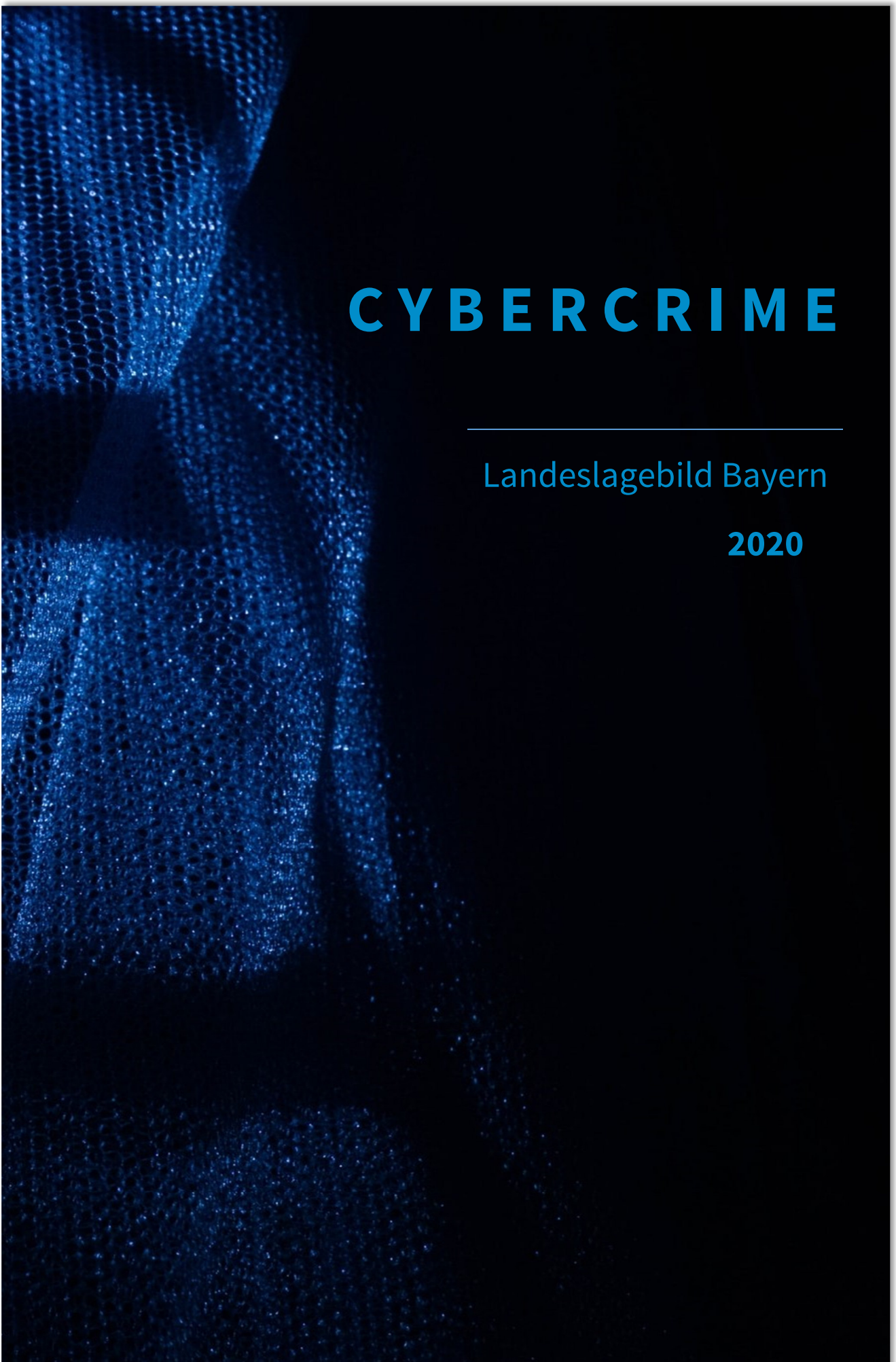
Bayerisches
Landeskriminalamt



CYBERCRIME

Landeslagebild Bayern

2020

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.

Inhaltsverzeichnis

1 Vorwort

Im März 2020 stufte die Weltgesundheitsorganisation (WHO) die Ausbreitung des Coronavirus Sars-CoV-2 als globale Pandemie ein. Seitdem ist ein gravierender Wandel in nahezu allen Lebensbereichen spürbar: Grenzschließungen, Home-Office, Schließung von Schulen und anderen öffentlichen Einrichtungen, Kontaktbeschränkungen, Veranstaltungsverbote sowie die Schließung von Gastronomieeinrichtungen und anderen Möglichkeiten der Freizeitgestaltung. Das Coronavirus hat die Gesellschaft im Jahr 2020 in nahezu allen Bereichen maßgeblich geprägt. Dies führte auch zu einer weitgehenden Verlagerung des täglichen Lebens in die digitale Welt, was vor allem durch den Wegfall oder Einschränkungen analoger Pendants bedingt war. Die verstärkte Nutzung des Internets in allen erdenklichen Lebensbereichen (z.B. Home-Office, Home-Schooling, soziale Treffen, Freizeitgestaltung, Konsum) durch sämtliche Alters- und Gesellschaftsgruppen, rückte dieses Medium noch weit mehr in den Fokus, als es in den vergangenen Jahren bereits der Fall war. So war vor allem ein intensiverer Gebrauch von Streaming- und Messengerdiensten, Maildiensten sowie Social-Media zu verzeichnen. Die IT-Infrastruktur fungiert gerade in diesen Zeiten als tragender Pfeiler zur Aufrechterhaltung des gesellschaftlichen Lebens und wirtschaftlicher Prozesse. Sie gewährleistet den Austausch von Informationen und sicherte die Versorgung.

Diese Verlagerung hin zur digitalen Welt hat jedoch auch ihre Kehrseiten. So schuf sie unter anderem in kürzester Zeit eine erhebliche Vergrößerung der Angriffsfläche für Cyberkriminelle. Diese missbrauchen verstärkt die Ausbreitung des Coronavirus, die damit einhergehenden Besorgnisse und Unsicherheiten der Bevölkerung, sowie die vermehrte Nutzung von digitalen Angeboten für ihre kriminellen Absichten. So entwickelten sich rasant neue Phänomene, welche allesamt die Corona-Pandemie als Narrative ihrer Angriffe nutzten, ob durch DDoS-Attacken[1], Phishing-Mails[2] oder Warenbetrug mit Hygieneartikeln wie Atemschutzmasken und Desinfektionsmitteln. Bei den Tätern handelte es sich vielfach nicht um „Neueinsteiger“. Vielmehr wurden in den meisten Fällen bereits etablierte Modi Operandi auf die Bedingungen der Corona-Pandemie modifiziert.

Das vorliegende Jahreslagebild Cybercrime 2020 wirft einen Blick auf die Kriminalitätslage in diesem Deliktsbereich und stellt aktuelle Phänomene sowie die damit einhergehenden Bedrohungen dar. Hiermit soll sowohl staatlichen Stellen als auch Unternehmen und Privatpersonen ein Überblick über die im zurückliegenden Jahr in Bayern festgestellte Kriminalitätsbelastung durch Cybercrime Delikte ermöglicht werden.

[1] Näheres zu DDoS-Attacken siehe 4.2
[2] Näheres zu Phishing.Mails siehe 4.1

2 Begriffs**bestimmung**

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 im engeren Sinn“ und „Internet als Tatmittel“ geführt haben.

Unter dem Begriff „Cybercrime im engeren Sinn“ 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 2020 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. die folgenden 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 rechtswidrigen 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:

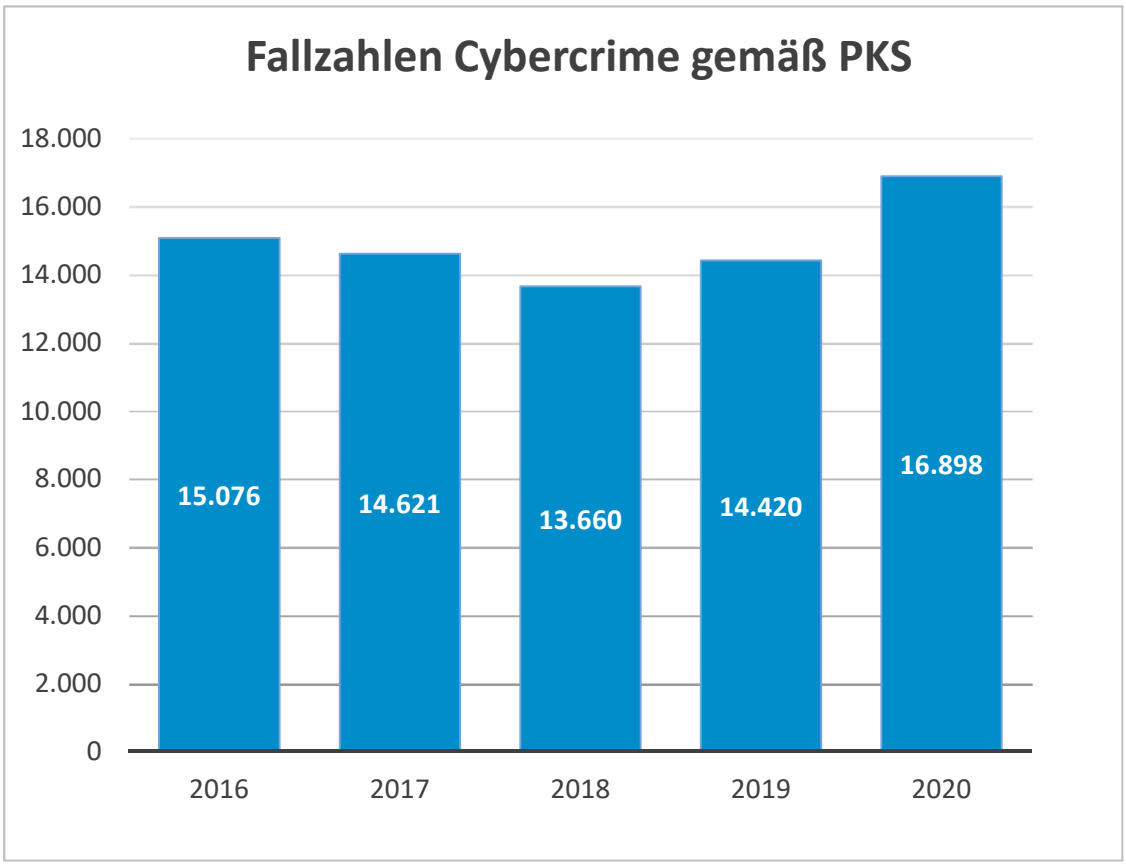
- Verbreitung und Besitzverschaffung von kinder-/jugendpornografischen Schriften
- Betrugsdelikte wie z. B. der Waren(-kredit)- und Leistungs(-kredit)betrug in Verbindung mit Online-Auktionen bzw. Online-Shops, soweit eine natürliche Person getäuscht wird
- Verbreitung urheberrechtlich geschützter Werke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

