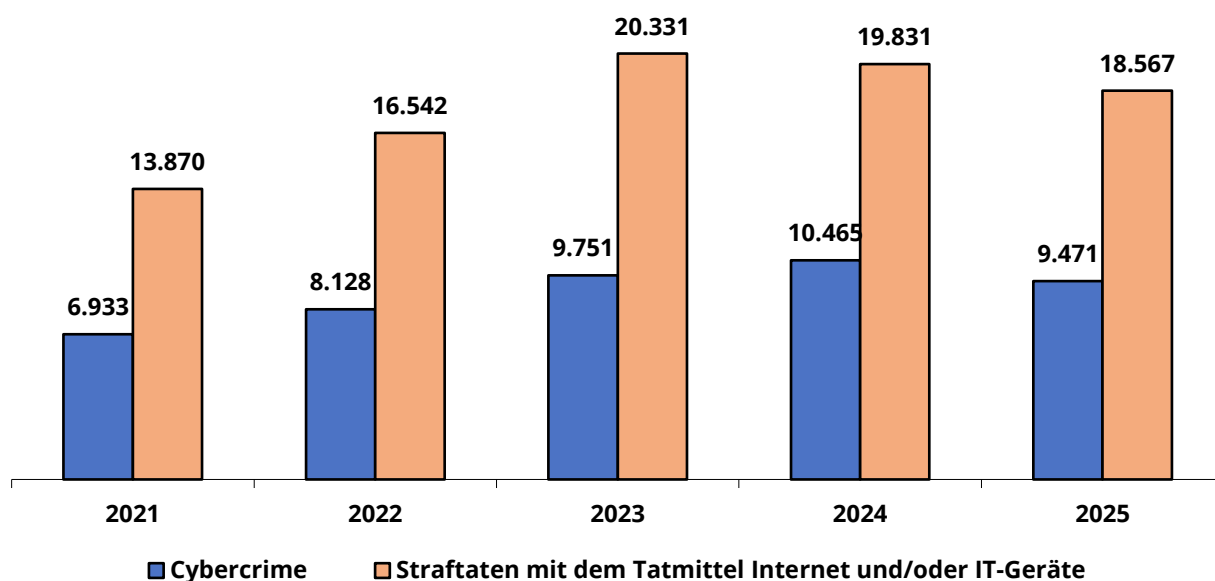
- Tatverdächtige 2021 bis 2025 (Quelle: PKS)

	2021	2022	2023	2024	2025	Veränderung	
Tatverdächtige (insgesamt)	5.574	5.614	6.191	6.735	7.359	↗	+9,3 %
männlich	3.911	3.907	4.247	4.691	5.103	↗	+8,8 %
weiblich	1.663	1.707	1.944	2.044	2.256	↗	+10,4 %
Erwachsene	4.255	4.219	4.785	5.056	5.388	↗	+6,6 %
Heranwachsende	528	490	490	507	499	↘	-1,6 %
Jugendliche	555	588	625	758	917	↗	+21,0 %
Kinder	236	317	291	414	555	↗	+34,1 %
Nichtdeutsche TV	475	484	557	790	891	↗	+12,8 %
Anteil nichtdeutscher TV in %	8,5	8,6	9,0	11,7	12,1	↗	+0,4 %-Punkte

¹³ vollendete und versuchte Taten

5.3 Auslandsstraftaten¹⁴

(Quelle: PKS-Ausland)



- Aufklärungsquoten

	2021	2022	2023	2024	2025
Cybercrime	2,8 %	2,7 %	2,7 %	1,8 %	1,9 %
Straftaten mit dem Tatmittel Internet und/oder IT-Geräte	10,1 %	9,5 %	7,4 %	5,8 %	3,4 %

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 gewährleisten 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.

Impressum

Polizeipräsidium des Landes Brandenburg
Bereich: Landeskriminalamt, LKA 121
Tramper Chaussee 1
16225 Eberswalde
E-Mail: cybercrime.lka@polizei.brandenburg.de

Nutzungshinweis

Die Nutzung der Daten ist nur mit Quellenangabe zulässig. Es gilt die Datenlizenz Deutschland -- Version 2.0
<https://www.govdata.de/dl-de/by-2-0>