Bayerisches
Landeskriminalamt

CYBERCRIME

Landeslagebild Bayern

2022

Inhaltsverzeichnis

Anmerkung: In diesem Bericht wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

1 Vorwort

Die Verbreitung digitaler Technologie und die Ausweitung digitaler Netzwerke führen zu erheblichen Veränderungen in der Art und Weise, wie Kriminalität begangen und bekämpft wird. Somit ist auch eine Verlagerung hin zu digitalen Straftaten und eine Steigerung der Fallzahlen im Bereich Cybercrime und Tatmittel Internet zu beobachten. Nicht nur die Anzahl an Straftaten steigt, sondern auch deren Professionalität, was sich im enorm ansteigenden Schaden widerspiegelt. Die Zahl der Fälle von sexuellem Missbrauch von Kindern und Jugendlichen über visuelle Medien ist zudem besonders deutlich gestiegen.

Diese Zunahme von Anzeigen bedeutet gleichzeitig einen Anstieg von auszuwertenden Daten. Das erfordert eine wirksame Kriminalitätsvorbeugung und -bekämpfung in Bayern, Lösungen für den Umgang mit der wachsenden Menge digitaler Daten und die Zusammenarbeit bei der Bewältigung der Herausforderungen, die die Digitalisierung und digitale Vernetzung mit sich bringen. Um hierbei effizient vorzugehen, ist es erforderlich, ein möglichst umfassendes polizeiliches Lagebild hierüber zu erhalten.

2022 wechselte der Fokus der Gesellschaft von der Coronapandemie auf den Angriffskrieg Russlands gegen die Ukraine und die damit einhergehende Energiekrise. Der Angriffskrieg mit seiner hybriden Kriegsführung führt unmittelbar vor Augen, welche Verwundbarkeiten durch den hohen Vernetzungsgrad von Systemen und bestehender Abhängigkeiten entstehen. Dies ist der Nährboden, den die schnelle pandemiebedingte Digitalisierung für die Cyberkriminalität geschaffen hat. Infolge des Angriffskriegs verwischen die Grenzen, nicht nur zwischen staatlichen und nichtstaatlichen Cyberkriminellen, sondern auch bei Tatorten von digitalen Angriffen, welche ebenfalls nach Deutschland überschwappen. Ein großes Thema waren dabei die kritischen Infrastrukturen, vor allem in Bezug auf die Energiekrise.

Parallel zur Digitalisierung hat sich ein differenziertes Bewusstsein im Umgang mit personenbezogenen Daten entwickelt. Seit dem Volkszählungsurteil des Bundesverfassungsgerichtes zur informationellen Selbstbestimmung von 1983 hat der Datenschutz in Deutschland und in Europa erheblich an Bedeutsamkeit gewonnen. Das effiziente Verarbeiten und Verwerten immer größer werdender Datenmengen insbesondere mittels Automatisierung ist für die Polizei eine große Herausforderung, um den hohen Stellenwert informationeller Selbstbestimmung gerecht zu werden.

Das bayerische Jahreslagebild Cybercrime wirft einen Blick auf die Kriminalitätslage dieses breit gefächerten Deliktsfeldes und erläutert die Trends aus polizeilicher Sicht. Neben differenzierten Zahlen aus der polizeilichen Kriminalstatistik wird im ersten Teil auch das Dunkelfeld im Bereich Cybercrime behandelt. Der zweite Teil dieses Berichts beschäftigt sich mit den wichtigsten aktuellen Phänomenen sowie den einschlägigen Modi Operandi.

2 Begriffsbestimmung

Der bei der Polizei bundesweit einheitlich definierte Begriff „Cybercrime“ umfasst sämtliche rechtswidrigen Taten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Ferner umfasst Cybercrime auch solche Taten, die mittels Informations- und Kommunikationstechnik begangen werden. Diese Definition beschreibt das Phänomen Cybercrime in seiner Gesamtheit. In der praktischen polizeilichen Umsetzung waren jedoch Differenzierungen erforderlich, die zu den Begrifflichkeiten „Cybercrime“ (ehemals „Computerkriminalität“) und „Internet als Tatmittel“ geführt haben.

Unter dem Begriff „Cybercrime“ werden der Definition folgend insbesondere solche Delikte zusammengefasst, in deren Tatbestandsmerkmalen selbst Elemente der Informationstechnologie enthalten sind. Aus dem Strafgesetzbuch (StGB) ergibt sich hieraus für das Berichtsjahr 2022 folgender Straftatenkatalog:

- Ausspähen von Daten (§ 202a StGB)
- Abfangen von Daten (§ 202b StGB)
- Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)
- Datenhehlerei (§ 202d StGB)
- Computerbetrug (§ 263a StGB)
- Fälschung beweiserheblicher Daten (§ 269 StGB)
- Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB)
- Falschbeurkundung und Urkundenunterdrückung im Zusammenhang mit Datenverarbeitung (§§ 271, 274 I Nr. 2, 348 StGB)
- Datenveränderung (§ 303a StGB)
- Computersabotage (§ 303b StGB)

In den Deliktsbereich der vorgenannten Taten fallen, unabhängig von der technischen Umsetzung, u. a. folgende Phänomene:

- Ausspähen von Zahlungskartendaten und sonstigen Daten im elektronischen Zahlungsverkehr im Internet (z. B. Prepaidkarten, Kreditkarten, Voucher)
- Abgreifen sonstiger personenbezogener Identifikations- und Zugangsdaten (z. B. durch Schadsoftware, Phishing-Seiten, E-Mail-Links)
- Abgreifen digitaler Signaturen (z. B. im E-Commerce und E-Government)
- Hacking (z. B. unberechtigtes Eindringen in informationstechnische Systeme)
- Überlastung von Servern durch massenhafte Anfragen, sog. Distributed-Denial-of-Service-Angriffe (DDoS)
- Verbreiten von Schadsoftware (z. B. Viren, Trojaner und Würmer)
- Aufbau und/oder Betrieb von Botnetzen (z. B. zur Verschleierung oder Anonymisierung von Täteraktivitäten)
- Computerbetrugsdelikte wie z. B. der Warenkredit- und Leistungskredit-Computerbetrug i. V. m. Online-Einkäufen, soweit ein automatisierter Abwicklungsprozess erfolgt, also eine Maschine und keine natürliche Person getäuscht wird.

Im Unterschied hierzu umfasst die Begrifflichkeit „Internet als Tatmittel“ sämtliche rechtswidrige Taten, bei denen das Internet zur Planung, Vorbereitung oder Ausführung eingesetzt wird. Hierbei steht das eigentliche Delikt im Vordergrund, während das Internet bzw. einzelne Komponenten des Internets lediglich als Tatmittel fungieren. Dabei kommen sowohl rechtswidrige Taten in Betracht, bei denen das bloße Einstellen von Informationen in das Internet bereits strafrechtlich

relevante Tatbestände erfüllt (sog. Äußerungs- bzw. Verbreitungsdelikte), als auch solche Delikte, bei denen das Internet als Kommunikationsmedium bei der Tatbestandsverwirklichung eingesetzt wird. Zur Orientierung dienen folgende Beispiele:

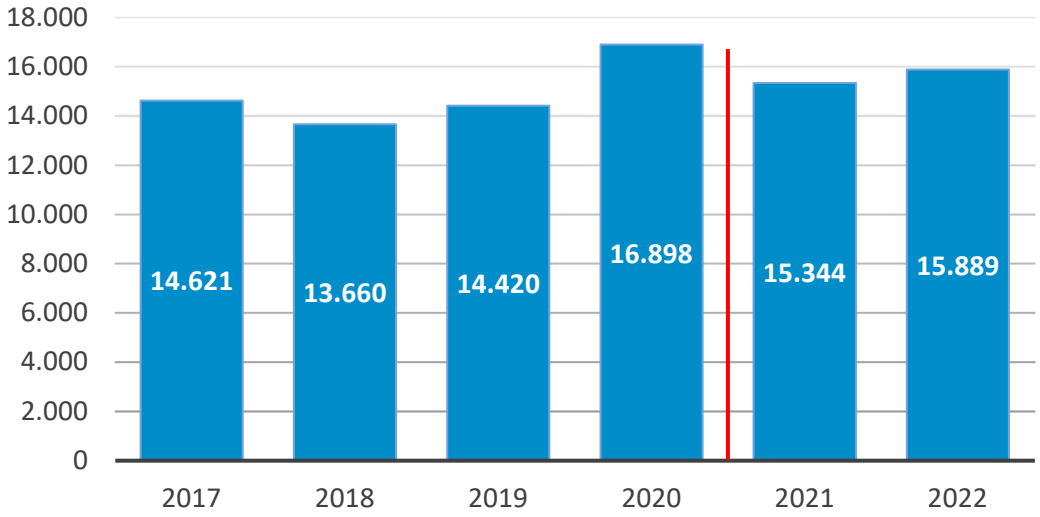
- Verbreitung und Besitzverschaffung von kinder-/jugendpornografischen Schriften
- Betrugsdelikte wie z. B. der Waren(-kredit)- und Leistungs(-kredit)betrug in Verbindung mit Online-Auktionen bzw. Online-Shops, soweit eine natürliche Person getäuscht wird
- Verbreitung urheberrechtlich geschützter Werke über Internet-Tauschbörsen
- Beleidigung/Bedrohung mittels E-Mail

Spielt das Internet bzw. die Informationstechnologie im Hinblick auf die Tatbestandsverwirklichung allerdings eine lediglich untergeordnete Rolle, wenn beispielsweise Kontakte bzw. Kontaktversuche über das Internet zwischen Täter und Opfer der eigentlichen Tat vorgelagert sind, ist die Tat nicht der Begrifflichkeit „Internet als Tatmittel“ zuzuordnen und fällt somit nicht in den Deliktsbereich Cybercrime.

3 Kriminalitätslage

3.1 Polizeiliche Kriminalstatistik (PKS)

In der Polizeilichen Kriminalstatistik wird der Teilbereich „Cybercrime“ durch den PKS-Summenschlüssel 897000 abgedeckt, da er den unter Abschnitt 2 aufgeführten Straftatenkatalog bzw. die Deliktsschlüssel in sich vereint. Für den Berichtszeitraum 2022 weist dieser Summenschlüssel für den Freistaat Bayern insgesamt **15.889** polizeilich erfasste Fälle aus, was einer Steigerung von 3,6 % im Vergleich zum Vorjahr und einem Anteil von 2,6 % der im Jahr 2022 polizeilich registrierten Gesamttaten entspricht[1]. Hierbei sei angemerkt, dass Delikte mit unbekanntem Tatort oder mit Tatort im Ausland nicht in die Statistik einfließen.



Mit Wirkung vom 01.01.2021 wurde der PKS-Summenschlüssel 897000 im Klartext von „Computerkriminalität“ in „Cybercrime“ umbenannt. Eine inhaltliche Änderung hat zur Folge, dass der Summenschlüssel 897000 nicht mehr unmittelbar mit den Vorjahren vergleichbar ist.

[1] Der Wegfall der Softwarepiraterie führt zwar dazu, dass der Summenschlüssel nicht mehr unmittelbar mit den Vorjahren vergleichbar ist. Gleichwohl ist dieses Delikt in der Gesamtschau zahlenmäßig vernachlässigbar.

3.1.1 Einzelne Deliktsfelder

Folgende Deliktsbereiche werden in der PKS unter dem o. g. Summenschlüssel Cybercrime (897000) zusammengefasst:

Ausspähen und Abfangen von Daten inkl. Vorbereitungshandlungen (678000)

Dieser Deliktsbereich umfasst das Erlangen von Daten (z. B. Zugangsdaten, Zahlungskartendaten, digitale Dokumente) unter Überwindung informationstechnischer Zugangssicherungen ohne Phishing[2]. Hier kam es zu 1.638 (2021: 1.994) in der PKS erfassten Fällen.

Datenveränderung und Computersabotage (674200)

Dieser Deliktsbereich umfasst das Eindringen in fremde IT mit anschließender Manipulation der dortigen Daten.[3] Hier kam es zu 632 (2021: 644) in der PKS erfassten Fällen.

Fälschung beweiserheblicher Daten und Täuschung im Rechtsverkehr (543000)

Dieser Deliktsbereich umfasst die missbräuchliche Verwendung personenbezogener Daten zur Erlangung von Zugangs- oder Zahlungskartendaten (Phishing) oder zum Tätigen von Rechtsgeschäften im Internet (Identitätsdiebstahl).[4] Hier kam es zu 3.611 (2021: 3.762) in der PKS erfassten Fällen.

Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN (516300)

Dieser Deliktsbereich umfasst den Einsatz von gestohlenen oder unterschlagenen Zahlungskarten (EC-Karte, Kreditkarte) an Geldausgabeautomaten oder Zahlungsterminals mit dazugehöriger PIN. Hier kam es zu 1.296 (2021: 1.093) in der PKS erfassten Fällen.

Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten (516520)

Dieser Deliktsbereich umfasst die Verwendung von ausgespähten, abgephishten oder geskimmten[5] Zahlungskartendaten für Einkäufe im Internet. Hier kam es zu 1.305 (2021: 1.310) in der PKS erfassten Fällen.

Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel (516920)

Dieser Deliktsbereich umfasst die unautorisierte Verwendung von Schecks, Guthabenkarten oder gehackten Konten bei Zahlungsdienstleistern zur Zahlung im Internet. Hier kam es zu 1.317 (2021: 939) in der PKS erfassten Fällen.

Computerbetrug (897100)

Aufgrund der Komplexität und den vielen Möglichkeiten, Computerbetrug zu begehen, wurde speziell für diesen Straftatbestand der Summenschlüssel 897100 eingeführt. Hierunter werden neben den drei zuvor genannten Deliktsbereichen in Zusammenhang mit Zahlungskarten(daten) / Zahlungsmitteln folgende Computerbetrugsdeliktsbereiche subsumiert: Betrügerisches Erlangen von Kraftfahrzeugen (4 in der PKS erfasste Fälle), Missbräuchliche Nutzung von Telekommunikationsdiensten (9 in der PKS erfasste Fälle), Überweisungscomputerbetrug (194 in der PKS erfasste Fälle), Leistungskreditcomputerbetrug (416 in der PKS erfasste Fälle), Abrechnungsbetrug im Gesundheitswesen nach § 263a StGB (1 in der PKS erfasster Fall), Warenkreditcomputerbetrug (3.222 in der PKS erfasste Fälle) und der sonstige Computerbetrug als Auffangdeliktsschlüssel (2.244 in der PKS erfasste Fälle). Zusammengenommen entfallen auf

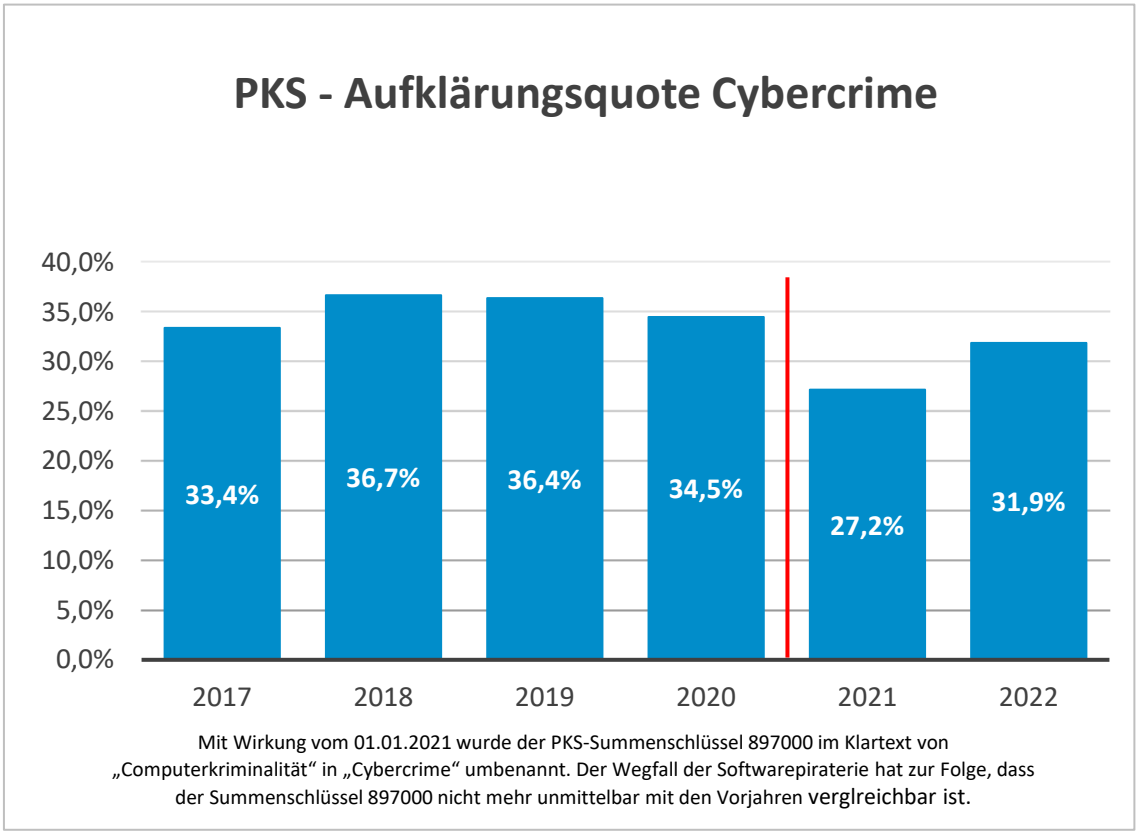
[2] Phishing: Der Versuch durch Manipulation an persönliche Daten des Internet-Benutzers zu gelangen.
[3] Besonders erwähnenswert sind hier die Phänomenbereiche DDoS-Angriffe (4.3) und Ransomware (4.4).
[4] Näheres zu Identitätsdiebstahl siehe 4.1.
[5] Skimming: Unautorisiertes Auslesen der Daten von Magnetstreifen der Bankkarten.