Spielt das Internet bzw. die Informationstechnologie im Hinblick auf die Tatbestandsverwirklichung allerdings eine lediglich untergeordnete Rolle, beispielsweise wenn 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 im engeren Sinn“ durch den Summenschlüssel „Cybercrime“ (897000) abgedeckt. Für den Berichtszeitraum 2020 weist dieser Summenschlüssel für den Freistaat Bayern eine Zahl von insgesamt **16.898** polizeilich erfassten Fällen aus, was einem **Anstieg von 17,2 %** im Vergleich zum Vorjahr entspricht (2019: 14.420). Ein solcher Anstieg ist in den letzten Jahren nicht ungewöhnlich, da das Internet aufgrund der Möglichkeiten und Anonymität immer mehr von Kriminellen genutzt wird. Mit diesen Fallzahlen entfällt auf den Bereich Cybercrime gem. PKS ein Anteil von **2,8 %** der im Jahr 2020 polizeilich registrierten Gesamttaten.



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.[3] Hier kam es zu **1.784** in der PKS erfassten Fällen.

Datenveränderung und Computersabotage (674200)

Dieser Deliktsbereich umfasst das Eindringen in fremde IT-Systeme mit anschließender Manipulation der dortigen Daten.[4] Hier kam es zu **696** 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).[5] Hier kam es zu **3.698** in der PKS erfassten Fällen.

Softwarepiraterie (715100, 715200)

Dieser Deliktsbereich umfasst die Anfertigung von Raubkopien kommerzieller Software zu privatem oder gewerbsmäßigem Nutzen. Hier kam es zu **10** 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 **1.271** in der PKS erfassten Fällen.

Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten (516520)

Dieser Deliktsbereich umfasst die Verwendung von ausgespähten, abgephishten oder geskimmten[6] Zahlungskartendaten für Einkäufe im Internet. Hier kam es zu **1.493** 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 **799** in der PKS erfassten Fällen.

Computerbetrug (897100)

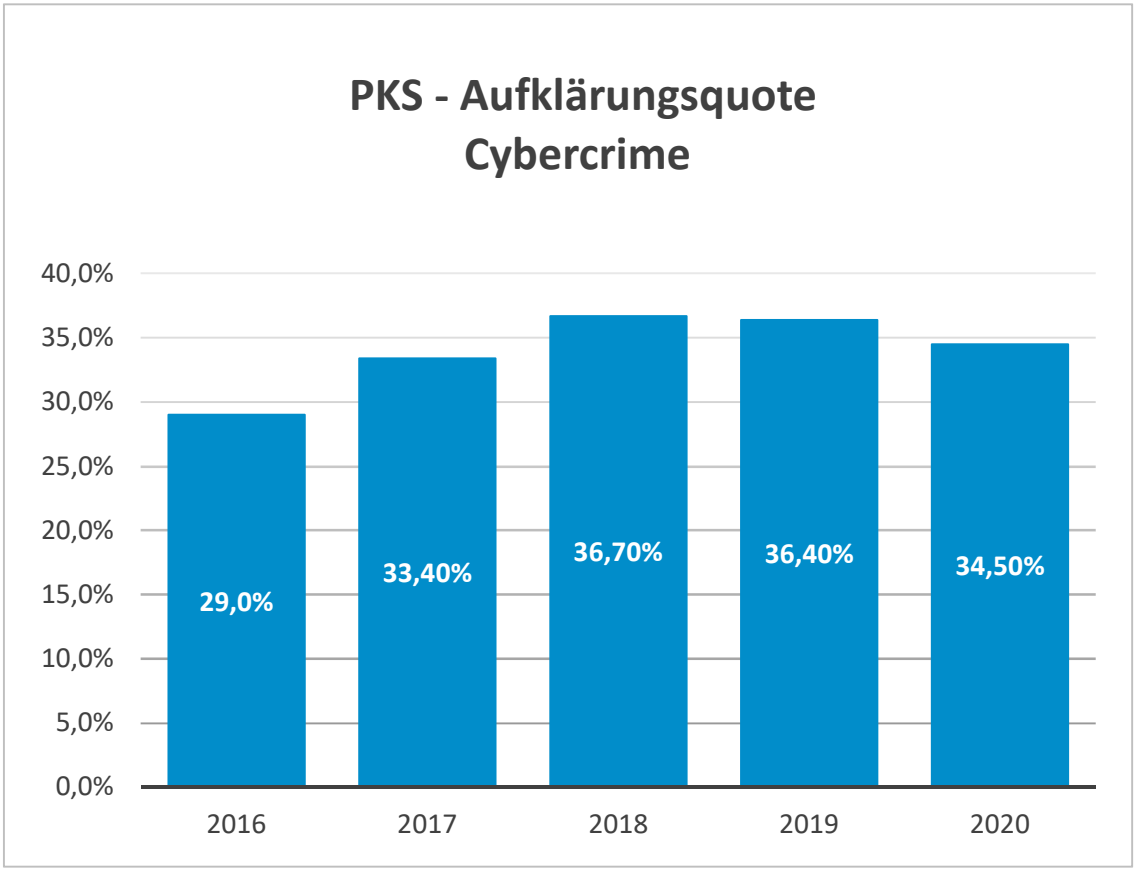
Aufgrund der Komplexität und den vielen Möglichkeiten, einen Computerbetrug zu begehen, wurde speziell für diesen Straftatbestand der Summenschlüssel 897100 eingeführt. Hierunter werden neben den drei zuvor genannten Deliktsbereichen in Zusammenhang mit Zahlungskarten(daten)/Zahlungsmitteln folgende Computerbetrugsdeliktsbereiche subsumiert: Betrügerisches Erlangen von Kraftfahrzeugen (**5** in der PKS erfasste Fälle), Missbräuchliche Nutzung von Telekommunikationsdiensten (**7** in der PKS erfasste Fälle), Überweisungscomputerbe-

[3] Seit 2017 fällt in diesen Deliktsbereich auch die Datenhehlerei, also der Handel mit illegal erlangten Daten zum eigenen oder fremden Vorteil.
[4] Besonders erwähnenswert sind hier die Phänomenbereiche DDoS-Angriffe (4.2.) und Ransomware (4.3.).
[5] Näheres zu Identitätsdiebstahl siehe 4.1.
[6] Beim Skimming werden illegal Kartendaten erlangt, indem Daten von Magnetstreifen ausgelesen und auf gefälschte Karten kopiert werden

trug (**190** in der PKS erfasste Fälle), Leistungskreditcomputerbetrug (**1.549** in der PKS erfasste Fälle), Warenkreditcomputerbetrug (**2.756** in der PKS erfasste Fälle) und der sonstige Computerbetrug als Auffangdeliktsschlüssel (**2.640** in der PKS erfasste Fälle). Zusammengenommen entfallen auf den Deliktsbereich Computerbetrug somit **10.710** in der PKS erfasste Fälle