den Deliktsbereich Computerbetrug somit 10.008 (2021: 8.944) in der PKS erfasste Fälle

3.1.2 Aufklärungsquote

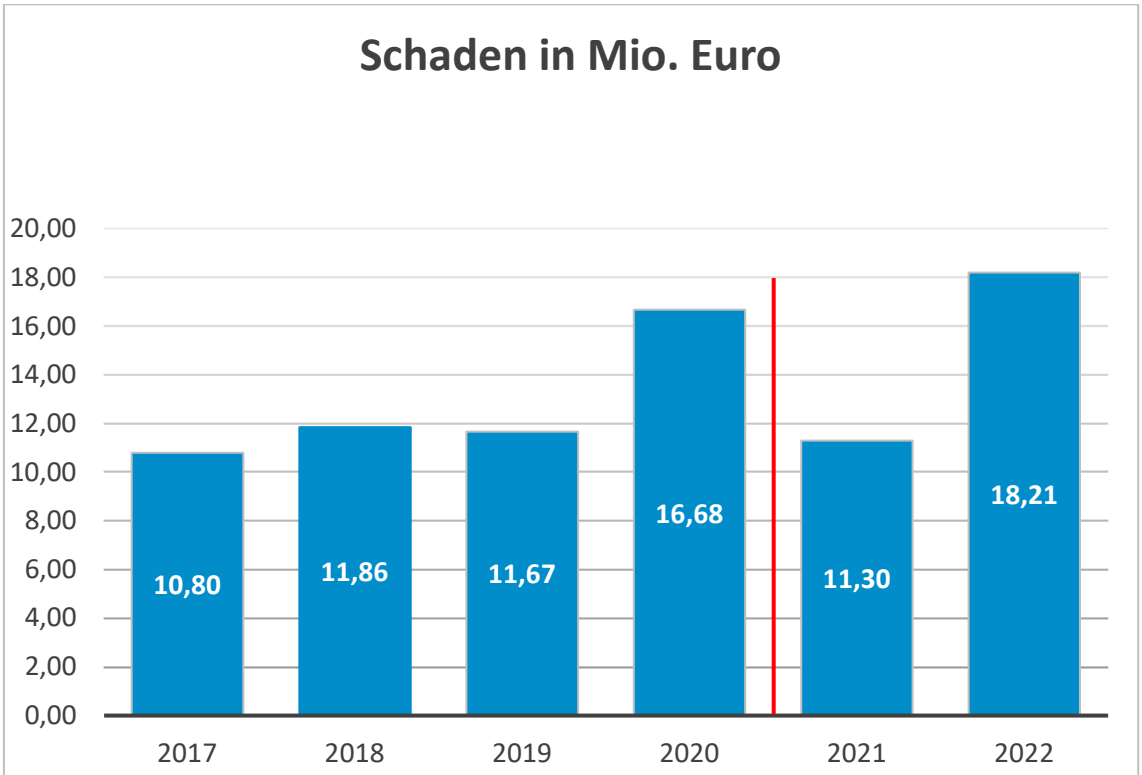
Im Jahr 2022 wurden insgesamt 5.069 Fälle aufgeklärt. Die Aufklärungsquote betrug 31,9 % und liegt damit über den 27,2 % des Vorjahres.

Maßgeblichen Anteil daran hat die 36,1 % betragende Aufklärungsquote im Deliktsbereich Computerbetrug, welcher im Vorberichtszeitraum noch 32,1 % Aufklärungsquote aufwies.



3.1.3 Schadensentwicklung gem. PKS

Gemäß PKS summierte sich der durch Cybercrime verursachte Schaden im Jahr 2022 auf 18,2 Millionen Euro. Damit steigt die Schadenssumme um rund 6,9 Millionen Euro gegenüber dem Vorjahr. Diesbezüglich ist jedoch anzumerken, dass in der bundeseinheitlichen PKS nur Schäden aus den Deliktsfeldern „Computerbetrug“ mit Tätern aus dem Inland registriert werden und in die Schadenssumme mit einfließen. Genaugenommen handelt es sich bei der in der nachfolgenden Tabelle dargestellten Schadenssumme für 2022 nur um den Beuteschaden, welcher aus dem Deliktsbereich „Computerbetrug“ resultiert. Lösegeld, das beispielsweise nach einer Verschlüsselung von IT-Systemen für deren Entschlüsselung erpresst wurde, oder Schäden, die durch eine Kompromittierung kompletter Firmennetze mit einhergehendem Produktionsausfall entstanden sind, finden in der Statistik keine Berücksichtigung. Ebenso Computerbetrugsdelikte, bei welchen der Täter nicht nachweislich aus dem Inland agiert. Diese Schadensangaben beruhen auf polizeilich erfassten Fällen, im Gegensatz zu den meisten in der Literatur angegebenen Schadenszahlen, welche aus Schätzungen bestehen.



Mit Wirkung vom 01.01.2021 wurde der PKS-Summenschlüssel 897000 im Klartext von „Computerkriminalität“ in „Cybercrime“ umbenannt. Eine inhaltliche Änderung hat zur Folge, dass der Summenschlüssel 897000 nicht mehr unmittelbar mit den Vorjahren vergleichbar ist.

3.1.4 Internet als Tatmittel

Um auch den zweiten Bereich „Internet als Tatmittel“ in Zahlen ausdrücken zu können, stehen für die Erfassung derartiger Delikte in der PKS entsprechende Sonderkennungen zur Verfügung. Deren Auswertung ergab, dass im Berichtszeitraum 2022 das Internet in 45.065 Fällen als Tatmittel eingesetzt wurde, was einem Anstieg von 14,2 % im Vergleich zum Vorjahr entspricht. Unter anderem kam das Internet als Tatmittel in folgenden Deliktsfeldern bei der Tatbestandsverwirklichung zum Einsatz:

Beleidigung (673000)

Dieser Deliktsbereich umfasst neben der Beleidigung auch die üble Nachrede und Verleumdung, welche per E-Mail, Chatnachricht oder Posting begangen wird. Hier kam es zu 2.012 (2021: 2.271) in der PKS erfassten Fällen.

Betrug (510000)

Dieser Deliktsbereich umfasst sämtliche Betrugstaten, die unter Zuhilfenahme des Internets begangen werden. Hierzu wurden 23.248 (2021: 22.137) Fälle in der PKS erfasst, was einen Großteil der Sachverhalte, die mit dem Internet als Tatmittel begangen wurden, ausmacht.

Rauschgiftkriminalität (891000)

Dieser Deliktsbereich umfasst sämtliche rechtswidrige Taten nach dem BtMG, wobei der Großteil der Anzeigen auf dem Rauschgifthandel/-erwerb im Darknet beruht. Hier kam es zu 1.768 (2021: 1.006) in der PKS erfassten Fällen.

Nötigung (232200)

Dieser Deliktsbereich umfasst neben der Nötigung auch die Bedrohung und Nachstellung (Stalking), welche über das Internet begangen und vollendet wird. Hier kam es zu 226 (2021: 218) in der PKS erfassten Fällen.

Pornografie (143000)

Zur strafbaren Verbreitung pornografischer Schriften wurde das Internet in 6.488 (2021: 4.749) angezeigten Fällen der PKS genutzt. Davon entfielen auf die Bereiche Kinderpornografie 5.249, Jugendpornografie 748, Gewalt-/Tierpornografie 39 und sonstige pornografische Schriften 452 in der PKS erfasste Fälle.

Internet als Tatmittel

Aufklärungsquote

Bei den 45.065 in der PKS erfassten Delikten mit dem Internet als Tatmittel lag die Aufklärungsquote bei 52,5 %, also 0,2 Prozentpunkte höher als im Vorjahr. Besonders hervorzuheben sind hier die hohen Aufklärungsquoten in den Bereichen Pornografie (85,6 %) und Rauschgiftkriminalität (88,1 %).

Schadenshöhe

Parallel zu den höheren Fallzahlen stieg die Schadenshöhe der mit dem Internet als Tatmittel begangenen Taten im Vergleich zum Vorjahr um 16,6 Millionen Euro auf 44,7 Millionen Euro. Wie bei der Schadensentwicklung gem. PKS bei Cybercrime im engeren Sinne (3.1.3) muss allerdings auch hier bedacht werden, dass in die genannte Schadenssumme nur die Beute-/Vermögensschäden und nicht die durch die Taten verursachten Sachschäden mit einfließen. Gleiches gilt für Anzeigen, bei welchen der Täter nicht nachweislich aus dem Inland agiert.

3.2 Auswertung der polizeilichen Vorgangsverwaltung (IGVP)

In der PKS werden derzeit nur zu im Inland begangenen Delikten Fallzahlen veröffentlicht. Im Bereich Cybercrime, in dem die Täter aufgrund der Omnipräsenz des Internets nicht an Ländergrenzen gebunden sind und weltweit von jedem Internetanschluss aus agieren können, sind viele Auslandsdelikte bzw. Delikte mit unbekanntem Tatort festzustellen.

Darüber hinaus werden Fälle von Cybercrime, bei denen in Tateinheit ein höherwertiges Delikt aus einem anderen Deliktsbereich zur PKS gemeldet wird, zwar in der Gesamtstatistik, aber nicht im Summenschlüssel „Cybercrime“ abgebildet. Als Beispiel seien hier Fälle im Zusammenhang mit Lösegelderpressungen auf Grund vorangegangener Accountübernahme im Bereich Social Media genannt. Hier stellt die Erpressung aufgrund des Strafmaßes das höherwertige Delikt gegenüber der gleichzeitig erfüllten Datenveränderung dar, weshalb diese Fälle ausschließlich unter der Rubrik „Eigentumsdelikte“ in der PKS abgebildet werden. Diesem Vorgehen liegt das bundesweit einheitlich zur Anwendung kommende Prinzip der Einmalerfassung von polizeilichen Vorgängen in der PKS zu Grunde. Bei Nichtbeachtung dieses Prinzips würde es zwangsläufig zu statistischen Fehlern kommen, da die Mehrfacherfassung von Fällen in unterschiedlichen Deliktsbereichen beispielsweise auch eine Mehrfachzählung der Täter zur Folge hätte, von denen die Straftaten begangen wurden.

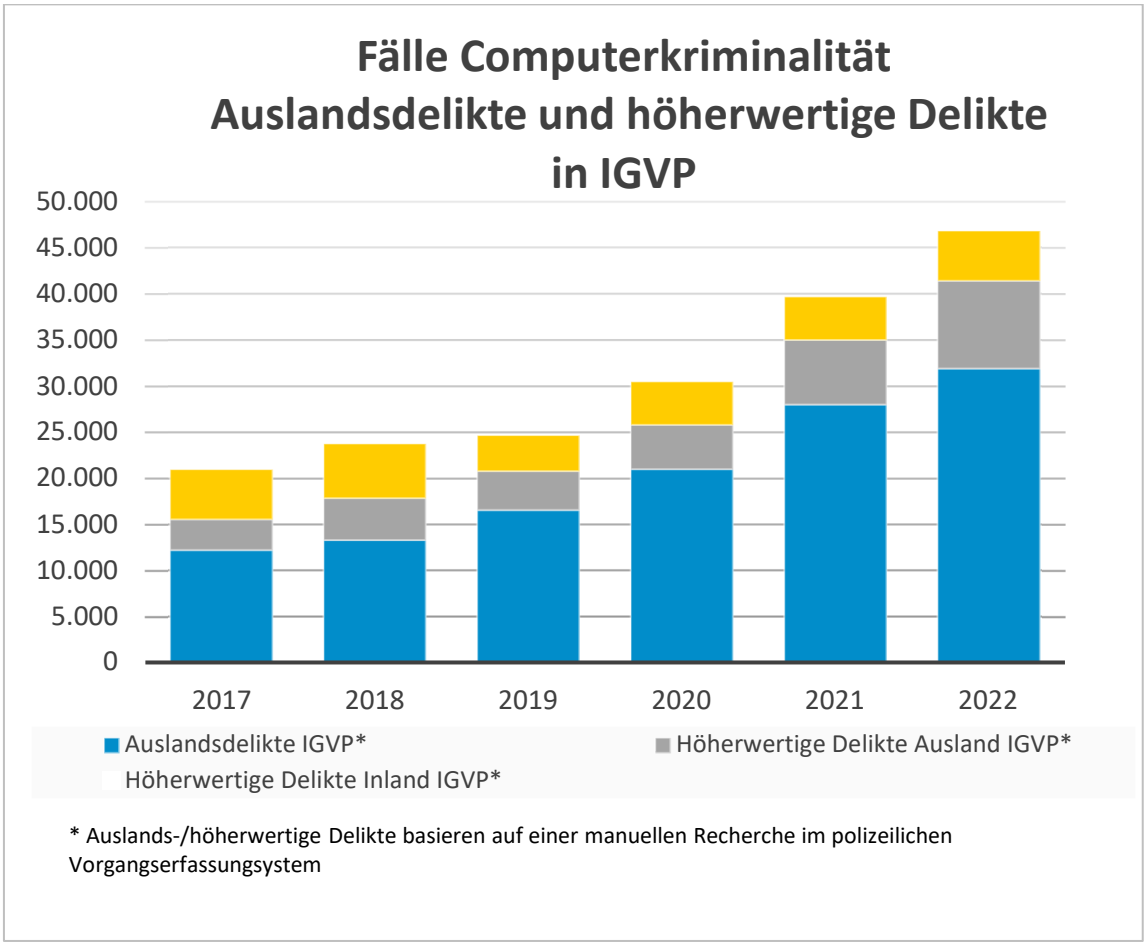
Um eine Annäherung an das spezifische Fallaufkommen im Deliktsfeld Cybercrime in Bayern zu erreichen, wird bei der Erstellung des jährlichen Lagebilds neben der Erhebung der Delikte aus der PKS stets auch eine manuelle Auswertung der polizeilichen Vorgangsverwaltung (IGVP) vorgenommen. Dabei werden im Ausland begangene Cybercrime-Delikte sowie Taten, die aufgrund eines gleichzeitig begangenen höherwertigen Delikts nicht als Cybercrime in die PKS eingehen, gesondert gezählt.

In diesem Zusammenhang wird jedoch ausdrücklich darauf hingewiesen, dass IGVP grundsätzlich ein dynamischer Datenbestand ist, der zur Erstellung polizeilicher Lagebilder geeignet ist. Auswertungen und Analysen geben damit stets nur den aktuellen Erfassungsstand zum Zeitpunkt der Abfrage wieder, der sich auch bezogen auf rückwirkende Zeiträume aufgrund laufender Ermittlungen und Qualitätssicherungsmaßnahmen kontinuierlich ändert. **Die im vorliegenden Lagebild genannten Fallzahlen aus IGVP für das Jahr 2022 stellen eine Momentaufnahme zum Stichtag 18.01.2023 dar und sind nicht reproduzierbar.** Gleichwohl lassen sich anhand der jeweiligen Entwicklungen Tendenzen feststellen und zueinander in Verhältnis setzen.

Die Auswertung von IGVP in Bezug auf Auslandsdelikte zeigte, dass dort im Berichtszeitraum ca. 31.900 entsprechende Fälle erfasst wurden.

Die IGVP-Auswertung in der Konstellation höherwertiges Delikt in Zusammenhang mit einem Cyberdelikt zeigte im Berichtszeitraum etwa 5.400 Fälle mit Tatort in Bayern und ca. 9.500 Fälle mit Tatort außerhalb Bayerns bzw. unbekannt.

Die anhand einer Auswertung von IGVP ermittelte Entwicklung über die letzten Jahre lässt sich der nachfolgenden Grafik entnehmen.



* Auslands-/höherwertige Delikte basieren auf einer manuellen Recherche im polizeilichen Vorgangserfassungsystem

3.3 Dunkelfeld

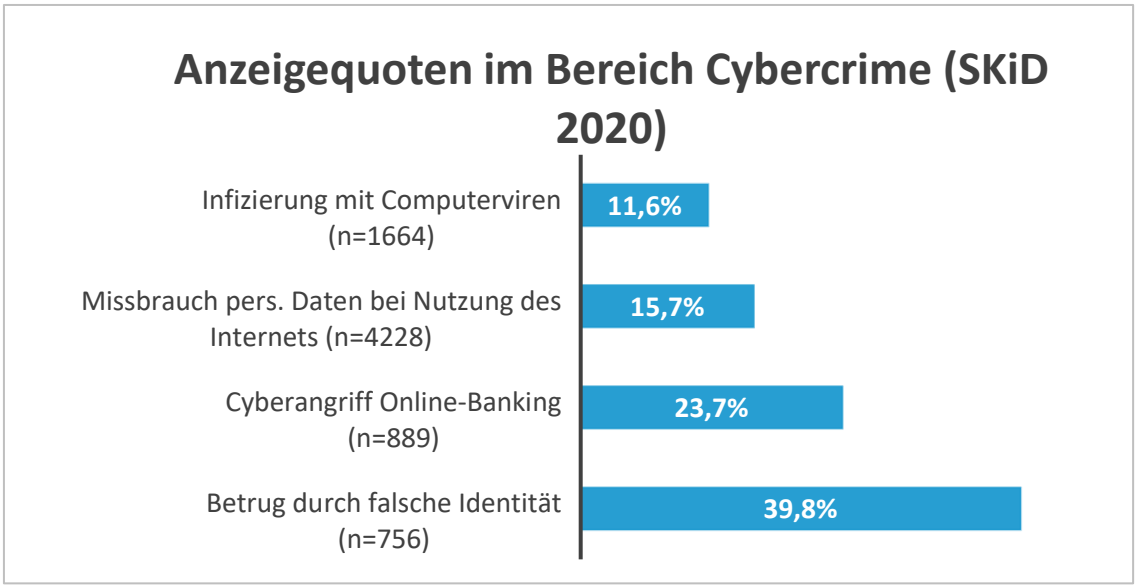
In Deutschland gab es in den letzten Jahren eine Zunahme von Krisen und gesellschaftlichen Spannungen, die Auswirkungen auf das kriminalitätsbezogene Sicherheitsempfinden der Bevölkerung haben. Diese Spannungen werden auch durch Veränderungsprozesse in der Gesellschaft wie die zunehmende Digitalisierung verstärkt. Dieses Zusammenspiel führt zu einer Zunahme von Delikten im Bereich der Cyberkriminalität. Regelmäßige repräsentative Studien, insbesondere Opferbefragungen und deren Auswertungen, sind erforderlich, um die Kriminalitätslage genauer zu verstehen. Um bei der Prävention und Bekämpfung von Cybercrime nicht nur auf Deliktszahlen im polizeilich bekannt gewordenen Hellfeld zu reagieren, sondern eine Annäherung an die Realität zu erreichen, ist ein Blick auf das Dunkelfeld unerlässlich.

Als empirische Grundlage wird für diesen Bereich die Dunkelfeldbefragung des bundesweiten Viktimisierungssurvey des Bundeskriminalamts und der Polizei der Länder „Sicherheit und Kriminalität in Deutschland - SKiD 2020“ herangezogen. Die Studie fußt auf einem entsprechenden Beschluss der Innenministerkonferenz (IMK). Aus dem Survey geht hervor, dass im Bereich der Cyberkriminalität ein besonders großes Dunkelfeld herrscht. Es werden hier nur 17,9 % der Straftaten angezeigt.

Eine Umfrage der Bitkom fällt ähnlich aus. Nur 22 % der Befragten gaben an, keine Erfahrungen mit Cyberkriminalität gemacht zu haben, 3 % wollten dazu keine Angaben machen. Drei von vier Internetnutzern waren im vergangenen Jahr von Cyberkriminalität betroffen, wovon lediglich 18 % Strafanzeige bei der Polizei stellten. An andere Behörden, wie etwa das Bundesamt für Sicherheit in der Informationstechnologie (BSI), haben sich 9 % gewandt. [67]

6 https://www.bitkom.org/Presse/Presseinformation/Drei-Viertel-Cyberkriminalitaet-betroffen (04.01.2023)
7 Die repräsentative Umfrage im Auftrag von Bitkom wurde unter 1014 Personen ab 16 Jahren in Deutschland durchgeführt.

Die folgende Abbildung zeigt das Anzeigeverhalten bei den einzelnen Vermögensdelikten im Bereich Cybercrime:



Das Diagramm illustriert im Bereich der Cyberkriminalität geringe Anzeigequoten. Vergleichsweise werden bei einem vollendeten Wohnungseinbruchsdiebstahl 87,6 % und bei einem Versuch 57,9 % der Taten zur Anzeige gebracht.

Gründe für und gegen eine Anzeige

Gründe für eine Anzeige (SKiD 2020)	Täter/in sollte gefasst/ bestraft werden	Um andere vor Tä-ter/in zu schützen	Weil so etwas nicht noch ein-mal passieren sollte	Nachweis für Versi-cherung benötigt	Um Scha-densersatz v. Täter/in geltend zu machen	Gestohlene Sachen sollen gefunden werden
Betrug durch falsche Identität (n = 116)	85,0%	79,6%	82,5%	2,2%	32,7%	17,2%
Infizierung mit Computerviren (n = 55)	83,9%	60,9%	62,7%	14,1%	1,2%	0,3%
Cyberangriff Online-Banking (n = 65)	54,6%	72,3%	67,4%	47,6%	45,0%	4,4%
Missbrauch pers. Daten bei Internetnutzung (n = 306)	75,8%	75,2%	70,8%	36,3%	36,7%	4,9%

Der häufigste von den befragten Bürgern genannte Grund Anzeige zu erstatten ist, dass der Täter gefasst und bestraft werden sollte. Der am zweithäufigsten genannte Grund ist, dass durch die Benachrichtigung der Polizei andere vor dem Täter oder der Täterin geschützt werden sollen. Bei Opfern von Cyberangriffen auf das Online-Banking ist dies sogar der am häufigsten genannte Grund für eine Anzeige. Eine nahezu gleichermaßen häufig genannte Motivation ist: „weil so etwas nicht noch einmal passieren sollte“.

Einer der am meisten genannten Gründe gegen eine Anzeige bei Internetdelikten lautet, dass die Tat als nicht schwerwiegend genug wahrgenommen werde. Ebenso oft genannt ist die Auffassung, dass die Polizei den Fall nicht aufklären könne. Im Bereich der Betrugs- und Internetkriminalität nennen 24 % bis 45 % der Opfer diesen Grund für ihre Entscheidung gegen eine Anzeige. Beim Betrug durch falsche Identität nimmt die Annahme, dass es keine Beweise für die Straftat gäbe, einen hohen Stellenwert bei der Entscheidung gegen eine Anzeigeerstattung ein. Dass die Straftat nicht der Polizei gemeldet wird, weil die „Angelegenheit selbst geregelt“ wird, ist insbesondere bei Cyberangriffen auf das Online-Banking mit 42,8 % relevant.

Fazit

Die Ergebnisse der SKiD-Befragung 2020 zeigen, dass Cyberkriminalität ein besonders auffälliger Deliktsbereich ist. Mit der zunehmenden Digitalisierung des täglichen Lebens wird das Internet für viele Bürgerinnen und Bürger immer wichtiger, aber auch riskanter. Laut den Ergebnissen von SKiD gab es die meisten Opfer in diesem Bereich. Allerdings werden nur wenige Straftaten im Internet von den Opfern angezeigt, was zu einem großen Dunkelfeld in der Kriminalstatistik führt. Unter anderem um diesen Teil der Cyberkriminalität den Strafverfolgungsbehörden zugänglicher zu machen, wurde das Netzwerkdurchsetzungsgesetz (NetzDG)[8] eingeführt, das Anbieter von sozialen Netzwerken verpflichten soll, bestimmte Straftaten an eine Zentralstelle im Bundeskriminalamt zu melden. Dies wird aufgrund Klage-/Eilverfahren bei keinem Verpflichteten durchgesetzt. Aber auch in Zukunft wird dies das gesamte Spektrum von strafrechtlich relevanten Risiken im Internet nicht abdecken. Daher wird es auch in Zukunft wichtig sein, die Sicherheitslage permanent zu beobachten, um die Bürger in Deutschland auch im Internet vor Kriminalität zu schützen.

[8] vgl. Abschnitt 5

3.4 Besondere Entwicklungen

Die aktuelle Lage in Bayern ist durch ein multithematisches Geschehen geprägt. Maßgeblich bestimmt der nach wie vor anhaltende Angriffskrieg Russlands gegen die Ukraine die mediale Berichterstattung. Darüber hinaus sind zunehmend die Folgen des Kriegs – und hier insbesondere der potentiellen Mangel an Ressourcen – in den Fokus der Öffentlichkeit gerückt. Neben Privatpersonen zielen Cyberangriffe auch mehr auf Unternehmen und Behörden ab. Vor dem Hintergrund der allgemeinen Bedrohungslage durch das Ausspähen, Verändern oder Zerstören von Daten sowie anderer Beeinträchtigungen mittels Manipulation und Sabotage von Servern erfahren gerade Institutionen eine steigende Belastung durch prorussische Cyberkriminelle. In diesem Kontext ergeben sich ein anwachsendes Gefahrenpotenzial und erhöhte Auswirkungen durch digitale Angriffe auf Wirtschaft und Infrastruktur, die grundlegend für den Erhalt des Lebensstandards und der öffentlichen Sicherheit und Ordnung sind. Auch die Veranstaltung des G7-Gipfels auf Schloss Elmau stellte die Bayerische Polizei hinsichtlich der diesjährigen Ereignisse vor Herausforderungen.

G7-Gipfel in Bayern

Die Bundesrepublik Deutschland hatte am 01.01.2022 turnusmäßig die Präsidentschaft der Gruppe der Sieben (G7) übernommen und war vom 26. bis 28.06.2022 Gastgeber des G7-Gipfels auf Schloss Elmau. Im Vergleich zum Jahr 2015 wurde der Thematik Cyberkriminalität eine wesentlich größere Bedeutung zugemessen und im Einsatzabschnitt „Kriminalpolizeiliche-Maßnahmen“ ein eigener Unterabschnitt „Cybercrime“ gebildet.

Von Seiten des Planungsstabs wurde großer Wert auf die Cybercrime-Präventionsberatung gelegt, weshalb die Zentrale Ansprechstelle Cybercrime (ZAC) im BLKA bereits weit im Vorfeld entsprechende Beratungsgespräche und Onlineveranstaltungen durchführte. Hierdurch konnten die durch den Planungsstab priorisierten Bedarfsträger erreicht und deren IT-Sicherheitsverantwortliche für die besondere Gefährdungslage hinsichtlich Cyberattacken im Kontext des G7-Gipfeltreffens sensibilisiert werden. Im Ergebnis wurden die Präventionsmaßnahmen von den Bedarfsträgern durchweg positiv angenommen.

Das Straftatenaufkommen war im Bereich Cyberkriminalität sehr überschaubar, letztendlich musste nur ein konkreter Vorfall bearbeitet werden. Am 19.06.2022, eine Woche vor der eigentlichen Veranstaltung, wurden drei Hyperlinks in Zusammenhang mit vertraulichen Polizeidokumenten aus dem G7 Gipfel 2015 von „anonym“ unter der URL https://de.indymedia.org veröffentlicht. „Indymedia“ ist ein Zusammenschluss von unabhängigen Medienorganisationen und hunderten von Journalisten, die nichthierarchische, nicht konzerngebundene Berichterstattung leisten. Die drei Links führten zu je einer Plattform in Österreich und Tschechien sowie zur Domain der Piratenpartei. Von Seiten der zuständigen Staatsanwaltschaft wurden keine Straftaten aus dem Bereich der Cyberkriminalität festgestellt. Es wurde ein Verfahren wegen des Verdachts eines Vergehens der Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht gem. § 353b StGB eingeleitet und die Sachbearbeitung durch das Dezernat 13 - Interne Ermittlungen des BLKA mit fachlicher Unterstützung durch das Dezernat 54 - Cybercrime übernommen.

Angriffskrieg Russlands gegen die Ukraine

Nach dem Ausbruch des Ukrainekrieges wurde die ständige Bewertung der Bedrohungslage vor allem im Bereich der Cybersicherheit sehr wichtig, auch für die Behörden mit Cybersicherheitsaufgaben in Bayern. Diese hatten sich bereits Anfang 2020 in der Cyberabwehr Bayern zusammengeschlossen und eine Austauschplattform aufgebaut (vgl. Abschnitt 7). Über diese ist eine permanente gemeinsame Bewertung der Situation sowie ggf. die kurzfristige Reaktionsmöglichkeit der beteiligten Behörden in Bayern sichergestellt.

Basierend auf der aktuellen Informationslage sind gezielte Cyberangriffe auf Deutschland durch russische staatliche Strukturen relativ unwahrscheinlich, Kollateralschäden mit Deutschlandbezug jedoch nicht auszuschließen. Dies gilt ebenso für mögliche Kollateralschäden durch Angriffe der Ukraine auf russische Einrichtungen. Zudem birgt die unübersichtliche Lage sich mit Kriegsparteien solidarisierender, aber staatlich nicht gesteuerter Cybercrime-Gruppen die Gefahr ungerichteter und wenig maßvoller Angriffe, von denen Deutschland direkt oder durch Kollateralschäden betroffen sein könnte.

Im Ergebnis sind bislang die Hinweise auf politische Bezüge zumeist nicht eindeutig, ausgenommen die offen pro-russisch auftretende Angreifergruppierung KillNet, welche bereits seit März 2022 DDoS-Angriffe auf Institutionen und Unternehmen in Ländern durchführt, welche die Ukraine in irgendeiner Form aktiv unterstützen. Darunter befanden sich vorwiegend im Mai 2022 auch 80 Webseiten (u. a. von Sicherheitsbehörden, Banken und Flughäfen) in Deutschland. Des Weiteren agierte die Gruppierung Anonymous offen pro-ukrainisch im Bereich des Diebstahls von Daten mit anschließender Veröffentlichung. Hier lag der Schwerpunkt bei Unternehmen des Energiesektors, die enge Geschäftsbeziehungen mit Russland unterhalten. Insgesamt wird zwar eine abstrakte Gefährdung durch Cyberangriffe von allen Behörden übereinstimmend konstatiert, die sich bislang glücklicherweise nicht konkretisiert hat. Die Cyberangriffe Russlands beschränken sich bislang auf die Ukraine selbst als kriegsbegleitende Maßnahmen zur Destabilisierung der kritischen Infrastrukturen. Der regelmäßige Informationsaustausch mit den Behörden des Bundes ist essentiell für die gemeinsame Bewertung.

Aus den Daten von XVigil, einer auf künstlicher Intelligenz basierender Risikoüberwachung der Firma CloudSEK geht hervor, dass die Zahl der Angriffe auf den Regierungssektor in der zweiten Jahreshälfte 2022 um 95 % gestiegen ist, verglichen mit dem gleichen Zeitraum im Jahr 2021.[9] In Zusammenhang mit Angriffen auf staatliche Akteure fällt im vergangenen Jahr immer häufiger das Wort „Hacktivisten“. Was für viele ein Neologismus scheint, ist ein Wort das bereits seit Ende der 90er Jahre existiert.[10] Diese Cyberkriminellen setzen in erster Linie leicht verfügbare Cyber-Tools wie Distributed Denial of Service (DDoS), Schwachstellen-Scanner und Doxing[11] ein, um Regierungen, Organisationen und Einzelpersonen zu stören und zu diffamieren. Diese nichtstaatlichen Akteure rechtfertigen Cyberangriffe mit ethischen Beweggründen und nutzen Cyberbedrohungen, um ihre Ziele durchzusetzen.

[9] „Unprecedented Increase in Cyber Attacks TargetingGovernment Entities in 2022“ von Cloudsek; Autoren Hansika Saxena und Aastha Mitta (https://cloudsek.com/whitepapers_reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022/)

[10] https://www.heise.de/tp/features/Infowar-und-politischer-Aktivismus-3446265.html(17.01.2023)

[11] Unautorisierte Veröffentlichung fremder privater Daten

Die bereits erwähnte kriminelle Organisation KillNet hat in 2022 besonders für Aufsehen gesorgt. Im April trat die kriminelle Gruppierung erstmals auch in Deutschland in Erscheinung. Durch gezielte DDoS-Angriffe wurde die Erreichbarkeit der Webseiten der Bundeswehr kurzzeitig eingeschränkt. Weiterhin waren auch die Internetauftritte der deutschen Flughäfen Hamburg und Bremen sowie der Kreditanstalt für Wiederaufbau (KfW) und der Commerzbank Ziel. Bei den Angriffen auf deutsche Einrichtungen handele es sich um Reaktionen auf die Unterstützung der Ukraine durch u. a. deutsche Rüstungshilfen.

DDoS-Angriffe auf die Bayerische Polizei

In der Nacht vom 02.05.2022 auf den 03.05.2022 kam es zu mehreren Distributed Denial of Service (DDoS) Angriffen auf die Webpräsenz der Bayerischen Polizei. Einem Telegram-Eintrag zur Folge ist der Angriff der prorussischen Gruppierung KillNet zuzuschreiben. Vorher hatte die Gruppierung mit Angriffen gegen deutsche Infrastruktur gedroht und dabei mehrere Domains staatlicher Institutionen, darunter u. a. bundestag.de, bmvg.de, bundespolizei.de sowie polizei.bayern.de, explizit erwähnt. Hintergrund war hierbei wohl der Protest gegen die Waffenlieferungen Deutschlands an die Ukraine.

Am Abend des 02.05.2022 kündigte Killnet via Telegram weitere DDoS-Angriffe in Deutschland an. Ab 21:00 Uhr, ca. eine Stunde nach der Veröffentlichung, erfolgten erste Angriffe auf deutsche Internetseiten. Die Ankündigung bezog sich im Schwerpunkt auf deutsche Regierungsstellen. Neben den Internetauftritten mehrerer Landespolizeien wurden unter anderem auch das BMVg, das BKA, der BND und die BPOL als potenzielle Ziele genannt. Auch Angriffe auf die Internetauftritte des Bundeskanzlers sowie des Deutschen Bundestages waren darin enthalten.