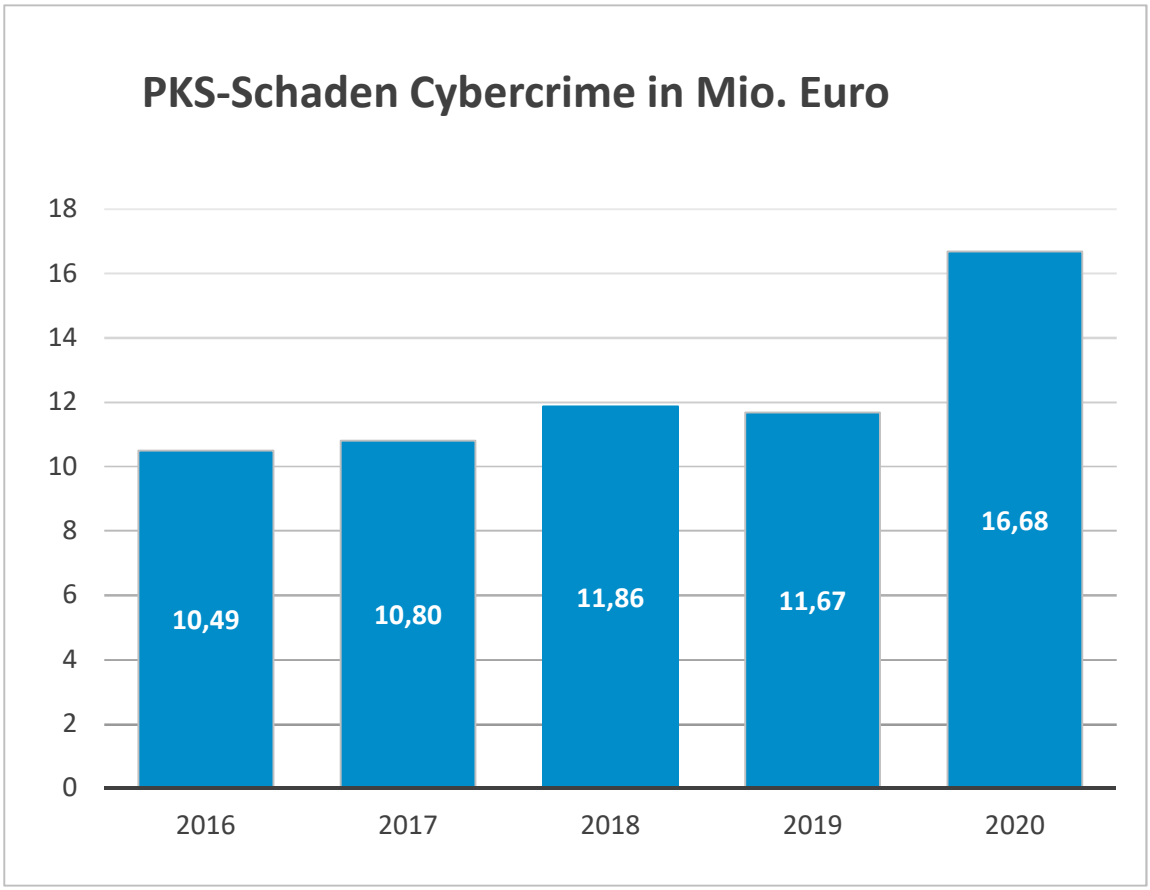
3.1.2 Aufklärungsquote

Im Jahr 2020 ist die Gesamtzahl der aufgeklärten Delikte mit **5.830 geklärten Fällen** gestiegen (2019: 5.253). Die Aufklärungsquote beträgt im Jahr 2020 **34,5 %** und liegt damit unter den 36,4 % des Vorjahres. Maßgeblichen Anteil an der nach wie vor hohen Aufklärung an Fällen haben die im Bereich von ca. 50 % angesiedelten Aufklärungsquoten in den Deliktsfeldern Warenkreditcomputerbetrug sowie Computerbetrug mittels rechtswidrig erlangter Zahlungskarte mit PIN.



3.1.3 Schadensentwicklung

Gemäß PKS summierte sich der durch Cybercrime verursachte Schaden im Jahr 2020 auf **16,68 Millionen Euro**. Damit stieg die Schadenssumme um rund 5 Millionen Euro gegenüber dem Vorjahr an (2019: 11,67 Millionen Euro). Diesbezüglich ist jedoch anzumerken, dass in der bundeseinheitlichen PKS nur Schäden aus den Deliktsfeldern Computerbetrug und Softwarepiraterie registriert werden und in die Schadenssumme mit einfließen. Somit handelt es sich bei den in der nachfolgenden Tabelle dargestellten Schadenssummen genau genommen nur um den Beuteschaden, welcher aus den Deliktsbereichen Computerbetrug und Softwarepiraterie 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.



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. Eine Auswertung dieser Sonderkennungen ergab, dass im Berichtsjahr 2020 das Internet in **35.652** Fällen als Tatmittel eingesetzt wurde, was einem **Anstieg um 20 %** 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 **1.672** in der PKS erfassten Fällen.

Betrug (510000)

Dieser Deliktsbereich umfasst sämtliche Betrugstaten, die unter Zuhilfenahme des Internets begangen werden. Hierzu wurden **23.320** 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 rechtswidrigen Taten nach dem BtMG, wobei der Großteil der Anzeigen auf dem Rauschgifthandel/-erwerb im Darknet beruht. Hier kam es zu **523** in der PKS erfassten Fällen.

Volksverhetzung (627000)

In Zeiten einer zunehmenden Bedeutung von politisch motivierter Kriminalität beschreibt dieser Deliktsbereich beispielhaft, wie das Internet auch für diese Zwecke genutzt wird. Hier kam es zu 463 in der PKS erfassten Fällen.

Nötigung (232200)

Dieser Deliktsbereich umfasst neben der Nötigung auch die Bedrohung und Nachstellung (Stalking), welche über das Internet begangen wird. Hier kam es zu **196** in der PKS erfassten Fällen.

Pornografie (143000)

Zur strafbaren Verbreitung pornografischer Schriften wurde das Internet in **2.137** Fällen der PKS genutzt, das entspricht einem Zuwachs[7] von 83,1%. Davon entfielen auf die Bereiche Kinderpornografie **1.507**, Jugendpornografie **235**, Gewalt-/Tierpornografie **23** und anderer pornografische Schriften **372** in der PKS erfasste Fälle.

Internet als Tatmittel

Aufklärungsquote

*Bei den 35.652 in der PKS erfassten Delikten mit dem Internet als Tatmittel lag die **Aufklärungsquote bei 49,7 %,** also 0,6 % höher als im Vorjahr (2019: 49,1 %). Besonders hervorzuheben sind hier die hohen Aufklärungsquoten in den Bereichen Pornografie (88 %) und Rauschgiftkriminalität (94,6 %).*

Schadenshöhe

*Mit den höheren Fallzahlen stieg auch die Schadenshöhe der mit dem Internet als Tatmittel begangenen Taten im Vergleich zum Vorjahr um 9,9 Millionen Euro auf **28,8 Millionen Euro** an (2019: 18,9 Millionen Euro). Wie bei der Schadensentwicklung gem. PKS (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 Sach-*

[7] Gründe für den Anstieg werden unter 4.10 erklärt

3.2 Auswertung der polizeilichen Vorgangsverwaltung (IGVP)

In der PKS werden bislang nur zu im Inland begangenen Delikten Fallzahlen veröffentlicht. Im Bereich Cybercrime, in dem die Täter auf Grund der Omnipräsenz des Internets nicht an Ländergrenzen gebunden sind und weltweit von jedem Internetanschluss aus agieren können, sind viele Auslandsdelikte festzustellen, da viele Täter bayerische Bürger und Unternehmen aus dem Ausland heraus schädigen oder der Handlungsort des Täters nicht bekannt ist.

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 Verschlüsselungen von IT-Systemen genannt. Hier stellt die Erpressung aufgrund des Strafmaßes das höherwertige Delikt gegenüber der gleichzeitig erfüllten Computersabotage 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.

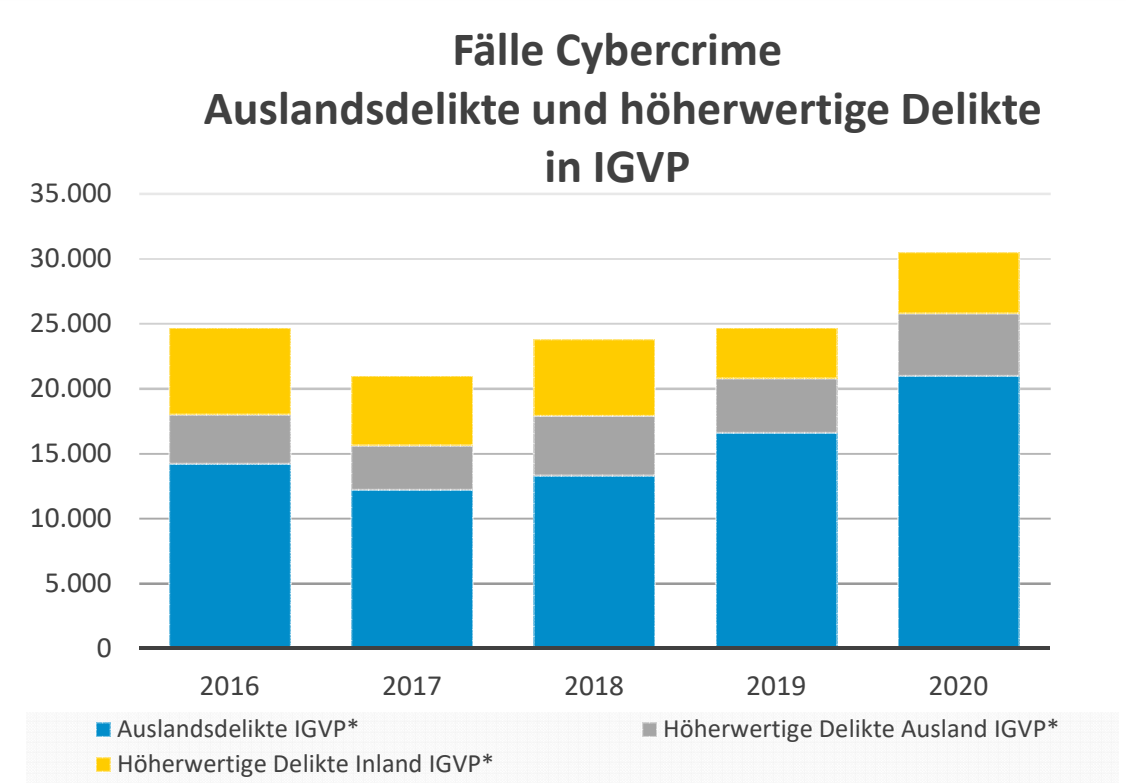
Um eine Annäherung an das spezifische Fallaufkommen im Deliktsfeld Cybercrime in Bayern zu erreichen, wird deshalb bei der Erstellung des jährlichen Lagebilds neben der Erhebung der Delikte aus der PKS stets auch eine manuelle Auswertung der polizeilichen Vorgangsverwaltung (IGVP) vorgenommen. Dabei 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 durch laufende Ermittlungen und Qualitätssicherungsmaßnahmen kontinuierlich ändert. **Die im vorliegenden Lagebild genannten Fallzahlen für das Jahr 2020 stellen eine Momentaufnahme zum Stichtag 26.02.2021 dar und sind nicht reproduzierbar.** Gleichwohl lassen sich anhand der jeweiligen Entwicklungen Tendenzen feststellen und zueinander in Verhältnis setzen.