Die Medienpräsenz von „Hacktivismus“ wurde auch von Betrügern für Erpressungsmails mit Bezug zum Angriffskrieg Russlands auf die Ukraine missbraucht. Hier geben sich die Cyberkriminellen als ukrainische Hacker aus und Lösegelder werden als Spenden beschönigt. Eine neue Variante hierbei war die

Stromausfall in der Ukraine bereits in 2015

Am 23.12.2015 kam es zu dem einem großen Stromausfall, von welchem ca. 230.000 Kunden in der Ukraine betroffen waren. Der Vorfall ereignete sich vor dem Hintergrund des politischen Konflikts zwischen Russland und der Ukraine Im Zusammenhang mit der Krim. Somit war der Verdacht naheliegend, Russland könne den Blackout verursacht haben. Auch das BSI machte Russland für die Cyberattacke verantwortlich.

Drohung, die Onlinepräsenz des Opfers unautorisiert zu verändern und ein Banner mit Aufforderung der Ukraine zu Spenden einzublenden, falls die „Spende“ nicht gezahlt wird. Hierbei ist dem BLKA jedoch kein Fall bekannt, bei welchem die Drohung umgesetzt wurde.

Energiekrise

In der Elektrizitätsbranche hat Russland bereits 2015 in der Ukraine bewiesen, dass es grundsätzlich in der Lage und willens ist, die Energieversorgung anderer Länder anzugreifen.

Der Einsatz von Industroyer2, eine Malware, welche speziell für den Einsatz gegen Elektrizitätsnetzwerke programmiert wurde, hat gezeigt, dass destruktive Cyberangriffe weiterhin eine Option für Russland in seinem Angriffskrieg gegen die Ukraine darstellen. Spätestens mit der veränderten sicherheitspolitischen Lage seit Beginn des russischen Angriffskriegs gegen die Ukraine muss damit gerechnet werden, dass die Kritischen Infrastrukturen auch in Deutschland zu einem potenziellen Ziel von Sabotageaktionen Russlands und anderer pro-russischer Akteure werden können.

Hinzu kommt, dass die Energieversorgung, insbesondere durch die Unterbrechung der

russischen Gaslieferungen und die daraus resultierenden möglichen Gasengpässe und damit steigenden Energiekosten, derzeit starken Veränderungen ausgesetzt ist. Aus diesem Grund rückt sie in den Mittelpunkt eines kontroversen gesellschaftlichen Diskurses in Deutschland. Angriffe auf den Energiesektor sind daher nicht nur prinzipiell geeignet, hohe wirtschaftliche Schäden hervorzurufen, sondern auch, das Sicherheitsgefühl der Bevölkerung empfindlich zu beeinträchtigen. Darüber hinaus können Angriffe auf den Energiesektor dazu beitragen, Narrative in Desinformationskampagnen zu formen und zu beeinflussen, um politischen Druck zu unterstützen. Eine konkrete Gefährdung für die deutsche Stromversorgung besteht derzeit laut einhelliger Bewertung der Experten nicht.

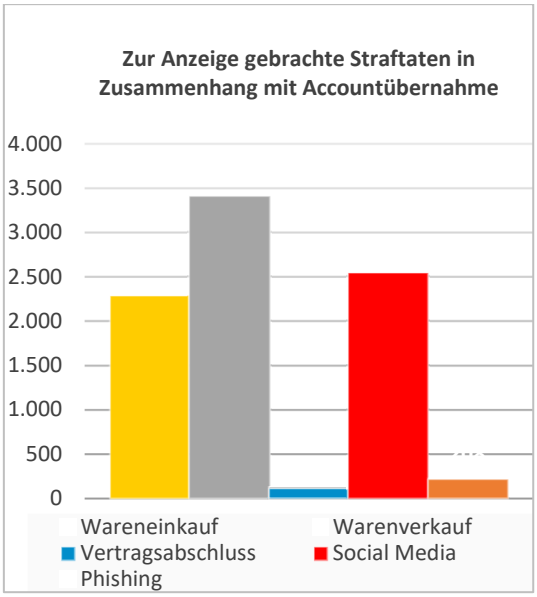
Nicht nur staatliche Akteure und Hacktivisten ziehen ihren Nutzen aus der Energiekrise, auch andere Cyberkriminelle versuchen durch die Krise zu profitieren. Beispielsweise wurden durch den Anstieg von Energiekosten Brennholz und Pellets in Fakeshops angeboten, meist deutlich günstiger als in legalen Online-Shops. Bei der oftmals großen Anzahl an bestellten Mengen entstanden so in vielen Fällen hohe Beuteschäden.

4 Aktuelle Phänomene

Im Folgenden werden in Bayern häufig auftretende Cybercrime-Phänomene und Modi Operandi dargestellt. Bei den jeweils angegebenen Fallzahlen handelt es sich – soweit nicht anders angegeben – um manuell recherchierte Zahlen aus der polizeilichen Vorgangsverwaltung IGVP, welche den Deliktsbereich Cybercrime auf die einzelnen Phänomene zugeschnitten beziffern.[12]

4.1 Identitätsdiebstahl

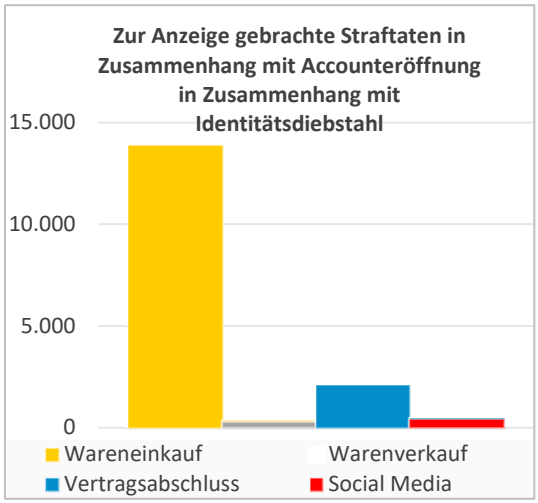
Von Identitätsdiebstahl wird gesprochen, wenn personenbezogene Daten einer natürlichen Person durch Dritte missbräuchlich verwendet werden. Vor allem während der Coronapandemie, in denen vermehrt Rechtsgeschäfte über das Internet abgewickelt wurden und physischer Kontakt eingeschränkt war, gewann dieses Phänomen zunehmend an Bedeutung und ist zu einer Art Massenphänomen mutiert. Durch die aktive Nutzung des Internets baut sich der Anwender eine digitale Identität auf, die sämtliche Nutzer-Accounts in verschiedenen sozialen Netzwerken, Online-Shops, Auktionsplattformen, Cloud-Diensten und im Online-Banking umfasst und ein begehrenswertes Ziel für Cyberkriminelle darstellt. Durch kriminelle Handlungen wollen die Täter einen Zugang zu derartigen Accounts sowie die darin enthaltenen personenbezogenen Daten erlangen und diese für eigene Zwecke missbrauchen. Sei es, um die erlangten Daten auf digitalen Schwarzmärkten zu verkaufen oder um die Daten selbst für betrügerische Online-Einkäufe einzusetzen. Insgesamt kam es 2022 zu ca. 8.500 Anzeigen (2021: ca. 5.000 Anzeigen) wegen derartiger Accountübernahmen. Somit stiegen die Fallzahlen im Vergleich zum Vorjahr erheblich. Die aktuelle Fallzahl setzt sich gemäß dem jeweils im Anschluss an die Accountübernahme getätigten Identitätsmissbrauch wie folgt zusammen:



Die Accountneueröffnung bezeichnet den Missbrauch von aus dem realen Leben bekannten personenbezogenen Daten. Mit diesen werden unbefugt im Internet digitale Identitäten angelegt sowie Bestellungen auf Rechnung getätigt, um die Waren in der Folge an Packstationen liefern zu lassen, wo diese anonym vom Täter abgeholt werden können, ohne dass dieser namentlich jemals in Erscheinung getreten ist. Diese Variante stellt insbesondere in Deutschland eine immer weiter zunehmende Deliktsform dar. Die mangelnde Durchführung von rechtsver-

[12] Zur qualitativen Einordnung darf auf die Ziffer 3.2 verwiesen werden.

bindlichen Identitätsfeststellungen in zahlreichen Online-Shops und Auktionshäusern öffnet den Tätern Tür und Tor für betrügerische Anschlusstaten. Opfer des Identitätsdiebstahls erfahren meist erst nach mehreren Wochen von der Tat, wenn sie beispielsweise von Inkassobüros per Post kontaktiert werden. Diese Variante der Accounteröffnung mit Echtpersonalien einer anderen Person führte 2022 zu ca. 16.700 Anzeigen (2021: 16.000 Anzeigen), die sich bezogen auf die Zielrichtung der missbräuchlichen Nutzung wie in folgender Grafik verzeichnet aufteilen.



Mit insgesamt ca. 25.200 Anzeigen steigt somit das Phänomen Identitätsdiebstahl insgesamt deutlich an.

4.2 Inkriminierte digitale Bezahlsysteme

Für einen Betrug mittels Onlinebezahldienst beschafft sich der Täter illegal die Zugangsdaten eines Kontos. Ist ein Bankkonto als Zahlungsquelle hinterlegt, haben die Kriminellen leichtes Spiel. Denn hier greifen die PSD2-Richtlinien nicht, die zweite Kontrolle fällt also aus. Für die Kunden mag das Bezahlen auf diesem Weg schnell und bequem sein. Für die Betrüger ist es jedoch eine attraktive Lücke im Sicherheitssystem.

Online-Händler befinden sich immer im Zwiespalt zwischen Sicherheit und Komfort für den Käufer. Umständliche und langwierige Registrierungsverfahren können schließlich zu einem Kaufabbruch führen und die Händler Umsatz kosten. Selbst wenn dies eine Möglichkeiten für Kriminelle bietet, so möchte kaum ein Online-Händler auf den Kauf auf Rechnung verzichten, da diese Bezahlmöglichkeit viele Neukunden generiert.

PSD2-Richtlinien

Auf die hohe Zahl an Cardingvorfällen reagierte die Europäische Kommission 2019 und führte am 14. September eine verpflichtende Zwei-Faktor-Authentifizierung durch die PSD2-Richtlinien ein. Diese sind Richtlinien zur Regulierung von Zahlungsdiensten und Zahlungsdienstleistern mit Geltungsbereich in der gesamten EU und dem EWR. Demnach gilt für Online-Shops verpflichtend - mit Ausnahme von Kleinbeträgen - eine Authentifizierung mittels zweier Faktoren für den Endverbraucher, auch Starke Kunden Authentifizierung (SKA) genannt. Die zwei Faktoren werden aus den Bereichen „Haben“ (z. B. Schlüsseldatei) „Sein“ (Fingerabdruck, Iris etc.) und „Wissen“ (PIN oder Kennwort) gewählt.

Ein größeres Problem als die Accountübernahme von Bezahldienstleistern stellen die Neueröffnungen da. Die Opfer bekommen dann ein Schreiben von einem Inkasso-Unternehmen, weil sie unbekannte Ware, die sie angeblich erhalten haben, bezahlen sollen. Sie halten das Schreiben für unberechtigt und eine Betrugsmasche. Allerdings landen solche Opfer oft in den Datenbanken von Bonitätsermittlern wie der Schufa und haben ohne eigenes Verschulden die Konsequenzen daraus zu tragen. Im Nachgang müssen die Opfer eine Anzeige bei der Polizei aufgeben. Viele sehen sich in der Beweispflicht gegenüber den Inkassofirmen und versuchen zu belegen, dass die Ware gar nicht selbst bestellt wurde, um im schlimmsten Fall einem Gerichtsvollzug mit Pfändung zu entgehen.

Mit ca. 2.750 solcher Betrugsfälle im Jahr 2022 ist dieses Phänomen zahlenmäßig nicht herausragend gestiegen.

Ein gehäuftes Aufkommen von Betrugstaten in Zusammenhang mit ukrainischen PayPal-Konten und den Online-Verkaufsportalen Ebay-Kleinanzeigen und Vinted ist festzustellen. Dabei werden Waren zum Kauf angeboten und nicht geliefert. Die Bezahlung der Waren erfolgt an ukrainische PayPal-Konten der Täter mit der Zahlungsoption „Freunde und Familie“, daher ohne Käuferschutz. Käufer erhalten somit einerseits keine Erstattung durch PayPal und andererseits stellt PayPal bei ukrainischen Konten keine Täterdaten zur Verfügung. Für die Polizei bestehen daher auch weniger Ermittlungsansätze. Die Ursache ist darin zu sehen, dass seit 17.03.2022 PayPal eigenen Angaben zufolge aus humanitären Gründen seine Dienstleistungen für ukrainische PayPal-Accounts ausgeweitet hat, unter anderem durch Peer-to-Peer Zahlungen, Verzicht auf Gebühren, Möglichkeit der Abbuchung von Geldbeträgen auf hinterlegte Debit- und Kreditkarten sowie Einrichtung von PayPal-Konten durch geflüchtete Ukrainer aus dem Ausland. Dadurch wurden derartige Konten auch für Kriminelle interessant, um ihre Identität besser zu verschleiern.

4.3 DDoS-Angriffe (Distributed Denial of Service)

Unter dem Begriff DoS bzw. DDoS (dt. dezentralisierte Dienstblockade) versteht man in der Informationstechnologie die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Um eine solche Nichtverfügbarkeit von Websites oder anderen Internetservices zu erreichen, bedienen sich Internetkriminelle zunächst bestimmter Schadsoftware, mit der sie eine möglichst große Anzahl an Rechnern infizieren, um so die Kontrolle über diese zu erlangen. Die Gesamtheit sowie den Zusammenschluss sämtlicher infizierter Rechner bezeichnet man als „Botnetz“. Der eigentliche DDoS-Angriff besteht nun darin, mit Hilfe der gekaperten Rechner (Bots) zeitgleich eine Fülle an Datenpaketen an den jeweiligen Webserver zu schicken, bis dieser keine Kapazitäten mehr hat, um die Daten zu verarbeiten und folglich den Dienst einstellt.[13]

Je größer ein solches Botnetz ist, desto mehr Durchschlagskraft hat ein DDoS-Angriff und umso wahrscheinlicher ist es, dass der Angriff auch gut geschützte Systeme lahmlegt. Gerade in Zeiten, in denen das Internet und die digitale Vernetzung in immer mehr Lebensbereiche vordringen, gewinnen IoT[14]-Geräte zunehmend an Bedeutung für Internetkriminelle. So werden internetfähige Fernseher, Überwachungskameras, Smartwatches oder auch Kühlschränke vom Hersteller meist mit simplen oder gänzlich ohne Passwörter ausgeliefert. Die Firmware der IOT-Geräte wird zudem selten aktualisiert, wodurch sie zu attraktiven Zielen für automatisierte Angriffe aus dem Internet werden. Einmal infiziert, fungieren IoT-Geräte gleich einem Rechner in einem Botnetz.

2022 konnte ein Anstieg in Professionalität der DDoS-Angriffe verzeichnet werden. Die Angriffe erfolgten mit einer höheren Durchschnitts- und Maximal-Bandbreite.

Wie auch im Falle der Verschlüsselung durch Schadsoftware versuchen Internetkriminelle durch die Androhung und Untermauerung ihrer Drohung mit einer abgeschwächten DDoS-Attacke einen monetären Gewinn in Form von digitalen Währungen, wie z. B. Bitcoin[15], zu erzielen. Daneben spielen, wie bereits im Abschnitt 3.4 erwähnt, bei DDoS-Angriffen auch politische oder ideologische Motive eine Rolle. In Bayern wurden im Jahr 2022 insgesamt ca. 40 DDoS-Angriffe – und damit eine geringere Anzahl als im Vorjahr – polizeilich gemeldet. Erpressungsversuche im Rahmen von Fake-E-Mailwellen mit vermeintlichen DDoS-Attacken wurden als Versuch gewertet und fließen somit in die Statistik als solche mit ein. Diese Fake-E-Mailwellen sind nur noch einzeln zu beobachten und erklären somit die gesunkenen Fallzahlen der letzten Jahre.

[13] Man kann sich einen DDoS-Angriff vereinfacht so vorstellen, dass eine große Anzahl an Internetnutzern auf Befehl gleichzeitig eine bestimmte Internetseite aufruft, wodurch der Server, auf dem der Internetauftritt gehostet ist, abstürzt, weil er durch die Menge an zeitgleichen Anfragen überlastet ist. Der Unterschied zu dieser Veranschaulichung besteht lediglich darin, dass bei einem Botnetz der Rechner ohne Zutun und Wissen des Nutzers die Internetseite aufruft.

[14] Internet of Things (dt. Internet der Dinge) ist ein Sammelbegriff für Technologien, die es ermöglichen, physische und virtuelle Gegenstände miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen.

[15] Bitcoin (dt. digitale Münze) bezeichnet ein weltweit verfügbares dezentrales Zahlungssystem mit virtuellem Geld, dessen Umrechnungskurs sich durch Angebot und Nachfrage bestimmt.

4.4 Malware/Ransomware

Der Begriff Ransomware setzt sich aus den englischen Begriffen malware (dt. Schadprogramm)und ransom (dt. Lösegeld) zusammen und bezeichnet sämtliche Computerprogramme, welche den User bis zur Zahlung eines gewissen Geldbetrages an der Nutzung seines Computers oder am Zugriff auf seine Daten hindern. Man unterscheidet zwei verschiedene Arten von Ransomware: zum einen die Verhinderung der Nutzung des Rechners durch einen auf den Desktop projizierten Sperrbildschirm und zum anderen die Verhinderung des Dateizugriffs und/oder der Nutzung des gesamten Systems durch eine Verschlüsselung. Im zweiten Fall spricht man auch von einer sog. Krypto-Ransomware. Die einzelnen Verschlüsselungstrojaner unterscheiden sich untereinander dabei in der Art und Weise ihrer Verschlüsselung und ihrem Infektionsweg. Allen ist jedoch gemein, dass nach einer Infektion eine selbstständige Entschlüsselung unwahrscheinlich ist und die Lösegeldzahlung über den Tor-Browser (Darknet) meist in Form einer digitalen Währung erfolgen soll.