Eine Auswertung von IGVP in Bezug auf **Auslandsdelikte** ergab, dass dort im Berichtszeitraum **ca. 21.000** derartige Fälle erfasst wurden.

Eine IGVP-Auswertung in der Konstellation **höherwertiges Delikt** in Zusammenhang mit einem Computerdelikt ergab im Berichtszeitraum **ca. 4.700 Fälle mit Tatort in Bayern** und **ca. 4.800 Fälle mit Tatort außerhalb Bayerns bzw. unbekannt**.

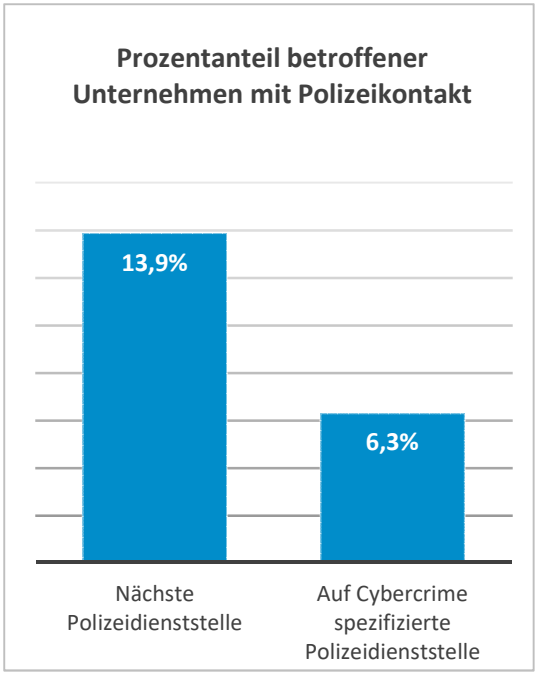
Die anhand der manuellen Auswertung von IGVP ermittelte Entwicklung über die letzten Jahre lässt sich der nachfolgenden Grafik entnehmen:



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

3.3 Dunkelfeld

Um Kriminalität wirksam und effektiv bekämpfen sowie präventiv tätig werden zu können, sind möglichst umfassende Kenntnisse über die Entwicklung der Kriminalität erforderlich. Diese sind anhand der genannten Zahlen nur teilweise generierbar, da es sich hierbei lediglich um das polizeilich bekannt gewordene Hellfeld im Deliktsbereich Cybercrime handelt. Um eine Annäherung an die tatsächliche Kriminalitätsbelastung zu erreichen, ist es jedoch notwendig, auch ein mutmaßliches Dunkelfeld dieses Deliktsbereichs zu berücksichtigen. Durch das Bundeskriminalamt (BKA) und die Polizeien der Länder wird derzeit eine Dunkelfeldstudie durchgeführt. Hierbei werden Opfererlebnisse in der Bevölkerung, des Anzeigeverhaltens, der Kriminalitätsfurcht und von Einstellung gegenüber der Polizei erhoben. Die bundesweite Befragung „Sicherheit und Kriminalität in Deutschland“ (SKiD) ist Ende des Jahres 2020 angelaufen und wird künftig zweijährig erfolgen. Die Ergebnisse dieser Studie stehen gegenwärtig noch nicht zur Verfügung, weshalb auf eine repräsentative Unternehmensbefragung[8] 2018/2019 vom kriminologischen Forschungsinstitut Niedersachsen e.V. zurückgegriffen wird. Im Rahmen der Studie wurden 5.000 Unternehmen ab 10 Beschäftigten in Deutschland gefragt, ob sie bereits einmal von einem Cyberangriff betroffen waren, welche IT-Sicherheitsmaßnahmen vorhanden sind und welche Folgen der schwerwiegendste Cyberangriff für das Unternehmen hatte. Daneben wurde erhoben, ob und an welche staatlichen Stellen sich Unternehmen bei einem schwerwiegenden Cyberangriff in den letzten 12 Monaten wandten. Laut der Studie erstatteten insgesamt 11,9 % der befragten Unternehmen bei einem schwerwiegenden Cyberangriff innerhalb der letzten 12 Monate Anzeige. Dabei brachten 13,9 % den Fall auf der örtlich nächsten Polizeidienststelle zur Anzeige, 6.3 % wandten sich an auf Cybercrime spezifizierte Polizeidienststellen.

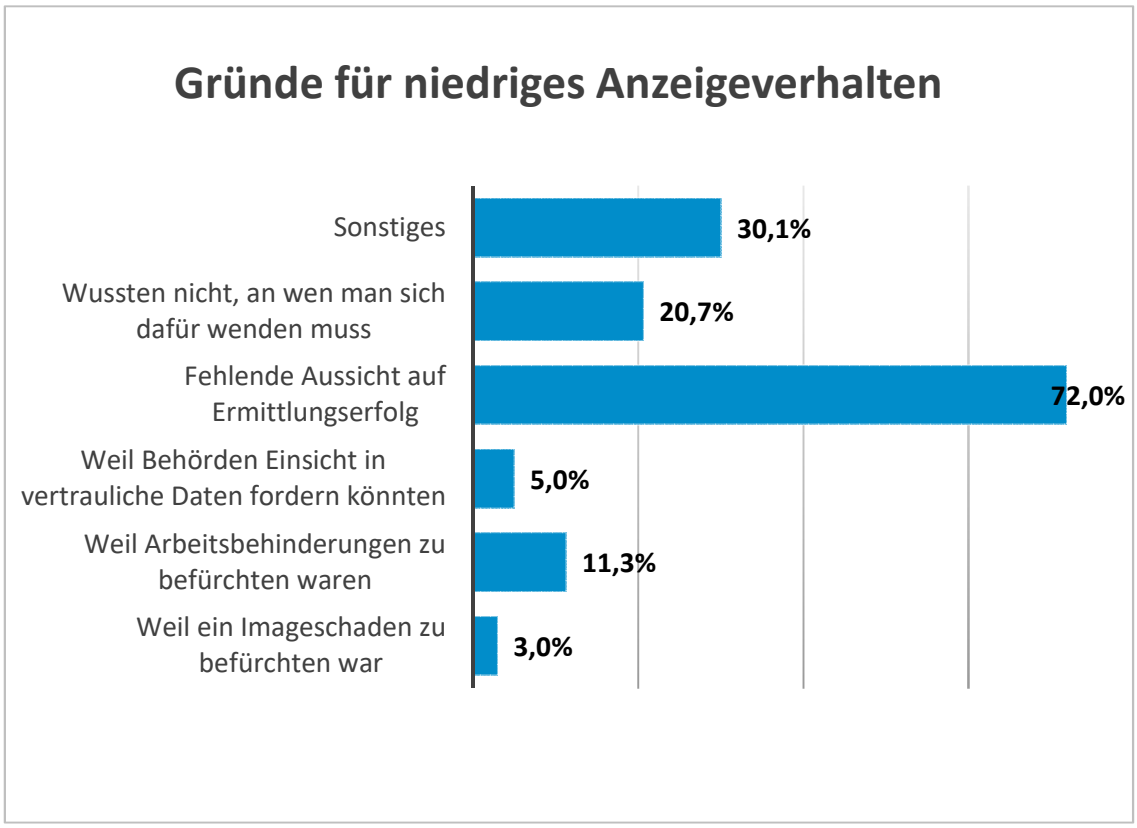


Aufgrund des relativ niedrigen Anteil an Unternehmen, die in den letzten 12 Monaten einen schwerwiegenden Cyberangriff bei der Polizei zur Anzeige brachten, kann vermutet werden, dass das Dunkelfeld in diesem Bereich groß ist.

[8] Dreißigacker, Arne / von Skarczinski, Bennet / Wollinger, Gina Rosa (2020).Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019, Hannover, (Kriminologisches Forschungsinstitut Niedersachsen e. V., Forschungsbericht Nr. 152)

Von den 11,9% der anzeigenden Unternehmen zeigte sich knapp die Hälfte (47,7 %) voll und ganz oder eher zufrieden mit der Arbeit der Polizei. Dennoch würden 93,7 % der Anzeigenden anderen Unternehmen die Anzeige von Cyberangriffen empfehlen. Nur ein kleiner Anteil von 4,9 % würde dies nicht tun.