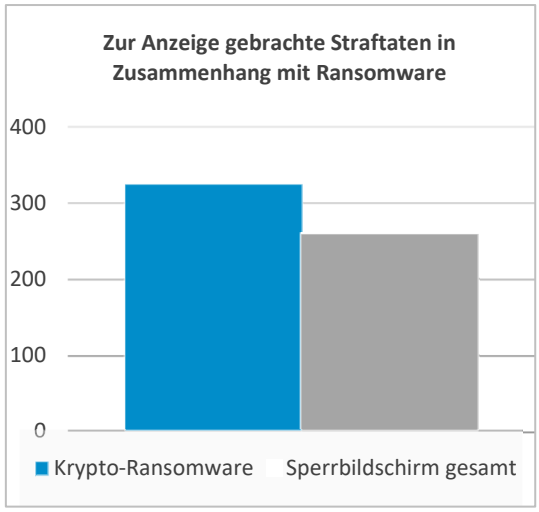
Die Erpressung durch Krypto-Ransomware bleibt trotz eines Rückgangs von ca. 380 auf rund 320 bzw. bei der Anzahl der angezeigten Sperrbildschirme von ca. 300 auf rund 260 Fälle auf anhaltend hohem Niveau.

Sperrbildschirme

Sperrbildschirme sind ein in den letzten Jahren „aus der Mode“ geratenes Phänomen, welches einen rasanten Anstieg in den letzten Jahren erfahren hat.

Der Benutzer schaltet seinen Computer ein und stellt fest, dass er kein Zugriff auf sein System hat. Auf dem Bildschirm erscheint eine ominöse Meldung, teilweise augenscheinlich von einer oder sogar mehreren Strafverfolgungsbehörden: „Behörden haben illegale Aktivitäten auf Ihrem Computer entdeckt.“ In den meisten Fällen wird diese illegale Aktivität mit Kinderpornografie in Verbindung gebracht und mit einem Logo der Strafverfolgungsbehörden untermauert. Aufgrund der Schwere der Tat und der Ächtung bei der allgemeinen Bevölkerung eignet sich dieser Vorwurf besonders gut, um das Opfer in Panik zu versetzten und zu irrationalen Handlungen zu verleiten. Besonders wenn sie von der Forderung begleitet wird, dass eine Geldstrafe gezahlt werden soll, um der strafrechtlichen Verfolgung und somit einer höheren Geldstrafe oder sogar einer Freiheitsstrafe zu entgehen.

Im Jahr 2022 kam es somit insgesamt zu ca. 580 angezeigten Ransomware-Vorfällen, die sich wie folgt aufteilen:



Die gängigsten Krypto-Ransomware-Varianten im Jahr 2022 waren unter anderem „Black Basta“ und „Lockbit“. Einer Verschlüsselung durch „Lockbit“ fiel z. B. der namhafte Babynahrungsmittelhersteller Hipp zum Opfer.

Die fortdauernde Kreativität der Erpresser zeigt, dass Ransomware ein dynamisches

Phänomen bleibt. Cybercrime-Gruppierungen arbeiten stetig daran, ihre Cyberangriffe innovativ und effektiver zu gestalten und so die Zahlung der Opfer zu sichern. Das Vertreiben von Ransomware und die damit einhergehenden „Begleitprozesse“ werden mehr und mehr zu einem Geschäftsmodell (Cybercrime as a Service).

CCaaS

Cybercrime-as-a-Service (kurz: „CCaaS“) beschreibt ein lukratives illegales Geschäftsmodell, bei dem IT-versierte Kriminelle ihr Know- How auf digitalen Schwarzmärkten gegen Bezahlung zur Verfügung stellen. Die angebotenen Dienstleistungen umfassen u. a. das Bereitstellen von Ransomware, Botnetzen und Anonymisierungsdiensten zur Identitätstarnung. Hierdurch ist es auch einem IT-Laien möglich, komplexe Cybercrime-Delikte zu begehen und hieraus Profit zu

Immer häufiger wird die Ransomware weiterverkauft an sogenannte „Affiliates“ (dt. Organisationsmitglieder). Bei diesem speziellen CCaaS-Modell müssen die „Affiliates“ nach einem erfolgreichen Angriff einen vorher festgelegten prozentualen Anteil des erbeuteten Lösegelds an den Anbieter entrichten, brauchen aber selbst weniger technische Kenntnisse. Dadurch wird Ransomware als Modus für mehr Kriminelle zugänglich und bleibt eines der dominierenden Themen im Bereich Cybercrime. Der Erpressungsprozess kann sich im Allgemeinen auf die folgenden zwei Punkte aufgegliedert werden:

Datendiebstahl Cyberkriminelle Gruppen extrahieren große Mengen sensibler Daten, bevor sie diese verschlüsseln. Dann drohen sie mit der Veröffentlichung oder dem Verkauf der sensiblen Daten, sofern keine Lösegeldforderungen bezahlt werden. Doch auch im Falle eines Bezahlens von „Lösegeld“ hat niemand Gewähr, dass die Daten nicht doch von Kriminellen weitergenutzt oder weitergegeben werden. Das Durchsickern z. B. sensibler Geschäftsinformationen führt zu erheblichen Schäden finanziell oder für das Image. Dieses Vorgehen wird häufig noch verschärft, indem Mitarbeiter eines betroffenen Unternehmens unter Druck gesetzt werden, dass neben Unternehmensdaten auch persönliche Daten veröffentlicht werden. Auch werden Geschäftspartner, Kunden oder Medien darüber informiert, dass es bei dem betroffenen Unternehmen zu einer Datenverletzung kam. Somit kann die Reputation bei Kunden und Mitarbeitern vermeintlich sinken ein weiteres Druckmittel für die Forderungen der Erpresser.

Dateiverschlüsselung Cyberkriminelle verschaffen sich Zugriff auf die Netzwerkinfrastruktur und verschlüsseln wertvolle Dateien und Systeme, um sie für ihre Opfer unzugänglich zu machen. Übliche Taktiken, um die Sicherheitsvorkehrungen zu umgehen oder auszuhebeln, sind (Dayzero)-Exploits[16], bösartige Anhänge oder Links zu bösartigen Downloads und Websites in E-Mails und Chats.

Die Opfer können durch Lösegeldzahlung oder durch einen auf der Internetseite der Initiative „No More Ransom“ veröffentlichten Decryptionkey bzw. falls vorhanden durch ein geeignetes Backup-System ihre Daten wiederherstellen. Dabei stellt ein funktionierendes Backup-System einen elementaren Baustein der Bewältigung einer Cyber-Erpressung dar.

Lockbit 2.0

Im April 2022 wurde das Cybercrime-QRT (Quick-Reaction-Team) des BLKA aufgrund eines Ransomware-Vorfalls verständigt. Betroffen war hierbei ein IT-Dienstleister aus Schwaben, dessen Arbeitsfähigkeit durch eine Verschlüsselung stark eingeschränkt war. Durch entsprechende VPN-/RDP-Verbindungen zu deren Kunden waren auch 29 weitere Unternehmen, darunter auch die

[16] Das Ausnutzen von in der Programmierung entstandenen Schwachstellen um unbefugt in Systeme einzudringen.

Donaustadtwerke Dillingen-Lauingen, unterschiedlich stark in ihrer Arbeitsfähigkeit limitiert. Durch Kontakt mit den Erpressern über das Tor-Netzwerk (Darknet) wurde für die Entschlüsselung und eine Nicht-Veröffentlichung von abgeflossenen Daten eine Summe von 800.000$ in BTC aufgerufen. Letztlich wurde vom geschädigten Unternehmen keine Zahlung geleistet, da die eigene sowie die Arbeitsfähigkeit der Kunden in Eigenregie über von der Verschlüsselung nicht betroffene Backups aufwändig wiederhergestellt werden konnte.

Von der gleichen Ransomware war im Mai 2022 ein Erdwärme-Versorger aus dem Münchener Umland betroffen. Die von der Täterschaft zunächst geforderten 100.000$ in BTC konnten durch Verhandlungen des Unternehmens auf 49.000$ reduziert werden - eine Zahlung unterblieb dennoch. Die Wiederherstellung der Systeme durch Backups und Neuinstallationen dauerte zum Zeitpunkt der Ermittlungen weiter an.

Bei beiden Unternehmen fand letztlich im Darknet-Auftritt der Täterschaft (sog. Leak-Page) die Veröffentlichung der vor der Verschlüsselung entwendeten Daten statt. Laut Aussagen der Unternehmen handelte es sich hierbei jedoch um keine betriebskritischen Daten.

4.5 Social Engineering

Social Engineering beschreibt die Gesamtheit von Techniken, die von Kriminellen genutzt werden, um ihre (menschlichen) Opfer zu manipulieren. Es wird versucht, vertrauliche Informationen zu erhalten oder die Opfer dazu zu bringen, Dinge zu tun, die einen Computer kompromittieren könnten. Man spricht dabei auch von „human hacking“, welches durch die starke Bedeutung von E-Mails, sozialen Netzwerken und elektronischer Kommunikation ein probates Mittel für Täter darstellt. Social Engineering umfasst allerdings nicht nur die direkte verbale Kommunikation zwischen Täter und Opfer, sondern auch die indirekte, bei der das Opfer gar nicht weiß, dass es gerade kommuniziert; so z. B. im Falle von Schadprogrammen, welche sich als normale Programm-Updates oder scheinbar gefahrlose Word-Dokumente (z. B. als Bewerbungsschreiben oder Rechnung) tarnen, die aber eine ausführbare schadhafte Datei enthalten. Im Folgenden werden einige typische Varianten erläutert, in denen die Methode des Social Engineering zum Einsatz kommt.

4.6.2 Phishing

„Phishing“ ist die meistgenutzte und bekannteste Variante, um an personenbezogene Daten zu gelangen. Gerade in diesem Bereich ist über die letzten Jahre hinweg ein hoher Grad an Professionalisierung erkennbar. Während früher noch breit gefächert E-Mails in schlechtem Deutsch oder Englisch verschickt wurden, sind heutzutage sehr authentisch wirkende und professionell erstellte Phishing-E-Mails im Umlauf. Sowohl die E-Mail selbst als auch der manipulierte Internetauftritt, auf den der Link in der E-Mail führt, sind ohne genauere Kenntnis der Erkennungsmerkmale oft nicht mehr vom tatsächlichen Firmenauftritt zu unterscheiden. Einmal in die Falle getappt, hat der Täter die Zugangsdaten und kann den jeweiligen Account übernehmen. Phishing-Angriffe werden nicht nur per E-Mail, sondern auch per Messenger oder über SMS-Nachrichten durchgeführt. Für letztere Variante hat sich das Kunstwort „Smishing“ gebildet, die Kombination aus SMS und Phishing. Dieses Phänomen trat bis zur großen Welle im April 2021 überwiegend außerhalb Deutschlands auf. Das Phänomen ebbte dieses Jahr mit ca. 1.720 Fälle wieder ab im Vergleich zu ca. 3.200 Fällen im Jahr 2021. SMS, welche Schadsoftware verbreiten, konnten kaum noch festgestellt werden.

4.5.1 Phone Scam

Support-Scam

Das Phänomen Support-Scam bezeichnet umgangssprachlich den klassischen Telefonschwindel. Die Täter, meist in großen Call-Centern im Ausland organisiert, nehmen quasi ein Telefonbuch zur Hand und arbeiten systematisch einen bestimmten Rufnummernbereich ab. Am anderen Ende der Leitung meldet sich das Opfer und bekommt beispielsweise von einem vermeintlichen Mitarbeiter eines Software-Unternehmens erklärt, dass sein Computer Teil eines Botnetzes bzw. von einem Trojaner befallen sei und deshalb die Lizenz für das Betriebssystem im Falle einer Nichtreparatur gesperrt werde. Hierdurch wird Entscheidungsdruck aufgebaut. Geschockt hiervon gewährt das Opfer dem Anrufer Fernzugriff auf seinen Rechner und tätigt Zahlungen für eine angeblich neue Lizenz oder Antivirus-Software mit der Kreditkarte bzw. per Online-Banking. Noch bevor das Opfer den Sachverhalt reflektieren kann, ist der Vermögensschaden bereits eingetreten und das „Service-Gespräch“ beendet. Dieser Modus Operandi ist bereits seit vielen Jahren bekannt und ein klassisches Beispiel für die Methode des Social Engineering. Trotz der Bekanntheit und stetigen Warnmeldungen zu dieser Betrugsmasche mussten im Jahr 2022 wieder

ca. 1.700 Anzeigen (2021: 1.800 Anzeigen) verzeichnet werden.

Eine Weiterentwicklung dieses Phänomens, bei der die Täter nicht mehr das Opfer anrufen, sondern das Opfer durch eine Warnmeldung auf seinem Computerbildschirm proaktiv zum Anruf genötigt wird, wird ebenfalls von den Callcentern genutzt. Durch ein Schadprogramm, welches sich das Opfer per E-Mail oder Drive-By-Exploit[17] „eingefangen" hat, wird dem Nutzer vorgetäuscht, dass sein Rechner infiziert sei und er schnellstmöglich die auf dem Bildschirm angezeigte Telefonnummer anrufen müsse, um größeren Schaden zu vermeiden. In manchen Fällen wird diese Forderung sogar mit einer Audio-Nachricht untermauert. Meldet sich das Opfer nun bei der Service-Nummer, nimmt das oben genannte Vorgehen seinen betrügerischen Lauf. Dieses Phänomen des Phone Scam 2.0 hat sich im Jahr 2022 in Bayern auf ca. 670 Anzeigen (2021: ca. 320 Anzeigen) mehr als verdoppelt.

Falsche Bankmitarbeiter

Der „Falsche Bankmitarbeiter" beschreibt ein Phänomen, das vielseitig und an den Modus des Support-Scams angelehnt ist. In fast allen Fällen erfolgt ein Anruf mit gespoofter[18] Nummer der Hausbank. Häufig abends oder am Wochenende und damit außerhalb der normalen Geschäftszeiten, um zu verhindern, dass das Opfer mit seiner Bank Rücksprache halten kann.

Im Verlauf des Telefonats geben sich die Betrüger als Bankmitarbeiter aus. Die Anrufer sprechen meist fehlerfreies Deutsch und sind auf das Gespräch gut vorbereitet. Je nach Professionalität des Täters wird sich mit dem Namen des regulären persönlichen Bankmitarbeiters, den aktuellen Kontoständen und den Umsätzen der Opfer Vertrauen erschlichen. In manchen Fällen werden E-Mail und Anruf in Kombination genutzt. Unter verschiedensten Vorwänden (Auslandsüberweisung, Online-Banking, auffällige Kontobewegungen und Änderung des Sicherheitssystems etc.) versuchen die Kriminellen an Bankdaten zu gelangen. Im Anschluss werden mit den gewonnenen Bankdaten unautorisierte Überweisungen mit großen Summen getätigt. Im Jahr 2022 kam es zu ca. 1.170 dieser Anrufe mit anschließendem Vermögensschaden. Eine Weiterentwicklung dieses Phänomens, bei der die Täter nicht mehr das Opfer anrufen, sondern das Opfer durch eine Warnmeldung auf seinem Computerbildschirm zum proaktiven Anruf genötigt wird, ist auch bei „Falschen Bankmitarbeitern" verbreitet und wurde bereits im Abschnitt Support-Scam beschrieben.

4.6.2 Payment Diversion Fraud

Das Umleiten von Zahlungsströmen per E-Mail ist eine Betrugsmasche, die sich des Identitätsdiebstahls und des Social-Engineerings bedient. Die Betrüger geben sich als Geschäftspartner aus. Mit gefälschten oder „gephishten" Informationen wird die vorgetäuschte Identität glaubhaft gemacht und im weiteren Verlauf darauf hingewiesen, dass sich Zahlungsmodalitäten oder Bankdaten geändert haben. Die Betrugsmasche ist relativ simpel und für die Täter äußerst lukrativ, da es sich bei den Opfern meist um Unternehmen handelt und der Beuteschaden häufig im fünf- bis sechsstelligen Bereich liegt. Aufgedeckt wird der Betrug meistens erst mit erheblicher zeitlicher Verzögerung, wenn Mahnungen für die vermeintlich bezahlte Ware eingehen. Für diese Mahnungen

[17] Beim Drive-By-Exploit werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Browser, in Browser-Plugins oder im Betriebssystem ausgenutzt, um Schadsoftware wie Trojaner unbemerkt auf dem PC zu installieren.

[18] Spoofing nennt man in der IT Täuschungsmethoden zur Verschleierung der eigenen Identität, z. B. werden im Display gefälschte Telefonnummern oder in E-Mails gefälschte Mailadressen sichtbar.

lassen sich die Firmen oft Zeit, um zum Beispiel das Verhältnis zwischen den Geschäftspartnern nicht zu belasten. Somit ist die Möglichkeit einer Rückbuchung meist nicht mehr gegeben. Details zu diesem Phänomen und Tipps, wie man sich davor schützen kann, werden in einem Präventionsvideo der ZAC Bayern zum Business-E-Mail Compromise[19] erklärt. Hierbei werden auch andere Varianten der Fälschung von Schriftverkehr erläutert. Im Jahr 2022 wurden ca. 310 gleichgelagerte Fälle verzeichnet, im Jahr 2021 waren es noch etwa 130 Fälle weniger.

4.5.2 Sicher Bezahlen Funktion

Im vergangenen Jahr wurde eine neuer Modus Operandi auf Ebay-Kleinanzeigen bekannt, bei dem die Bezahlmethode „Sicher bezahlen“ genutzt wird, welche auf dem Treuhandprinzip basiert. Bei der Betrugsmasche versucht der Geschädigte zwar die „Sicher bezahlen“ Funktion der App zu nutzen, jedoch akzeptieren die Täter das Angebot nicht und behaupten stattdessen, die Bezahlung hätte nicht funktioniert. Im Anschluss wird an den Käufer ein Link per SMS versendet, welcher auf Phishingseiten-Seiten führt. Auf diesen Seiten werden Käufer aufgefordert, ihre Kreditkartendaten einzugeben. Im Anschluss erfolgen Abbuchungen mit den gephishten Daten. Dieser Vorgang wird teilweise mehrfach wiederholt, indem dem Käufer suggeriert wird, dass die Transaktionen nicht durchgeführt werden konnten. 2022 kam es in ca. 410 zu solchen Abbuchungen.

[19] https://www.polizei.bayern.de/mam/videos/lka-bayern/zac.mp4

4.6 Varianten des Computerbetrugs

Wie bereits bei einzelnen Deliktsfeldern im Punkt 3.1.1 aufgezeigt, existieren zahlreiche Möglichkeiten, einen Computerbetrug zu begehen. Daher wird nachfolgend in einem eigenen Unterpunkt auf die aktuell gängigsten Begehungsweisen eingegangen.

4.8.1 Carding

Unter den Begriff „Carding“ fallen alle Computerbetrugshandlungen, bei denen Zahlungskartendaten widerrechtlich genutzt und dadurch Vermögensschäden bei den rechtmäßigen Besitzern durch unautorisierte Abbuchungen verursacht werden. Das betrifft sowohl die Daten von Kredit- und EC-Karten, die durch Phishing oder Skimming (oftmals im Ausland) erlangt werden, als auch die bei Online-Shops oder Online-Bezahldiensten hinterlegten Karten- bzw. Bankdaten.

An Beliebtheit, haben oben genannte unautorisierten Abbuchungen mittels „Near Field Communication“ (NFC) gewonnen. Unter NFC versteht man den kontaktlosen Austausch von Daten per Induktion. Dieser Datenaustausch findet durch die Annäherung eines Funktransponders an ein entsprechendes Lesegerät statt. Bei den übertragenen Daten kann es sich um digitale Visitenkarten, Textdateien, URLs und vieles mehr handeln. Im Alltag wird die NFC-Technologie häufig zur Zeiterfassung, zur Zugangskontrolle, in Erkennungsmarken bei Haus- und Nutztieren und auch zum kontaktlosen Bezahlen verwendet. Letzteres funktioniert entweder über ein mit NFC-Transponder ausgerüstetes Smartphone oder eine Smartwatch in Verbindung mit der entsprechenden App, oder mit einer NFC-fähigen Kredit- bzw. Debitkarte.

Durch Phishing erhalten die Täter Daten der Debit oder Kreditkarte. Nach einer Bestätigung, beispielsweise mit einer Mobile-PIN, werden die Daten in der Wallet auf dem Gerät hinterlegt. Künftig reicht das Öffnen der Wallet-App und die Bestätigung der Zahlung etwa per Fingerabdruck, Gesichtserkennung oder Telefon-PIN, um den Kauf über die Karte abzuwickeln oder die Bezahlung von Waren am stationären Ladenterminal.

Grundsätzlich ist eine Steigerung von Zahlungskarten-Straftaten feststellbar. Bayernweit kam es im Jahr 2022 zu insgesamt ca. 24.500 Carding-Vorfällen, im Jahr 2021 waren es ca. 14.500.[20]

4.8.2 Waren-/Leistungskreditcomputerbetrug (511000 und 517200)

Hierunter werden alle Computerbetrugshandlungen subsumiert, bei denen der Täter ohne Täuschung einer natürlichen Person einen Kaufvertrag über Waren oder Dienstleistungen abschließt und nach erfolgter Lieferung bzw. Leistung seitens des Opfers seiner Vertragspflicht, der ausstehenden Zahlung, nicht nachkommt. Diese Voraussetzungen sind immer bei einem sog. Kauf auf Rechnung bzw. einer Ratenzahlung erfüllt, bei dem die Bestell- und Kaufabwicklung ausschließlich maschinell erfolgt und keine Zahlung im Voraus stattfindet. Da für diesen Bereich keine spezifischen Zahlen aus der polizeilichen Vorgangsverwaltung erhoben werden können, wird hier auf die PKS zurückgegriffen, die diesen Deliktsbereich in einem eigenständigen Deliktschlüssel abbildet[21] und hierfür eine Fallzahl von 3.642 Vorgängen für das Jahr 2022 ausweist. Im Jahr 2021 waren es 3.367 Vorgänge.

[20] Der Grund für diese hohe angezeigte Fallzahl liegt in der Tatsache, dass die Opfer meist erst nach erfolgter Anzeigenerstattung die Schadenssumme von ihrer Bank zurückerstattet bekommen.
[21] Siehe einzelne Deliktsfelder (3.1.1).

4.8.3 Überweisungscomputerbetrug (518300)

Beim sog. „Überweisungscomputerbetrug“ reicht der Täter einen meist per Hand ge- oder verfälschten Überweisungsträger bei der Bank ein und veranlasst hierdurch im Erfolgsfall eine widerrechtliche Zahlung zu Lasten des rechtmäßigen Kontoinhabers. Zum Computerbetrug wird diese Tathandlung dann, wenn der Vorgang der Überweisungsabwicklung bankseitig rein maschinell erfolgt. Auch für diesen Deliktsbereich wird zur Fallzahlenermittlung auf den eigenständigen PKS-Deliktschlüssel zurückgegriffen. Dieser weist für das Jahr 2022 eine Fallzahl von 194 (2021: 142) Vorgängen aus.

4.7 Fake-Shops

Bei Fake-Shops handelt es sich um einen Modus Operandi, bei dem mit Hilfe des Internets in kürzester Zeit eine große Anzahl an Warenbetrügereien zu begehen und ein Maximum an Beute zu erzielen ist. Hierzu richten die Täter scheinbar echte Online-Shops ein, in denen meist höherpreisige elektronische Geräte, Schmuck oder Markenkleidung zu besonders günstigen Preisen angeboten werden. Dann sorgen die Täter dafür, dass ihre vermeintlich seriösen Online-Shops bei den Treffern von einschlägigen Online-Suchmaschinen relativ weit oben auf der Trefferliste erscheinen, um eine möglichst große Anzahl an Kaufwilligen zu erreichen. Als Zahlungsmöglichkeiten werden in den Shops meistens Vorkasse per Überweisung oder Kreditkartenzahlung angeboten. Nach erfolgter Zahlung warten die Käufer allerdings vergeblich auf die Lieferung der bezahlten Ware und bleiben aufgrund einer ggf. für sie unsicheren Zahlungsweise meist auf dem Schaden sitzen. Diesem Phänomen konnten im Jahr 2022 bayernweit insgesamt ca. 5.100 Anzeigen zugeordnet werden, was im Vergleich zu 2021 einem Rückgang von ca. 900 Fällen entspricht. Als Grund für den Rückgang wird das Ende der Pandemie und die damit verbundene Erholung der Lieferketten gesehen. Die neuen Engpässe von brennbaren Ressourcen wie Holz und Holzpellets als Ausfluss des Angriffskriegs Russlands auf die Ukraine wurden durch die Fakeshops bereits adaptiert. Das in Ungleichgewicht geratene Verhältnis zwischen Angebot und Nachfrage führte zu steigenden Preisen, vor allem bei Brennstoffen. Dieser Umstand begünstigte die Gewinnmöglichkeiten von Fakeshops durch unvorsichtigere Internetkäufer.

4.8 Erpressung per E-Mail

2022 war ein Jahr mit einem extrem hohen Aufkommen von Erpressungs-E-Mail-Wellen. Darunter versteht man E-Mails, in welchen dem Empfänger ein falscher Inhalt und in manchen Fällen auch ein falscher Absender vorgetäuscht wird, um damit Lösegeld zu erpressen. Wie die hohen Fallzahlen des Phänomens schon vermuten lassen, ist der Gegenstand der Drohung durch den Täter frei erfunden. Ein herausragendes Beispiel ist die Fake-E-Mail-Serie der sog. „Sexpressung“. Im Jahr 2022 wurden ca. 2.200 Fälle (2021: ca. 420) angezeigt. Die Gesamtzahl an Erpressungs-E-Mails beläuft sich auf ca. 2.800. Auch die Fake-E-Mails für „Spenden an die Ukraine“ fallen in diesen Bereich. Im vergangenen Jahr weisen Erpressungs-E-Mails vermehrt tatsächlichen Zugriff auf Accounts und Virenbefall der Computer von Geschädigten auf. Demnach ist es ratsam, elektronische Geräte hinsichtlich Malware zu prüfen und sämtliche Passwörter zu ändern. Es wird aber davon ausgegangen, dass nicht die Versender der E-Mails für die Übernahme von Nutzerkonten oder Infektion mit Malware verantwortlich sind, sondern die Täter auf Daten aus Datenleaks zugreifen.

Modus Operandi „Sexpressung“

Bei dieser Variante behauptet der Täter in einer E-Mail, er habe den Computer des Geschädigten infiltriert und die Kontrolle über Webcam und Mikrofon übernommen. So habe er das Opfer dabei aufgenommen, wie es Pornoseiten besucht und dabei masturbiert habe. Um zu verhindern, dass die angeblichen Aufnahmen an Kontakte per Social Media und E-Mail verbreitet werden, soll der Geschädigte einen bestimmten Betrag in Bitcoin an den Täter überweisen. In einzelnen Fällen sendet der Täter ein Passwort des Empfängers mit, um diesen zu verunsichern.

4.9 Corona und Cybercrime

Die Corona-Pandemie hat 2022 ihren Zenit überschritten und es waren nur noch geringe Auswirkungen im Bereich Cybercrime feststellbar. Der mediale Fokus richtet sich seither auf akutere Bedrohungslagen und damit einhergehend auch die Modi Operandi der Cyberkriminellen.

Mahnung für nicht bestellte Coronatests

Betrüger versuchten 2022 mit einer neuen Methode Geld zu erbeuten. Im vergangenen Jahr sind mehrfach Mahnungen wegen angeblich nicht bezahlter Corona-Tests bei Firmen, Vereinen aber auch Privatpersonen eingegangen. Ausgestellt waren die Zahlungsaufforderungen von der Firma IG Trade und humedical ALPHA-RIBS GmbH. Die Höhe der Rechnungen variierte zwischen vier bis knapp 35.000 Euro.

.

5 Projektgruppe Clearingstelle ZMI/NCMEC

Um einer zunehmenden Verrohung der Kommunikation in sozialen Netzwerken entgegenzuwirken und insbesondere Hass und Hetze im Internet einer konsequenten Strafverfolgung durch die zuständigen Behörden zuzuführen, wurde 2021 durch den Bundestag ein Maßnahmenpaket zur „Bekämpfung des Rechtsextremismus und der Hasskriminalität“ verabschiedet. Ein zentrales Element dieses Pakets ist die Anfang Februar 2022 in Kraft getretene Einführung einer Meldepflicht, die Anbieter großer sozialer Netzwerke mit mindestens zwei Millionen in Deutschland registrierten Nutzern dazu verpflichtet, bestimmte strafbare Inhalte an die „Zentrale Meldestelle für strafbare Inhalte im Internet“ (ZMI) im BKA zu mitzuteilen.

Aufgrund anhängiger Klage-/Eilverfahren einzelner Verpflichteter beim VG Köln wird die Meldepflicht durch das Bundesamt für Justiz (BfJ) aktuell zwar bei keinem Verpflichteten durchgesetzt. Gleichwohl ist die ZMI im BKA in den Wirkbetrieb gestartet und nimmt entsprechende Hinweise von mitwirkungswilligen Kooperationspartnern (u. a. Meldestelle REspect!) entgegen.

Zugleich besteht für US-amerikanische Internetdiensteanbieter aufgrund eines US-Bundesgesetzes die Verpflichtung, ihnen bekannt gewordene Hinweise auf Straftaten gegen die sexuelle Selbstbestimmung von Kindern und Jugendlichen oder Hinweise auf kinder- bzw. jugendpornografische Inhalte an die vom National Center for Missing & Exploited Children (NCMEC) betriebene CyberTipline mitzuteilen. Die bei NCMEC eingehenden Hinweise werden in standardisierter Form („CyberTipline Reports") aufbereitet und den für die weiteren Ermittlungen zuständigen Behörden in den USA oder im Ausland zur Verfügung gestellt. CyberTipline Reports mit Bezug zu Deutschland werden zunächst dem BKA bereitgestellt.

Das BKA leitet Hinweise aus den Bereichen ZMI und NCMEC nach Bewertung der Sachverhalte, Prüfung der strafrechtlichen Relevanz nach deutschem Strafrecht und der Feststellung der örtlichen Zuständigkeit an das zuständige Landeskriminalamt weiter.
Für die Entgegennahme und Bearbeitung der vom BKA übersandten Vorgänge wurde im Herbst 2022 eine gemeinsame Projektgruppe „Clearingstelle ZMI/NCMEC“ im Dezernat 54 des BLKA eingerichtet. Die neue Projektgruppe führt die operativen und strategischen Aufgaben der zuvor getrennten Themenbereiche unter einer Verantwortlichkeit zusammen. Die neue Struktur ermöglicht es, die etablierten Prozesse aus Bereichen ZMI und NCMEC weiter zu harmonisieren, die vorhandenen Ressourcen besser zu nutzen sowie übergreifende Anforderungen zu identifizieren und abgestimmt in die polizeilichen Strukturen einzubringen.

Den Mitarbeitern obliegt sowohl die Bearbeitung der eingegangenen Hinweise (insbesondere die inhaltliche Prüfung, Erfassung in den polizeilichen Vorgangsbearbeitungssystemen und die Weiterleitung an die zuständige Fachdienststelle bzw. die Staatsanwalt-

schaft) als auch die Betreuung und Weiterentwicklung der technischen Infrastruktur und der Geschäftsprozesse. Die Mitarbeitenden verstehen sich im Gesamtkontext als Bindeglied zwischen dem Bundeskriminalamt und den Fachdienststellen der Bayerischen Polizei. Sie stehen als fachliche Ansprechpartner zur Verfügung und vertreten die Interessen der Bayerischen Polizei in verschiedenen Facharbeitsgruppen und Gremien.

Vorgangszahlen

Eine große Herausforderung liegt in der konstant hohen Zahl übermittelter Vorgänge. Während im Jahr 2021 etwa 3.400 NCMEC-Vorgänge vom BKA an das BLKA übermittelt wurden, lag diese Zahl im Jahr 2022 bei etwa 8.700. Ursächlich für diesen enormen Anstieg waren das geänderte Meldeverhalten eines einzelnen Diensteanbieters nach der Verabschiedung einer zeitlich befristeten Bereichsausnahme zur ePrivacy-Richtlinie auf EU-Ebene. Diese erlaubt es den Anbietern, private Online-Nachrichten im Hinblick auf kinderpornografische Inhalte oder Grooming-Sachverhalte zu durchsuchen. Eine weitere Ursache für den Anstieg stellte die fortlaufende Anpassung der Bearbeitungskapazitäten im BKA zur zeitnahen Weiterleitung der vorliegenden Hinweise an die Länder dar.

Gleichzeitig lassen sich aus den NCMEC-Hinweisen stetig verändernde Erscheinungsformen und Phänomenen im Deliktsbereich erkennen, welche die Anpassung und Abstimmung der vorhandenen Prozesse erfordern.
Im Bereich ZMI wurden über 200 Vorgänge vom BKA an das BLKA übersandt. Die Vorgänge verteilen sich relativ gleichmäßig über alle Präsidien der Landespolizei. Deliktische Schwerpunkte sind in den Bereichen Volksverhetzung (32,5 %), Belohnung und Billigung von Straftaten (29,6 %) und gegen Personen des politischen Lebens gerichtete Beleidigungen, üble Nachreden und Verleumdungen (22,7 %) erkennbar.

Ausblick

Die Zahl der Hinweise in den Bereichen NCMEC und ZMI wird nach den Erfahrungen der letzten Jahre auch zukünftig weiterhin deutlich zunehmen.

Möglicherweise werden die Fallzahlen im Bereich NCMEC aufgrund von Sondereffekten (maßgeblich aufgrund zeitlich befristeter Bereichsausnahme zur ePrivacy-Richtlinie und des geänderten Meldeverhaltens eines Anbieters) im Jahr 2023 nicht so extrem wie in den Vorjahren ansteigen. Aufgrund der stetigen Verbesserung der technischen Möglichkeiten zur Erkennung inkriminierten Materials auf Seiten der Anbieter ist aber weiterhin mit einem steten Anstieg der Vorgänge zu rechnen.