Die Gründe für das nach wie vor zurückhaltende Anzeigeverhalten geschädigter Unternehmen sind vielfältig. So nennen die befragten Unternehmen unter anderem nachfolgende Gründe für das Nichtanzeigen des schwerwiegendsten Cyberangriffs:



3.4 Besondere Bedrohungslagen

Neben Privatpersonen zielen Cyberangriffe auch immer mehr auf Unternehmen und Behörden ab, welche durch das Ausspähen, Verändern oder Zerstören von Daten und andere Beeinträchtigungen wie der Manipulation von Servern eine steigende Belastung erfahren. Vor allem in Zeiten der Corona-Pandemie bietet die Nutzung unsicherer bzw. behelfsmäßiger Anbindungen an bestehende Systeme und Netzwerke – wie es beim Home-Office regelmäßig der Fall ist – ein Einfallstor für Cyberkriminelle. In diesem Kontext ergeben sich ein anwachsendes Gefahrenpotenzial und gravierendere Auswirkungen durch digitale Angriffe auf Wirtschaft und Infrastruktur, die – vor allem in Zeiten des Lockdowns – von grundlegender Wichtigkeit sind.

ZAC

Die „Zentrale Ansprechstelle Cybercrime (ZAC)“ ist als zentraler Ansprechpartner der Bayerischen Polizei für alle bayerischen Unternehmen, Behörden, Verbände, Vereine und sonstigen Institutionen beim Bayerischen Landeskriminalamt angesiedelt. Die ZAC hat die Förderung der vertrauensvollen Zusammenarbeit zwischen Polizei, Wirtschaft, Forschung und Behörden zur Aufgabe. Dabei berät sie als kompetenter Partner im Kampf gegen Cybercrime Bedarfsträger im Vorfeld und klärt z.B. im Rahmen von Vorträgen über Präventionsmaßnahmen auf. Die ZAC ist darüber hinaus auch „Ersthelfer“ und Berater für von Cybercrime betroffene Institutionen.

Cyberabwehr Bayern

Vor dem Hintergrund einer sich verschärfenden und überregionalen Bedrohungslage aus dem Cyberraum hat die Bayerische Staatsregierung zu Beginn des Jahres 2020 die „Cyberabwehr Bayern“ geschaffen. Dabei handelt es sich um eine behördeninterne Informations- und Kooperationsplattform für alle bayerischen Landesbehörden mit Cyber-Sicherheitsaufgaben. Die Cyberabwehr hält regelmäßig Besprechungen ab, um sich über aktuelle cybersicherheitsrelevante Ereignisse auszutauschen, diese aus der jeweils behördenspezifischen Perspektive zu bewerten und sich maßnahmenorientiert abzustimmen. Dadurch werden Kompetenzen gebündelt, Ressourcen effizienter eingesetzt und Reaktionszeiten – vor allem in Krisenlagen – verkürzt sowie ein breiterer Überblick über die aktuelle Cyberlage ermöglicht.

Dieses Gremium hat sich bereits im 1. Quartal des Jahres 2020 bewährt, als zu Beginn der Corona-Pandemie unverzüglich und behördenübergeifend auf neue Modi Operandi der Täter reagiert werden konnte. In der Cyberabwehr sind vertreten: das Bayerische Landesamt für Verfassungsschutz, das Bayerische Landeskriminalamt, die Generalstaatsanwaltschaft Bamberg, das Landesamt für Sicherheit in der Informationstechnik, das Landesamt für Datenschutzaufsicht und der Landesbeauftragte für Datenschutz.

4 Aktuelle Phänomene

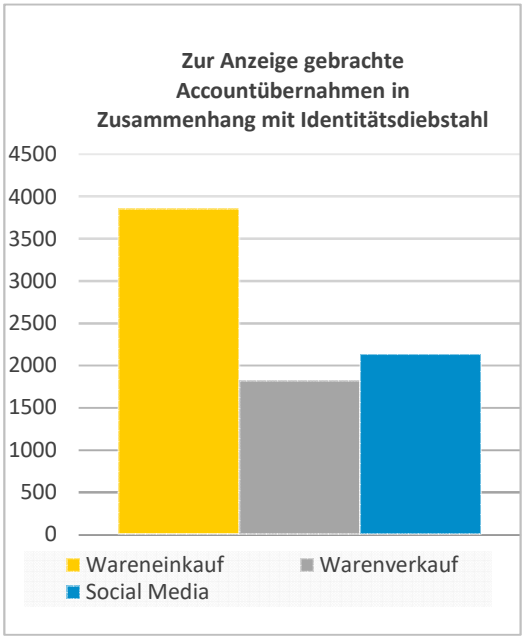
Im Folgenden werden in Bayern häufig auftretende Cybercrime-Phänomene und Modi Operandi dargestellt. Bei den jeweils angegebenen Fallzahlen handelt es sich – soweit nicht anders angegeben – um manuell recherchierte Zahlen aus der polizeilichen Vorgangsverwaltung IGVP, welche den Deliktsbereich Cybercrime auf die einzelnen Phänomene zugeschnitten beziffern.[9]

Anmerkung: Da auch einige im letztjährigen Bericht genannte Phänomene nach wie vor relevant sind, werden diese hier erneut erwähnt und mit den aktuellen Fallzahlen fortgeschrieben.

4.1 Identitätsdiebstahl

Von Identitätsdiebstahl wird gesprochen, wenn personenbezogene Daten einer natürlichen Person durch Dritte missbräuchlich verwendet werden. Vor allem während des coronabedingten Lockdowns, in dem vermehrt Rechtsgeschäfte über das Internet abgewickelt werden und physischer Kontakt gemieden wird, gewinnt dieses Phänomen zunehmend an Bedeutung und hat sich zwischenzeitlich zu einer Art Massenphänomen entwickelt. 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. Die Täter wollen einen Zugang zu derartigen Accounts sowie 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 oder unberechtigte Online-Banking-Transaktionen einzusetzen. So konnte beispielsweise im Zeitraum von Februar bis April 2020 eine hohe Anzahl missbrauchter Paypal-Accounts festgestellt werden. Grund hierfür war eine Sicherheitslücke in Verbindung mit Google Pay[10], die Anfang 2020 an Bedeutung gewann.

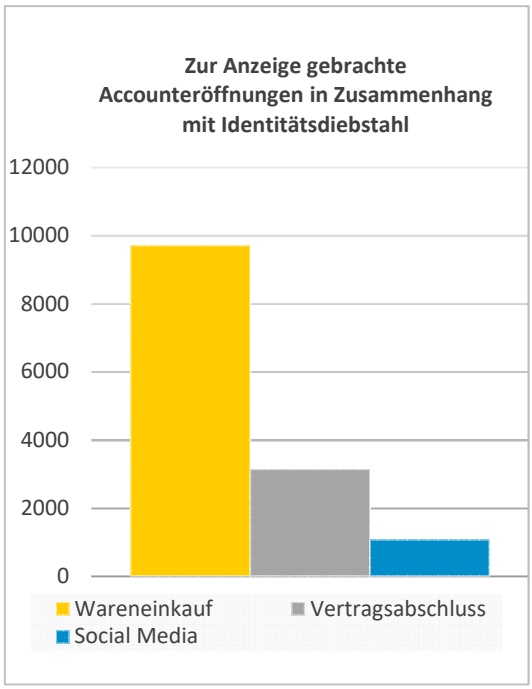
Insgesamt kam es 2020 zu **ca. 8.000** Anzeigen (2019: ca. 4.000 Anzeigen) wegen derartiger Accountübernahmen. Dies entspricht einem Anstieg von 4.000 Fällen bzw. 100 % im Vergleich zum Vorjahr. Die aktuelle Fallzahl setzt sich gemäß dem im Anschluss an die Account-übernahme getätigten Identitätsmissbrauch wie folgt zusammen:



[9] Zur qualitativen Einordnung darf auf die Ziffer 3.2 (Seite 13) verwiesen werden.
[10] Bezahldienst der Firma Google

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, verfügt der Täter über die Zugangsdaten seiner Opfer und kann den jeweiligen Account übernehmen.



Eine weitere Variante dieses Phänomens ist der Missbrauch von aus dem realen Leben bekannten personenbezogenen Daten. Mit diesen werden im Internet falsche digitale Identitäten angelegt und Bestellungen auf Rechnung getätigt, um diese in der Folge an Packstationen liefern zu lassen, wo sie anonym vom Täter abgeholt werden können, ohne dass dieser beim Vertragsschluss jemals in Erscheinung getreten ist. Diese Variante stellt insbesondere in Deutschland eine immer weiter zunehmende Deliktsform dar. Insbesondere die mangelnde Durchführung von rechtsverbindlichen Identitätsfeststellungen in zahlreichen Online-Shops und Auktionshäusern öffnet den Tätern Tür und Tor für betrügerische Anschlusstaten. Opfer von Identitätsdiebstahl 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 2020 zu **ca**. **14.000 Anzeigen** (2019: 10.500 Anzeigen), die sich bezogen auf die Zielrichtung der missbräuchlichen Nutzung wie folgt aufteilen:

Mit insgesamt ca. 21.000 Anzeigen hat dieser Phänomenbereich somit seinen bisherigen statistischen Höchststand erreicht.
Mit ein Grund hierfür dürfte die relativ einfache und doch effektive Begehungsweise sein. Gerade die Variante der betrügerischen Accounteröffnung mit Echtpersonalien einer anderen Person hat aufgrund eines aktuellen Modus Operandi wieder an Bedeutung gewonnen. Hier werden von den Betrügern erschlichene Ausweiskopien genutzt, um ihre falsche Identität bei Accounteröffnungen vermeintlich zu verifizieren. Diese Daten werden durch die Täter erhoben, indem sie sich beispielsweise im Internet als Markforschungsinstitute ausgeben und mit attraktiven Jobangeboten werben. Bei der Anmeldung eines Jobinteressenten muss dessen Identitätspapier in digitaler Form hochgeladen werden, welches so zu den Betrügern gelangt. In gleicher Weise wird auch bei gefälschten Stellenangeboten und Online-Auktionsplattformen vorgegangen. Gerade in der Corona-Krise suchen viele Menschen aufgrund der wirtschaftlich schwierigen Situation nach weiteren Ein-

künften. Ebenfalls ist eine höhere Akzeptanz gegenüber Onlinebewerbungen zu vermuten, um das Infektionsrisiko zu mindern. Auch die Anzahl der potentiellen Opfer ist aufgrund der Verlagerung auf das Medium Internet im Ein- und Verkauf gestiegen.

4.2 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. 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.[11]

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[12]-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 und deren Firmware selten aktualisiert, wodurch derartige IoT-Geräte zu attraktiven Zielen für automatisierte Angriffe aus dem Internet werden. Einmal infiziert, fungieren IoT-Geräte gleich einem Rechner in einem Botnetz.

VPN-Server als attraktive Ziele für Cyberkriminelle

Die bereits erwähnten Folgen des Corona-Virus führten zu einer deutlichen Steigerung von Home-Office-Zeiten und damit des Datenverkehrs in Deutschland. Der deutsche Internetknoten DE-CIX verzeichnete zu Beginn des ersten Lockdowns einen Anstieg von 10 Prozent zu Spitzenzeiten gegenüber dem Niveau vor Beginn der Corona-Pandemie. An kleineren Internetknoten wie zum Beispiel DE-CIX Düsseldorf sogar um mehr als 20%. (https://www.de-cix.net/Files/4a22a4ef28f33c3b648cbb99e69e3658a12cab6d/Warum-das-Netz-haelt---Die-Internetinfrastruktur-in-Zeiten-von-COVID-19.pdf.(15.04.2021)

Vor dem Hintergrund der größeren Auslastung braucht es geringeren Aufwand, um Server und Online-Dienste zu überlasten und, je nach Ausgestaltung des Angriffs, einen VPN-Server oder eine Firewall zum Absturz zu bringen. Dadurch steigt die Gefahr, mit einem relativ einfach auszuführenden DDoS-Angriff alle Mitarbeitenden eines Unternehmens gleichzeitig an ihrer Arbeit zu hindern.

Wie auch bei der Verschlüsselung durch Schadsoftware versuchen Internetkriminelle durch die Androhung und Untermauerung dieser Drohung mit einer abgeschwächten DDoS-Attacke einen monetären Gewinn in Form von digitalen

[11] 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.

[12] Internet of Things, auf Deutsch „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.

Währungen, wie z. B. Bitcoin[13], zu erzielen. Daneben spielen bei DDoS-Angriffen teilweise auch politische oder ideologische Motive eine Rolle. Im coronageprägten Jahr 2020 waren auch vermehrt der Bildungs- und Gesundheitssektor im Visier der Täter, z.B. die Lernplattform Mebis und das Robert-Koch-Institut. In Bayern wurden im Jahr 2020 insgesamt **ca. 50 DDoS-Angriffe** – und damit ca. 150 Vorfälle weniger im Vergleich zum Vorjahr – polizeilich gemeldet. Erpressungsversuche im Rahmen von Fake-E-Mailwellen vermeintlicher DDos-Androhungen waren im Jahr 2020 nur vereinzelt festzustellen, dies erklärt auch den Rückgang der Fallzahlen.

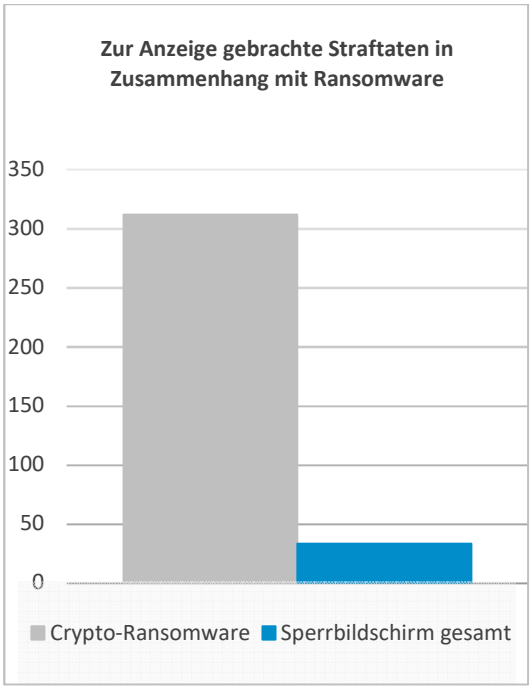
4.3 Malware/Ransomware

Der Begriff Ransomware setzt sich aus den englischen Begriffen ransom (dt. Lösegeld) und malware (dt. Schadprogramm) zusammen und bezeichnet sämtliche Computerprogramme, die den User bis zur Zahlung eines bestimmten Geldbetrags 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. Kryptos ist altgriechisch für geheim und beschreibt die Vorgehensweise der Verschlüsselung in einen „Geheimcode“. Die einzelnen Verschlüsselungstrojaner unterscheiden sich untereinander in der Art und Weise ihrer Verschlüsselung, ihrem Infektionsweg und in der Höhe des zu zahlenden Lösegeldes. Allen gemeinsam ist jedoch, dass nach einer Infektion eine selbstständige Entschlüsselung nahezu unmöglich ist und die Lösegeldzahlung über den Tor-Browser[14] meist in Form einer digitalen Währung erfolgen soll.

Im Vergleich zum Vorjahr stagniert die Anzahl angezeigter Krypto-Ransomware bei ca. 300 Fällen, während sich die Anzahl angezeigter Sperrbildschirme um ca. 30 Fälle reduzierte.

Im Jahr 2020 kam es somit insgesamt zu **330** angezeigten Ransomware-Vorfällen, die sich wie folgt aufteilen:



Die gängigsten Ransomware-Varianten im Jahr 2020 waren unter anderem „Phobos“, „Sodinokibi“ und „Doppelpaymer“.
Eine besonders aggressive Variante bei Ransomware-Fällen war im Jahr 2020 das

[13] Bitcoin (dt. digitale Münze) bezeichnet ein weltweit verfügbares dezentrales Zahlungssystem mit virtuellem Geld, dessen Umrechnungskurs sich durch Angebot und Nachfrage bestimmt.
[14] Internet-Browser, der zum anonymisierten Zugriff auf besonders geschützte Seiten im Internet (sog. Darknet) nötig ist.

sog. „Public Shaming“. Im Gegensatz zu bislang typischer Ransomware wurden die Daten der Opfer dabei vor der Verschlüsselung abgegriffen und die Geschädigten seitens der Erpresser zusätzlich mit der Drohung der Veröffentlichung dieser sensiblen Daten unter Druck gesetzt. Die Angreifer setzten hierbei gezielt auf „schmutzige Geheimnisse“, Kundendaten oder Unternehmensinterna. Sofern die Unternehmen nicht zahlen, werden bei diesem Modus Operandi die Daten im Darknet verkauft oder der Öffentlichkeit zur Verfügung gestellt und die betroffenen Personen darüber informiert, wo diese Daten „geleaked“ wurden. Dies macht eine erfolgreiche Wiederherstellung des infizierten IT-Systems lediglich zu einer partiellen Problemlösung. Die bereits genannten Ransomware-Varianten „Doppelpaymer“ und „Sodinokibi“ verfolgen ebenfalls diese Strategie.

4.4 Social Engineering

Social Engineering beschreibt die Gesamtheit von Techniken, die von Kriminellen genutzt werden, um ihre Opfer zu manipulieren und dadurch vertrauliche Informationen zu erhalten oder die Opfer dazu zu bringen, Dinge zu tun, die den Computer kompromittieren könnten. Man spricht dabei auch von „human hacking“, welches durch die verbreitete Nutzung 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) tarnen, die aber eine ausführbare schädliche Datei enthalten. Im Folgenden werden einige typische Varianten erläutert, bei denen die Methode des Social Engineering zum Einsatz kommt.

4.4.1 Phone Scam

Das Phänomen Phone Scam bezeichnet umgangssprachlich den klassischen Telefonschwindel. Die Täter, meist in großen Call-Centern im Ausland organisiert, nehmen 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 oder von einem Trojaner befallen sei und deshalb die Lizenz für das Betriebssystem im Falle einer Nichtreparatur gesperrt werde, um den Betrogenen unter Entscheidungsdruck zu setzen. Geschockt hiervon gewährt das Opfer dem Anrufer daraufhin 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 2020 ca. **1.350** Anzeigen (2019: 1.700 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, kommt ebenfalls unter Nutzung von Callcentern zum Einsatz. Durch ein Schadprogramm, welches sich das Opfer per E-Mail oder

Drive-By-Exploit[15] 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.

Warnmeldung auf der Facebook-Seite des BLKA

Dieses Phänomen des sogenannten Phone Scam 2.0 hat im Jahr 2020 in Bayern zu **ca. 200** Anzeigen (2019: ca. 240 Anzeigen) geführt.