Unabhängig von den technischen Entwicklungen wurden und werden auf EU-Ebene verschiedene Initiativen vorangetrieben, die weitere Meldeverpflichtungen für Anbieter im Internet vorsehen.

So wurde am 23. April 2022 das Gesetz über digitale Dienste (Digital Services Act) vom Europäischen Parlament und vom Europäischen Rat angenommen, das am 16. November 2022 in Kraft trat. Erhält ein Hosting-Dienstanbieter Kenntnis von Informationen, die den Verdacht einer Straftat begründen, die eine Gefahr für das Leben oder die Sicherheit einer Person oder von Personen darstellt, so muss er seinen Verdacht ab Februar 2024 den zuständigen Strafverfolgungs- oder Justizbehörden mitteilen.

Zusätzlich hat die EU-Kommission im Mai 2022 einen ersten Entwurf für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen

Missbrauchs von Kindern (CSA-VO) vorgelegt. Die CSA-VO soll die in der EU tätigen Provider künftig (analog zu den US-amerikanischen Vorgaben im Bereich NCMEC) verpflichten, Hinweise auf Straftaten gegen die sexuelle Selbstbestimmung von Kindern und Jugendlichen oder Hinweise auf kinder- bzw. jugendpornografische Inhalte, von denen sie Kenntnis erlangen, an eine europäische Zentralstelle zu melden. Der Entwurf sieht vor, dass Anbieter auf behördliche Anordnung hin ggf. auch verpflichtet werden können, ihre Angebote aktiv nach kinder- und jugendpornografischen Inhalten sowie Grooming-Sachverhalten zu durchsuchen. In der derzeit vorliegenden Fassung des Entwurfs sollen von diesen Anordnungen auch verschlüsselte Kommunikationsinhalte (z. B. Chats oder Messenger) umfasst sein, was im öffentlichen Diskurs zu teils intensiven Diskussionen führt.

6 Prävention

Prävention stellt die Gesamtheit aller staatlichen und privaten Bemühungen dar, welche die Kriminalität als gesellschaftliches Phänomen oder als individuelles Ereignis verhüten, mindern oder in ihren Folgen gering halten soll. In diesem Kontext fällt der Kriminalprävention im Phänomenbereich Cybercrime ein besonderer Stellenwert zu, da hier insbesondere im gewerblichen Bereich ein einzelner unbedachter Mausklick zu erheblichen wirtschaftlichen Schäden führen kann. Der Auftrag der Polizei besteht hier neben einer konsequenten Strafverfolgung darin, durch auf den jeweiligen Bedarfsträger gezielt abgestimmte Präventionsberatung auf menschlicher wie technischer Ebene einen IT-Grundschutz zu etablieren, der auch einer sich stetig weiterentwickelnden Cyberkriminalität standhält.

Ziele der polizeilichen Präventionsberatung beinhalten im Bereich Cybercrime insbesondere:

- Schutz der Bürgerinnen und Bürger sowie Unternehmen vor Straftaten aus dem Phänomenbereich der Cyberkriminalität (Computerkriminalität und Tatmittel Internet).
- Information und Sensibilisierung der Bürgerinnen und Bürger, der kleinen und mittleren Unternehmen sowie der gesellschaftlichen Akteure hinsichtlich der Gefahren und Phänomene im Zusammenhang mit Cyberkriminalität
- Stärkung der Eigenverantwortlichkeit zum effektiven Schutz vor Cyberkriminalität, insbesondere durch Schaffung von Möglichkeiten der „Hilfe zur Selbsthilfe“
- Stärkung des objektiven und subjektiven Sicherheitsgefühls im Umgang mit dem Internet sowie neuen Medien im privaten und gewerblichen Bereich

Dies bedarf einer fachlichen und organisatorischen Differenzierung der Cybercrime-Präventionsberatung nach Zielgruppen zum Zwecke einer angesichts des komplexen Themenbereichs zwingend erforderlichen gezielten Abstimmung der Präventionsarbeit und -methodik auf unterschiedliche Bedarfsträger.

6.1 Zielgruppe Bürgerinnen und Bürger

Hierbei wird die Prävention im Bereich Cybercrime in die Themenfelder „Internetkriminalität“ und „Neue Medien“ gegliedert.

Neue Medien

Die Hauptzielgruppen des Themenfelds „Neue Medien“ sind Kinder und Jugendliche an weiterführenden Schulen und Vereinen sowie Eltern, Erziehungsberechtigte und Multiplikatoren wie Pädagogen etc.
Ziele sind hierbei die Sensibilisierung im Umgang mit persönlichen Daten und hinsichtlich der Gefahren der Internetnutzung, die Schaffung eines Unrechtsbewusstseins im Zusammenhang mit Urheberrechtsverletzungen und das Verbreiten von strafbaren Inhalten sowie die Vermittlung von Informationen zu bekannten Vorgehensweisen von Kriminellen im Bereich der sozialen Medien.

Gerade im Deliktsfeld „Verbreitung, Erwerb und Besitz von kinderpornographischen Inhalten“ wurden in der polizeilichen Kriminalstatistik mehr Anzeigen als im Vorjahr registriert. Kinder und Jugendliche können über die sozialen Medien und Messengerdienste problematische und verbotene Inhalte leicht und ungefiltert erhalten. Oft werden diese Inhalte dann auch ohne Bewertung weiterversendet. Insbesondere hier ist es der Polizei in ihrer Präventionsarbeit ein großes Anliegen aufzuklären, da es sich bei dem § 184b Strafgesetzbuch um ein Verbrechen handelt. Die im Frühjahr 2021 veröffentlichte Kampagne „DEIN Smartphone, DEINE Entscheidung“ des BLKA hat zum Ziel, Schülerinnen und Schüler über die strafrechtlichen Aspekte zu informieren und die daraus resultierenden möglichen Folgen zu erläutern. So wurde die Kampagne auch im Jahr 2022 weiter von den Präventionsbeamten durchgeführt. Im vergangenen Jahr fanden hierzu 1.195 Schulunterrichte und Vorträge in Bayern statt. Über Elternbriefe und bei Informationsabenden konnten neben den Eltern auch Pädagogen zu diesem Thema informiert werden.

Material aus der Kampagne „DEIN Smartphone, DEINE Entscheidung“ BLKA SG 513

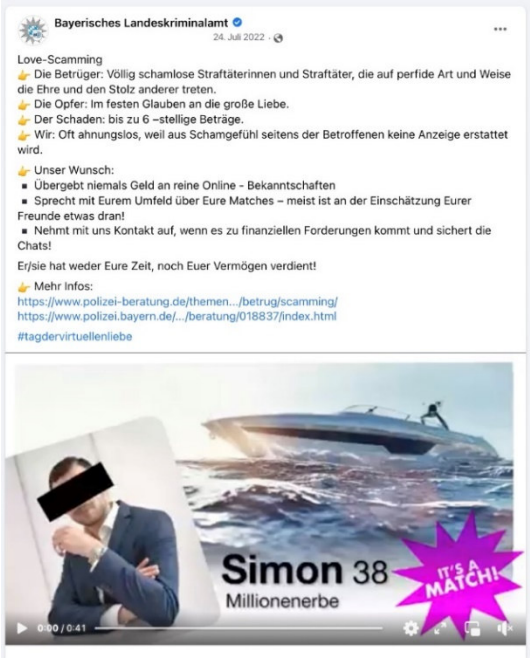
Internetkriminalität

Zielgruppe des Themenfeldes „Internetkriminalität“ sind alle Internetnutzer. Ziele sind hierbei die Sensibilisierung im Umgang mit persönlichen Daten und hinsichtlich Gefahren insbesondere beim Online-Handel sowie die Erzeugung einer Eigenverantwortlichkeit für die PC-Sicherung gegen Schadsoftware und Fremdzugriff. Präventive Maßnahmen sind z. B. der Internetauftritt des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (www.polizei-beratung.de). Auch in den sozialen Medien werden durch die Polizei Warnmeldungen zu häufigen oder neu auftretenden Vorgehensweisen gesteuert.

Ein immer wiederkehrendes Phänomen ist der „Betrug mit der Liebe“. Gerade in der Coronazeit waren viele Menschen einsam – insbesondere Singles. Über Datingportale sowie Chats in Onlinespielen wurden Kontakte geknüpft. Aber nicht jeder meint es immer ernst und ist ehrlich.

Schnell hat man der vermeintlich großen Liebe Geld überwiesen. Die Gründe dafür können unterschiedlich sein. Es wird Geld für die Anreise zum ersten Date benötigt. Oder es ist plötzlich eine Notsituation eingetreten. Am Ende ist das Geld weg und die große Liebe auch. Die Dunkelziffer hierbei ist vermutlich sehr hoch. Viele Menschen scheuen sich – oft aus Scham – vor einer Anzeigenerstattung bei der Polizei.

Um aber auch diese Menschen zu erreichen, hat das BLKA im Juli 2022 bei Facebook und Instagram zu dem Thema kurze, werbewirksame Animationen im Stil eines Datingprofils erstellt. Das Datingprofil des potentiellen "Traumkandidaten" oder der "Traumkandidatin" ändert sich nach einigen Sekunden in ein "Albtraumprofil".



Warnmeldung auf der Facebook-Seite des BLKA

Neben der Öffentlichkeitsarbeit im Social-Media-Bereich bietet die Polizei auch Präventionsvorträge u. a. zu den Themen „Identitätsdiebstahl und Betrugsmaschen im Internet“ an. So konnten in 302 solcher Vorträge Erwachsene, insbesondere Senioren, informiert werden.

6.2 Zielgruppe Gewerbetreibende, kleine und mittelständische Unternehmen (KMU)

Ziel der Prävention ist die Vermittlung grundsätzlicher Verhaltensweisen und Schutzmaßnahmen zur IT-Sicherheit sowie das Erkennen der Notwendigkeit eines eigenen IT-Sicherheitskonzeptes. Hiermit sollen Straftaten oder Vorbereitungshandlungen im gewerblichen Bereich verhindert werden, die der Computerkriminalität (Cybercrime im engeren Sinne) zuzuordnen sind oder bei denen das Tatmittel Internet (Cybercrime im weiteren Sinne) eingesetzt wird. Nennenswerte Delikte in diesem Bereich sind beispielsweise Business-E-Mail Compromise/CEO-Fraud, DDoS- und Ransomware-Angriffe.

Präventionsmaßnamen in diesem Bereich sind zum Beispiel Vorträge und Informationsgespräche bei Interessenvertretungen wie Industrie- und Handwerkskammern und Industrieverbänden. Diese können sowohl in Präsenz als auch digital erfolgen, um eine möglichst große Anzahl an Teilnehmern und Multiplikatoren zu erreichen. Infolgedessen wurden Präventionsangebote für unterschiedliche Zielgruppen entwickelt.

Wichtig sind dabei auch der Aufbau und die Pflege eines regionalen wie überregionalen Informations- und Beratungsnetzwerkes im gewerblichen Bereich, insbesondere durch intensive Kontaktpflege zu Unternehmen, (IT-)Ansprechpartnern und IT-Dienstleistern.

Insofern war die Zentrale Ansprechstelle Cybercrime (ZAC) wieder auf der IT-Sicherheitsmesse „it-sa“ in Nürnberg vertreten. Die überregionale Koordination von Cybercrime-Präventionsmaßnahmen speziell für den Bereich gewerblicher Zielgruppen gehört ebenso dazu wie die anlassbezogene Einbindung von benachbarten Behörden (z. B. die Behörden der Cyberabwehr Bayern) und die Abstimmung mit diesen. Eine anlassbezogene Steuerung von Warnmeldungen zu aktuellen Phänomenen respektive potentiell geschädigten Unternehmen wird mit den genannten Behörden auch abgestimmt.

6.3 Zielgruppe KRITIS, Sub-KRITIS und große Unternehmen

Wie auch im Bereich der KMU ist das Ziel der Präventionsarbeit, die Vermittlung grundsätzlicher Verhaltensweisen und Schutzmaßnahmen zur IT-Sicherheit sowie das Erkennen der Notwendigkeit eines eigenen IT-Sicherheitskonzeptes. Zusätzlich zu den genannten Punkten spielen die Themen Krisenbewältigung und Cyber-Resilienz eine große Bedeutung, da diese Zielgruppen vermehrt im Fokus einiger Tätergruppierungen stehen. Bedarfsträger in diesem Bereich beschränken sich auf:

KRITIS: Organisationen, Unternehmen und Institutionen mit hoher Bedeutung für das Funktionieren des Gemeinwesens, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden und welche durch das BSI auf Grundlage der BSI-KritisV entsprechend klassifiziert wurden.

Sub-KRITIS: Organisationen, Unternehmen und Institutionen, welche die KRITIS-Definition erfüllen, jedoch die Schwellenwerte der BSI-KritisV nicht überschreiten.

Unternehmen im besonderen öffentlichen Interesse: Organisationen, Unternehmen und Institutionen, welche laut Gesetzgebung der KRITIS-Definition nicht entsprechen, jedoch von erheblicher volkswirtschaftlicher Bedeutung sind, mit der Herstellung/Entwicklung schützenswerter Güter (§ 60 AWV) betraut sind oder Betriebsbereiche oberer Klassen gemäß Störfall-VO betreiben.

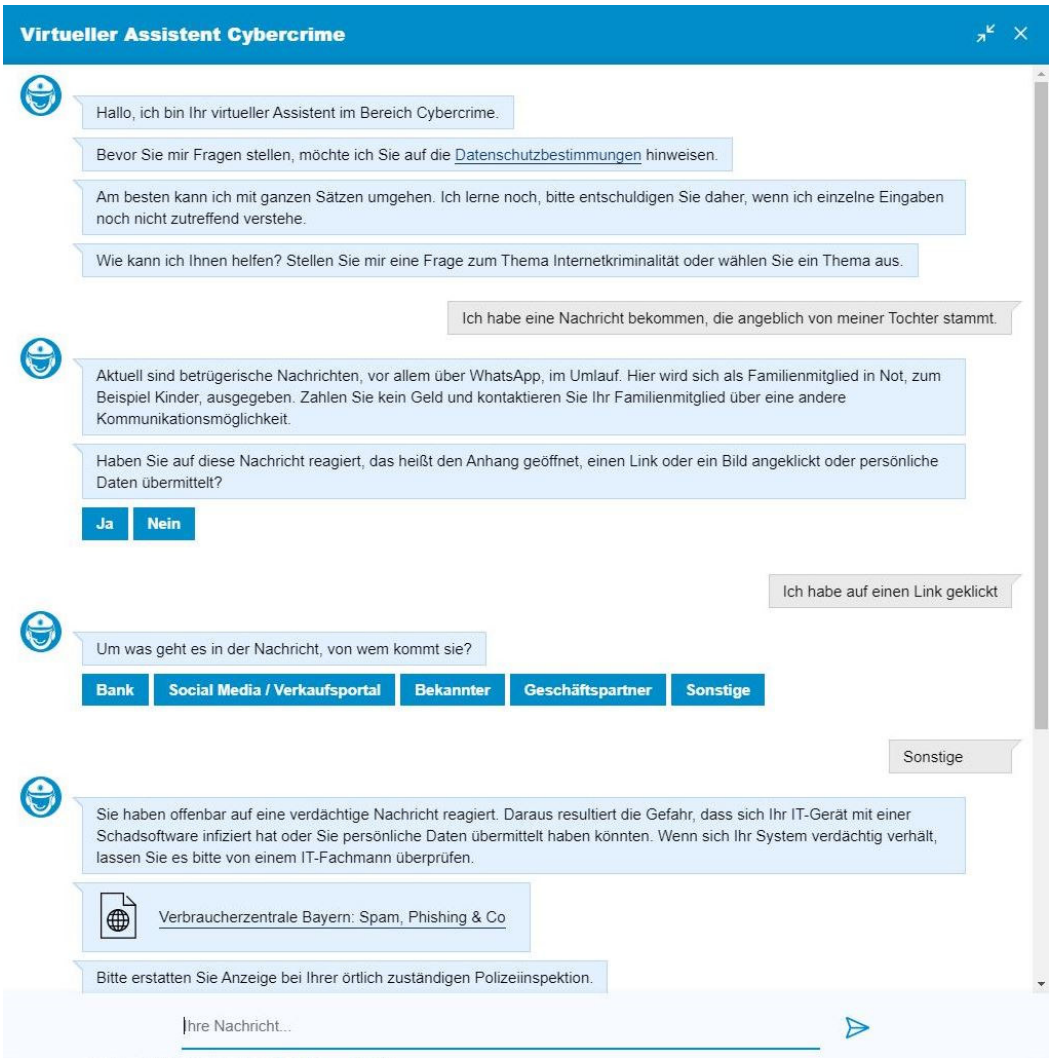
Sonstige börsennotierte sowie international vernetzte und/oder umsatzstarke Unternehmen mit Sitz bzw. Niederlassungen in Bayern.

Ziel ist vor allem die Vermeidung von Versorgungsengpässen, die Aufrechterhaltung der öffentlichen Sicherheit und der Schutz von Unternehmen, Organisationen und Institutionen mit hoher Bedeutung für das Funktionieren des Gemeinwesens. Im Rahmen dieses Präventionsauftrags wurden im Jahr 2022 insgesamt 87 Informationsgespräche, interaktive Krisenübungen zum Thema Ransomware und Awareness-Vorträge mit der bayerischen Wirtschaft durch die Zentrale Ansprechstelle Cybercrime (ZAC) im BLKA durchgeführt, teils digital oder auch analog in Präsenz. Dies entspricht einer Steigerung von etwa 64 % zum Vorjahr. Zudem führte die ZAC im Rahmen der Präventionskampagne Cybercrime anlässlich des G7-Gipfeltreffens 24 Sensibilisierungsgespräche mit besonders gefährdeten Organisationen durch.