4.4.2 Payment Diversion Fraud

Das Umleiten von Zahlungsströmen ist eine Betrugsmasche, die sich des Identitätsdiebstahls und des Social Engineerings bedient. Die Betrüger geben sich dabei im geschäftlichen E-Mail-Verkehr als bereits bekannte Geschäftspartner aus. Mit gefälschten oder abgephishten Informationen wird die gefälschte Identität glaubhaft gemacht und im weiteren Verlauf darauf hingewiesen, dass sich Zahlungsmodalitäten oder Bankdaten zur Rechnungszahlung angeblich geändert haben. Diese Betrugsmasche ist für die Täter lukrativ, da es sich bei den Opfern meist um Unternehmen handelt und somit der Beuteschaden häufig im fünf- bis sechsstelligen Bereich liegt. Aufgedeckt wird der Betrug meist erst mit erheblicher zeitlicher Verzögerung, wenn Mahnungen für die vermeintlich bereits bezahlte Ware eingehen. Hierbei lassen sich Firmen oft Zeit, um das Verhältnis zwischen den Geschäftspartnern nicht zu belasten. Somit ist die Möglichkeit einer Rückbuchung meist nicht mehr gegeben. In Bayern wurden im Jahr 2020 **ca. 200** derartige Fälle verzeichnet. Der immense Anstieg lässt sich möglicherweise durch die zunehmende Umstellung von persönlichen Geschäftskontakten auf elektronischen Schriftverkehr erklären.

4.5 Sonstige Malware

Im internationalen Vergleich gehört Deutschland nach Belgien und Schweden zu den am häufigsten von Malware-Attacken betroffenen Ländern[16]. Auch bei den Erpressungssummen gibt es eine Zunahme von 66% in den ersten drei Quartalen des Jahres 2020.[17]

Die Malware „Emotet“ und damit zusammenhängende Malware-Module stellte auch im Jahr 2020 eine der größten Gefahren für Unternehmens-IT dar. Es häufen sich ausländische, sicherheitsbehördliche und

[15] Drive-By-Exploit bezeichnet die automatisierte Ausnutzung von Sicherheitslücken auf einem PC. Dabei werden beim Besuch einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Browser, in Browser-Plugins oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.
[16] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf (19.03.2021).
[17] https://www.munichre.com/topics-online/de/digitalisation/cyber/cyberversicherung-risiken-und-trends-2020.html.(19.03.2021)

externe Hinweise, dass Cybertäter die Corona-Krise auch in Deutschland für die Verbreitung neuer Varianten verschiedener Schadsoftware-Module ausnutzen, für welche „Emotet“ als eine Art Verteiler diente. Das in der Vergangenheit bekannt gewordene Zusammenspiel der Malware-Module „TrickBot“, „Ryuk“ und anderer Module mit „Emotet“ stellte im Jahr 2020 ein erhebliches Gefahrenpotenzial dar.[18]

Emotet

Seit Ende 2018 ist „Emotet“ in der 4. Generation festzustellen und in der Lage, E Mails auszulesen und mit Hilfe dieser Daten neue Nachrichten zu generieren. Die so erzeugten E-Mails wirken authentisch, sind an das Kommunikationsverhalten der angegriffenen Firma angepasst und verleiten das Opfer zum Öffnen schadhafter Links oder Anhänge oder zur Zahlung angeblicher Rechnungen. Im Gegensatz zum Spearphishing werden diese Nachrichten nicht manuell erstellt und können dadurch in höherer Schlagzahl verschickt werden, das sog. „Dynamite Phishing“.
Via geöffnetem Anhang einer E-Mail mit schadhaften Makros in elektronischen Dokumenten oder einem Hyperlink wird das Unternehmensnetzwerk mit Emotet infiziert. Konsekutiv liest Emotet sämtliche Kennwörter, E-Mails und Kontakte aus; dies wird „Outlookharvesting“ genannt. Die Malware nutzt die ausgelesenen Informationen für nachfolgende E-Mail-Wellen, um weitere Geräte zu infizieren. Die fingierten E-Mails beziehen sich auf echte geschäftliche Abläufe, nutzen den passenden Absender und dessen Signatur. Dies fördert die Akzeptanz der versandten Mails und die Verbreitung der Malware. Neben diesem „Spam-Modul“ verfügt Emotet über ein „Wurm-Modul“, mit dem er sich selbständig im Netzwerk verbreitet, ohne erst aktiviert werden zu müssen. Im zweiten Schritt fungiert Emotet als Türöffner für zusätzliche Malware.

Insbesondere die enge Verzahnung von Lieferketten und die besonderen Vorkehrungen, die beispielsweise bei der Impfstoff-Distribution getroffen werden müssen, können als Angriffsfläche für Cyberangriffe dienen (sog. Supply Chain-Angriffe). So kann beispielsweise jeder Betriebsausfall (z.B. bei der Kühlung der Impfstoffe) zur Verzögerung der Auslieferung von Vakzinen führen.

4.5.1 SolarWinds

Einer bislang unbekannten Täterschaft ist es gelungen, die Management- und Monitoring-Software „Orion“ des US-amerikanischen Softwareunternehmens SolarWinds dahingehend zu kompromittieren, dass Schadsoftware der Täter über reguläre Softwareaktualisierungen an Kunden verteilt wurde.
Nach aktuellem Kenntnisstand erfolgte dieser Supply-Chain-Angriff[19] bereits im März 2020 und wurde erst am 13.12.2020 durch das US-amerikanische Sicherheitsunternehmen FireEye publik gemacht. FireEye hatte demzufolge am 08.12.2020 eine Kompromittierung der eigenen Systeme festgestellt und die Malware, die sich hinter den Orion-Updates versteckte, als „Sunburst-Backdoor[20]“ benannt.
Um möglichst lange unerkannt zu bleiben, wurden die durch den Trojaner manipulierten Dateien mit einem – von SolarWinds gestohlenen – Zertifikat seitens der Täter signiert und über offizielle SolarWinds Update-Server verteilt. Nach Angaben von SolarWinds haben weltweit ca. 18.000 Kunden das kompromittierte Update in diesem Zeitraum heruntergeladen. Dazu gehören neben privaten Unternehmen auch Behörden und staatliche Einrichtungen. Ausgelegt ist Sunburst auf das langfristige Sammeln und Ausleiten von Informationen und Daten.

[18] „Emotet“ stellte bis zur Abschaltung der „Emotet“-Infrastruktur durch eine internationale Polizeiaktion im Januar 2021, an der unter anderem das Bundeskriminalamt beteiligt war, ein erhebliches Gefahrenpotenzial dar.
[19] Ein Supply-Chain-Angriff ist ein Cyberangriff, der versucht, einem Unternehmen Schaden zuzufügen, indem er auf weniger sichere Elemente in der Lieferkette abzielt. Ein Angriff auf die Lieferkette kann in jeder Branche auftreten. (Quelle: https://de.qaz.wiki/wiki/Supply_chain_attack)
[20] Als Backdoor (dt.: Hintertür) bezeichnet man den Teil einer Software, der es ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer geschützten Funktion eines Computerprogramms zu erlangen.

4.6 Varianten des Computerbetrugs

Wie bereits bei einzelnen Deliktsfeldern unter 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.

4.6.1 Carding

Unter den Begriff Carding fallen alle Computerbetrugshandlungen, bei denen Zahlungskartendaten widerrechtlich genutzt und dadurch Vermögensschäden bei den rechtmäßigen Besitzern 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.

Grundsätzlich ist ein Rückgang von Zahlungskarten-Aktivität feststellbar, wovon im Zusammenhang mit den Ausgangsbeschränkungen und den angeordneten Lockdowns auszugehen war. Bayernweit kam es im Jahr 2020 zu insgesamt **ca. 17.500** Carding-Vorfällen, im Vorjahr waren es ca. 16.100 Fälle.[21]

4.6.2 Waren-/Leistungskreditcomputerbetrug

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. Dies ist immer bei einem sog. Kauf auf Rechnung bzw. Ratenzahlung der Fall, 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[22] und hierfür eine Fallzahl von **4.305** Vorgängen für das Jahr 2020 ausweist.

4.6.3 Überweisungscomputerbetrug

Beim sog. Überweisungscomputerbetrug reicht der Täter einen meist manuell 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 2020 eine Fallzahl von **190** Vorgängen aus.

[21] 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. Somit sind die eigentlich Geschädigten die Banken, welche diese durch Carding verursachten Schäden über die Gebühren im Rahmen der Kontoführung auf die Kunden und damit die Allgemeinheit umlegen.

[22] Siehe einzelne Deliktsfelder (3.1.1).

4.7 Fake-Shops

Bei Fake-Shops handelt es sich um einen mehr oder weniger professionell angelegten Modus Operandi, um mit Hilfe des Internets in kürzester Zeit eine große Anzahl an Warenbetrügen zu begehen und ein Maximum an Beute zu erzielen. Hierzu richten die Täter scheinbar echte Online-Shops ein, in denen meist hochwertige 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 meist Vorkasse per Überweisung oder Kreditkartenzahlung angeboten. Nach erfolgter Zahlung warten die Käufer allerdings vergeblich auf die Lieferung der bezahlten Ware und bleiben aufgrund der für sie unsicheren Zahlungsart meist auf dem Schaden sitzen.