7 Chatbot der Bayerischen Polizei

Mit dem Maßnahmenpaket „Online? Aber sicher!“, welches vom Bayerischen Ministerrat in seiner Sitzung vom 26.02.2019 beschlossen wurde, soll den Bürgerinnen und Bürgern mit leicht umzusetzenden Sicherheitsmaßnahmen ein selbstbestimmtes Handeln im Cyberraum ermöglicht werden. Dazu zählt auch die Verbesserung der Kontaktaufnahme mit staatlichen Stellen. Aus diesem Grund richtete das Bayerische Landeskriminalamt zunächst im Zeitraum 2019 bis 2020 die Hotline für IT-Notfälle ein. Um dieses Angebot noch zu erweitern und rund um die Uhr zu Cybercrime-Themen beraten zu können, wurde im September 2022 zusätzlich ein text-basiertes Dialogsystem (Chatbot) eingeführt, der sog. „Virtuelle Assistent Cybercrime“.

Zur Realisierung dieses Projektes erfolgte nach eingehenden Tests die Beschaffung einer Software des Unternehmens Ubitec GmbH aus Österreich und deren Weiterentwicklung. Das System ist in der Lage, Nutzereingaben zu verarbeiten, zu kategorisieren und zuvor definierten Themenkomplexen über Algorithmen zuzuordnen.



Erste Testphase

Zum Anlernen der KI-gestützten Software gründete die Zentralstelle Cybercrime des Bayerischen Landeskriminalamtes ein dreiköpfiges Redaktionsteam, dessen Aufgabe es war, relevante Phänomene im Bereich Cybercrime anhand von möglichen Usereingaben und dazu passenden Antworten des Chatbots aufzubereiten und strukturiert in das Redaktionssystem einzupflegen. Um möglichst viele Eingaben zu generieren, wurde das Team in einer ersten Testphase durch die Präsidien München, Mittelfranken und Schwaben Nord tatkräftig unterstützt, indem die Kollegen durchaus phantasievoll Fragen an das Testsystem stellten und die Antworten bewerteten. Sich ähnelnde Phänomene konnten so durch zunehmend komplexere Fragen- und Antwortstrukturen voneinander abgegrenzt werden, um dem jeweiligen Anwender möglichst passende Hinweise und Handlungsanweisungen geben zu können.

Auf Rückfragen des Chatbots kann der User mittels verschiedener Eingabeoptionen reagieren und auf diese Weise das Ereignis bzw. die Fragestellung eingrenzen. Zusätzlich ist ein Glossar eingepflegt, womit auf Nachfrage einzelne Begrifflichkeiten definiert oder allgemeine Auskünfte, wie z. B. zu Kriminalitätsphänomenen, erteilt werden können.

Erfolgreiche zweite Testphase

Nach einer erfolgreichen zweiten Testphase wurde der Chatbot am 21.09.2022 durch die VK Web Info Medien in den Internetauftritt der Bayerischen Polizei aufgenommen und ist dort auf verschiedenen Seiten zum Thema “Internetkriminalität“ erreichbar. Es wurden seit Einführung bis Ende 2022 mehr als 1.200 Konversationen geführt. Das Redaktionsteam des Sachgebiets 541 im Bayerischen Landeskriminalamt wird diese Dialoge auch in Zukunft begleiten und die Eingaben tagesaktuell überprüfen sowie fehlende Inhalte ergänzen. Auf diese Weise wird die Kompetenz des Chatbots immer weiter verbessert und fortlaufend an die bestehenden Bedürfnisse der Bürgerinnen und Bürger angepasst.

8 Cyber-Sicherheitsbehörden in Bayern

Die Cyberabwehr Bayern ist eine Informations- und Koordinationsplattform für die Zusammenarbeit der Behörden mit Cybersicherheitsaufgaben in Bayern. Sie wurde Anfang 2020 eingerichtet. Ständige Teilnehmer sind das Cyber-Allianz-Zentrum Bayern im Bayerischen Landesamt für Verfassungsschutz (CAZ), das Landesamt für Sicherheit in der Informationstechnik (LSI), die Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg sowie das Landesamt für Datenschutzaufsicht (BayLDA) und der Landesbeauftragte für den Datenschutz (BayLfD) und das Dezernat 54 im Bayerischen Landeskriminalamt (BLKA) als Vertreter der Polizei. Die wesentlichen Ziele der Cyberabwehr Bayern sind die Verbesserung des Informationsstandes und der Reaktionsfähigkeit der beteiligten Einrichtungen, indem ein kontinuierlicher Informationsaustausch zur Cybersicherheitslage erfolgt, hieraus ein gemeinsames Cyber-Lagebild abgeleitet wird und geeignete Maßnahmen beschleunigt umgesetzt werden können.

Die möglichst frühzeitigen Informationen der Teilnehmer über relevante Entwicklungen werden vorwiegend durch regelmäßige Lagebesprechungen sichergestellt. Jährlich wird als Resultat der gemeinsamen Bewertungen ein abgestimmtes Lagebild zur Cybersicherheit für Bayern erstellt. Relevant sind hierbei Informationen, die für die Erkennung, Feststellung, Bewertung, Abwehr oder Vermeidung von Cybervorfällen oder deren Auswirkungen insbesondere auf Kritische Infrastrukturen von Bedeutung sein können. Im Jahr 2022 wurden über 80 herausragende Vorfälle besprochen, darunter der Angriff auf den IT-Dienstleister der Donaustadtwerke Dillingen und die BlackBasta-Angriffe auf Sixt und AGCO.

Zudem werden die operativen Aktivitäten, beispielsweise Warnmeldungen und Präventionsinitiativen der beteiligten Einrichtungen, abgestimmt und das Krisenmanagement bei relevanten Lagen unterstützt. Für Cybersicherheitsvorfälle bei Unternehmen und Behörden in Bayern wurde des Weiteren eine Behördenübersicht erstellt, wann welche Behörde wie in der Krisenbewältigung zuständig ist. Am 09.11.2022 wurde schließlich das Cyber-Lagezentrum eröffnet, in dessen Räumlichkeiten die Cyberabwehr Bayern ihre Besprechungen nun unter besten Bedingungen mit professioneller Ausstattung durchführen kann.

Seit 2021 wird das Netzwerk noch ausgebaut durch Verbindungsbeamte im Nationalen Cyber-Abwehrzentrum, welche die Vernetzung auf Bundesebene und die ständige Kommunikation mit den dortigen Partnerbehörden sicherstellen. Letztlich wird durch die Teilnehmer auch auf der strategisch-politischen Ebene der Ressortkreis für Cybersicherheit unterstützt, die bayerische Cybersicherheitsstrategie weiterzuentwickeln und den Ministerrat kompetent zu beraten. Der aktuelle Fokus für die Cybersicherheitsstrategie der kommenden Jahre liegt auf der weiteren Stärkung der Resilienz auf allen Ebenen: von den Bürgerinnen und Bürgern über Unternehmen und Wissenschaft bis hin zu den Behörden und der staatlichen IT-Infrastruktur selbst.

Die Plattform der Cyberabwehr wird auch genutzt, um die IT-Experten der beteiligten Behörden direkt zu vernetzen, welche sich zwischenzeitlich regelmäßig über Themen wie beispielsweise Malware-Analysewerkzeuge, Threat Intelligence, technische Details zu aktuellen Angriffswellen und deren Detektion austauschen. Von den deutlich beschleunigten und verbesserten Informationsflüssen profitieren dann wieder alle Behörden einzeln vor allem im Bereich des Krisenmanagements und schlussendlich auch Unternehmen, die in akuten Krisensituationen durch Cyberangriffe bei den Behörden Unterstützung suchen.

9 Zukünftige Entwicklung

Zunehmende Regulierung der Cybersecurity durch die EU und Länder

Die Digitalisierung von Unternehmen spielt ein zentrales Thema in Europa und bringt enorme Chancen. Vor allem im Bereich der kritischen Sektoren birgt eine zunehmende Abhängigkeit von Technologie auch viele Herausforderungen. Während zwischen den Ländern Unterschiede bestehen, ist das Potenzial für eine erfolgreiche Digitalisierung in ganz Europa allgegenwärtig. Durch die Stärkung der Reaktionsfähigkeit im Bereich Cybersicherheit im Hinblick auf einen offenen und geschützten Cyberraum soll das Vertrauen der Bürgerinnen und Bürger in digitale Instrumente und Dienste gestärkt werden.

Die Herausforderung der Umsetzung besteht laut EU darin, sicherzustellen, dass der Informationsaustausch nicht nur sinnvoll ist, sondern auch einen vollständigen Überblick über das Gesamtbild ermöglicht. Das Erreichen eines gemeinsamen Verständnisses auf der Grundlage einer akzeptierten Terminologie ist in dieser Hinsicht ein wichtiger Faktor.

Die NIS2[22] soll zur Koordinierung der Krisenreaktion auf EU-Ebene beitragen. Eine der Vorgehensweise ist, neben KRITIS auch die Industrie mit in die Verantwortung zu nehmen.

Risiken von künstlicher Intelligenz im Bereich der Cyberkriminalität

Künstliche Intelligenz hat in den letzten Jahren große Fortschritte gemacht und wird in immer mehr Bereichen eingesetzt. Ein Bereich, in dem AI[23] eine große Rolle spielt, ist die Cyberkriminalität.

Eines der größten Risiken von AI in Bezug auf Cyberkriminalität ist, dass es Cyberkriminellen ermöglicht, ihre Angriffe zu automatisieren und dadurch noch effektiver zu werden. Ein Beispiel hierfür ist das sogenannte "Phishing", bei dem Angreifer versuchen, vertrauliche Informationen wie Passwörter oder Kreditkartendaten von Benutzern zu stehlen. Mit AI-Tools können Angreifer automatisch tausende von E-Mails versenden, die gefälschte Login-Seiten enthalten und so eine große Anzahl von Benutzern täuschen.
Ein weiteres Risiko von AI in Bezug auf Cyberkriminalität ist die Fähigkeit von Angreifern, ihre Angriffe zu "lernen" und dadurch immer schwieriger zu erkennen. Ein Beispiel hierfür sind sogenannte "Deepfake"-Angriffe, bei denen AI-Tools verwendet werden, um gefälschte Bilder oder Videos zu erstellen, die echt wirken. Dies kann dazu führen, dass es schwieriger wird, Angriffe zu erkennen und abzuwehren.

Ein weiteres Risiko von AI im Bereich der Cyberkriminalität ist die Tatsache, dass sie auch für die Entwicklung von sogenannten "Malware" (schädlicher Software) verwendet werden kann. So können Angreifer AI-Tools verwenden, um Schadsoftware zu entwickeln, die in der Lage ist, sich selbst zu "heilen" und sich vor Entfernung zu schützen.

Abschließend lässt sich sagen, dass AI sowohl für Angreifer als auch für Verteidiger von großer Bedeutung ist. Während sie Angreifern ermöglicht, ihre Angriffe zu automati-

[22] NIS ist ein Akronym für „Network and Information Security“. Ursprünglich handelte es sich um eine Direktive der EU aus dem Jahr 2016. Faktisch erließ die Union eine Gesetzesvorlage bezüglich der Stärkung der Cybersicherheit
[23] Artifical Intelligence (AI; dt. Künstliche Intelligenz)

sieren und dadurch noch effektiver zu werden, kann sie auch dazu verwendet werden, Angriffe zu erkennen und abzuwehren. Es ist wichtig, dass Unternehmen und Regulierungsbehörden sich bewusst mit den Risiken von AI im Bereich der Cyberkriminalität auseinandersetzen und Maßnahmen ergreifen, um sich dagegen zu schützen.

Hinweis in eigener Sache: Dieser Abschnitt wurde von **ChatGPT** generiert auf den Befehl „Schreibe mir 1.000 Wörter über die Risiken von AI im Bereich der Cyberkriminalität“ hin und unverändert in das Jahreslagebild 2022 aufgenommen, um zu demonstrieren wie weit künstliche Intelligenz bereits fortgeschritten und öffentlich zugänglich ist. ChatGPT ist ein Prototyp eines textbasierten Dialogsystems, welches auf künstlicher Intelligenz beruht. Es wurde von dem US-amerikanischen Unternehmen OpenAI entwickelt und im November 2022 veröffentlicht.

10 Fazit

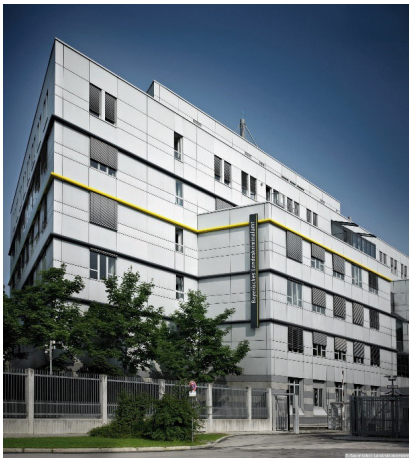
Cybercrime ist eine immer größer werdende Herausforderung in unserer digitalen Welt. Es umfasst eine Vielzahl von Delikten, darunter Hacking, Phishing, Erpressung, Datendiebstahl und Online-Betrug. Diese Angriffe können sowohl für Unternehmen als auch für Einzelpersonen unangenehme Folgen haben, wie zum Beispiel finanzielle Verluste, Rufschädigung und Verlust der eigenen digitalen Identität. Diesbezüglich war 2022 ein unruhiges Jahr mit massiven Wellen an Erpressungs-E-Mails und beinahe monatlichen Meldungen über gestohlene Nutzerdaten aus den Beständen großer Unternehmen. Zunehmend wurden mehrere staatliche Institutionen Ziel von Angriffen durch Cyberkriminelle. Diese Entwicklungen schwächen das Sicherheitsgefühl der Bevölkerung bezogen auf das Internet und die Sicherheit der persönlichen Daten erheblich.

Digitalisierung und digitale Vernetzung führen zu tiefgreifenden Veränderungen in der Kriminalität und der Kriminalitätsbekämpfung. Es gibt auch weiterhin eine Verlagerung von klassischen Kriminalitätsformen in den digitalen Raum, wie beispielsweise im Deliktsbereich Erpressung, begleitet von stark steigenden Zahlen in ausgewählten Kriminalitätsbereichen und einen insgesamt starken Anstieg auch in anderen Bereichen. Um erfolgreich gegen diese Herausforderungen zu bestehen, ist es von besonderer Bedeutung, optimal und effizient mit den steigenden Datenmengen umzugehen. Der Austausch und die enge Zusammenarbeit zwischen allen staatlichen Behörden mit Sicherheitsaufgaben und den privaten Unternehmen ist dafür genauso unerlässlich wie die Information und Aufklärung der Bevölkerung und daher als gesamtgesellschaftliche Aufgabe zu sehen.

Während staatliche Behörden für die Verfolgung und Bestrafung von Tätern verantwortlich sind, sollten sich Unternehmen auf präventive Maßnahmen konzentrieren, um ihre IT-Systeme und Daten zu schützen. Ein wichtiger Aspekt ist dabei die Aufklärung der Mitarbeiter über die Gefahren des Internets und wie man sich vor derartigen Angriffen schützen kann. Dies umfasst sowohl Phishing- und Social Engineering-Techniken als auch die Bereitstellung von Ressourcen für Einzelpersonen, um auf diese Weise über sichere Passwortpraktiken und den Schutz persönlicher Daten zu informieren. Damit einhergehend ist die Aufklärung der Bürger, hier gerade der internetaffinen jüngeren Generation von Bedeutung und sollte bereits in der Schule erfolgen. Mit einem aufklärenden Konzept zur Medienerziehung inklusive praktischen Handlungsanweisungen kann das Gefährdungspotential bereits zu einem nicht unerheblichen Teil minimiert werden.

Dabei ist auch die Reduzierung des Dunkelfelds nicht zu vernachlässigen. Erst durch die Erstattung einer Strafanzeige ist es den Strafverfolgungsbehörden überhaupt möglich, hinreichend aktiv zu werden. Ohne eine solche Aufhellung des Dunkelfeldes blieben die meisten Cyberdelikte straffrei und fördern dadurch die Underground Economy – die Grundlage für weitergehende Straftaten. Auch Zusammenhänge zwischen einzelnen Taten können ohne ein entsprechendes Anzeigeverhalten nicht erkannt werden.

Gelingt all das, kann die Digitalisierung zukunftssicher voranschreiten und den Ruf als „Wilder Westen“ ablegen. Denn das Internet steht für Freiheit, doch Freiheit funktioniert nicht ohne Verantwortung.



Impressum

Herausgeber
Bayerisches Landeskriminalamt
Zentralstelle Cybercrime
Maillingerstraße 15, 80636 München

Tel. 089/1212-0
Fax 089/1212-4974
E-Mail: blka.sg541@polizei.bayern.de

Redaktion v.i.S.d.P.
Alexander Löffler
Dr. Evi Haberberger

Druck
Eigendruck BLKA
Maillingerstraße 15
80636 München

Stand
03/2022

Bildnachweis
BLKA
Cover von Maxpixel.net

www.polizei.bayern.de