Diesem Phänomen konnten im Jahr 2020 bayernweit insgesamt **ca. 4.300** Anzeigen zugeordnet werden, was im Vergleich zu 2019 einer Steigerung von ca. 3600 Fällen entspricht. Der schon seit Jahren steigende Trend an Fallzahlen wurde durch den Wechsel in das Onlineshopping nochmals begünstigt. Auch viele „Internetlaien“ erwarben verschiedenste Waren online und waren leichte Opfer. Hinzu kommen noch die Engpässe an Gütern: zeitweise Lieferengpässe z. B. bei Masken und Desinfektionsmittel sowie der limitierte Verkauf der Spielekonsolen X-Box Series X und Playstation 5 brachten Viele dazu, vorschnell zu handeln und riefen damit eine Menge neuer Fakeshops auf den Plan.

4.8 Fake-E-Mail-Wellen

2020 war ein Jahr mit einem hohen Aufkommen von Fake-E-Mail-Wellen. Darunter versteht man eine E-Mail, in der dem Empfänger ein falscher Absender und Inhalt vorgetäuscht wird, um damit entweder Geld zu erpressen oder die Systeme und den Geschäftsbetrieb des Opfers zu stören. Wie der Name des Phänomens schon vermuten lässt, ist der Gegenstand der Drohung durch den Täter in der Regel frei erfunden. In diesem Bereich wurden im Jahr 2020 500 Fälle angezeigt. Im Vergleich zum Vorjahr kam es hier zu einer Reduzierung um 64,2 % (2019: 1.400). Ein herausragendes Beispiel ist die Fake-Email-Serie der sog. „Sexpressung“.

Modus Operandi „Sexpressung“

Im Jahr 2020 beschäftigte das Phänomen der „Sexpressung“ die bayerische Polizei bereits mit rund ca. 470 zur Anzeige gebrachten Fällen. Es wird jedoch von einer überdurchschnittlich hohen Dunkelziffer ausgegangen, da die Thematik viele Geschädigte von der Anzeigenerstattung abhält. Bei dieser besonders dreisten Masche behauptete 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 in Social Media und E-Mail verbreitet werden, sollte der Geschädigte einen bestimmten Betrag in Bitcoin an den Täter überweisen.

Auch die Fake-E-Mails für Corona-Soforthilfe fallen in diesen Bereich und werden unter Punkt 4.10 erläutert.

4.9 Jackpotting/Blackboxing

Beim sog. Jackpotting wird Malware auf den Rechner eines Geldautomaten via USB-Port eingespielt. Hierzu brechen die Täter die Verkleidung des Geldautomaten auf. Über den infizierten Rechner erfolgt anschließend ein Fremdzugriff durch eine bestimmte Anwendung. Dadurch werden zahlreiche unautorisierte Auszahlungen an das Auszahlungsmodul des Geldautomaten veranlasst.
Blackboxing ist eine modifizierte Variante von Jackpotting, bei welcher die Kommunikation zwischen Rechner des Geldautomaten und Auszahlungsmodul getrennt wird. Anschließend übernimmt ein tätereigener Rechner die unterbrochene Verbindung zu dem Auszahlungsmodul mit dem Ziel, unautorisierte Bargeldauszahlungen zu veranlassen. Bayernweit kam es im Jahr 2020 zu sieben derartigen Fällen. Signifikant ist hier jedoch nicht die Anzahl der Fälle, sondern die kriminelle Energie des Vorgehens, da hier sowohl virtuell als auch real in besonders gesicherten Bereichen agiert wird.

4.10 Darknet-Ermittlungen im Bereich Kinderpornografie

Die Spezialisten des Dezernats Cybercrime des Bayerischen Landeskriminalamts erzielten im Jahr 2020 bemerkenswerte Ermittlungserfolge im Kampf gegen die Verbreitung von Kinderpornografie und den sexuellen Missbrauch von Kindern.

Im Anschluss an eine im März 2019 durch die Kriminalpolizei Würzburg erfolgte Festnahme eines Mannes unter anderem wegen des schweren sexuellen Missbrauchs von Kindern wurden durch die bei der Generalstaatsanwaltschaft Bamberg angesiedelte Zentralstelle Cybercrime Bayern und das Bayerische Landeskriminalamt umfangreiche Folgeermittlungen zu den Kontakten und Verbindungen des Festgenommenen in der über das Internet weltweit vernetzten Pädophilenszene begonnen. Mit großem Aufwand wurden alle bei dem Mann aufgefundenen Datenträger und Kommunikationsspuren gesichert und akribisch ausgewertet.

Diese für fast eineinhalb Jahre im Verborgenen geführten Ermittlungen richteten sich gegen pädophile Netzwerke im sog. Darknet, über die in großem Stil Kinderpornografie verbreitet wird. Im Verlauf der Jahre 2019 und 2020 konnte so eine Vielzahl von Mitgliedern dieser Netzwerke identifiziert und festgenommen werden. Durch intensive und akribische Ermittlungsarbeit ist es gelungen, bislang 44 männliche Personen aus der vermeintlichen Anonymität des Darknets zu holen und namentlich als Tatverdächtige zu ermitteln. Davon sind neben 27 in Deutschland wohnenden Beschuldigten 17 Personen im Ausland wohnhaft. Die Ermittlungsverfahren zu diesen Tatverdächtigen wurden nach Belgien, Frankreich, Italien, Österreich und in die Schweiz abgegeben und von den dortigen Behörden weitergeführt.

Bei vielen weiteren Nutzern der im Fokus stehenden kinderpornografischen Internetseiten konnten durch die Ermittlungen vielversprechende Ansätze zu deren Identifizierung gewonnen werden. Diese Ermittlungserkenntnisse wurden ebenfalls an die örtlich zuständigen Strafverfolgungsbehörden u. a. in Deutschland, Albanien, Dänemark, Ecuador, England, Jordanien, Mexiko, Polen, Russland, Tschechien und in den USA zur weiteren Bearbeitung abgegeben. Aktuell führen die Generalstaatsanwaltschaft Bamberg und das Bayerische Landeskriminalamt noch in 13 weiteren Fällen Ermittlungen gegen bislang unbekannte

Tatverdächtige, um diese ebenfalls zu identifizieren.

In Kooperation mit verschiedenen ausländischen Strafverfolgungsbehörden führten die hier getätigten Ermittlungen bereits zu mehreren und besonders bemerkenswerten Erfolgen:

- Unter hohem Ermittlungsaufwand gelang es, einen Schweizer Staatsbürger als Tatverdächtigen zu identifizieren. Nach Weitergabe dieser Information an die Schweizer Behörden konnte dort ermittelt werden, dass dieser Mann in der Schweiz in Kontakt zu einer alleinstehenden Mutter stand und an deren 5-jährigem Jungen bereits sexuelle Handlungen vorgenommen hatte. Unmittelbar vor einem weiteren Missbrauch des Kindes gelang im letzten Augenblick die Festnahme des Tatverdächtigen durch die Schweizer Polizei. Der Mann sitzt seitdem in der Schweiz in Untersuchungshaft.

- Die Ermittlungen des Bayerischen Landeskriminalamtes und der Zentralstelle Cybercrime Bayern führten zur Identifizierung der Betreiber eines Darknet-Forums, auf dem zwischen ca. 1.000 registrierten Nutzern Kinderpornografie getauscht und verbreitet wurde. Nach Einschaltung der österreichischen Sicherheitsbehörden fand das BKA Wien aufgrund der aus Bayern übermittelten Erkenntnisse heraus, dass es sich bei den Betreibern der Darknetseite um bereits einschlägig verurteilte Pädophile handelte, die aktuell eine Haftstrafe in einer Justizvollzugsanstalt in Wien verbüßten. Die kinderpornografische Darknet-Plattform wurde äußerst konspirativ unter Beteiligung von mehreren Häftlingen aus einer Haftzelle dieses Wiener Gefängnisses betrieben. Durch die Enttarnung dieses Betreibernetzwerks konnte das betreffende Darknetforum geschlossen werden und ist seitdem nicht mehr verfügbar.

- In einem weiteren Beispiel konnte aufgrund detaillierter Hinweise der bayerischen Ermittler ein französischer Staatsangehöriger durch die Polizei in Paris festgenommen werden. Gegen ihn besteht u. a. der Vorwurf, regelmäßig Reisen in asiatische Länder unternommen und dort mindestens zwei Jungen im Alter von 7 bzw. 13 Jahren sexuell missbraucht zu haben. Der Tatverdächtige filmte diese Missbrauchstaten und stellte die Aufnahmen ins Darknet. Durch die Festnahme dieses Mannes konnte auch der bevorstehende Missbrauch von zwei Kindern in Frankreich verhindert werden. Der Tatverdächtige sitzt seit seiner Festnahme in Paris in Untersuchungshaft.

Trotz dieser herausragenden Erfolge stellen die beim Bayerischen Landeskriminalamt geführten Ermittlungen in Bezug auf die weltweit vernetzte Pädophilenszene nur Nadelstiche dar. Die hohe Anzahl an Mitgliedern bei den im Darknet zahlreich verfügbaren Pädophilie-Foren und die große Menge des dort verbreiteten kinderpornografischen Bild- und Filmmaterials bestätigen regelmäßig die Erfahrung von Ermittlern, dass es einen riesigen weltweiten Markt für Kinderpornografie gibt.

4.11 Modifikationen während der Corona-Pandemie

Die Corona-Pandemie hatte im Jahr 2020 tiefgreifende Auswirkungen auf fast jeden Lebensbereich. Dies gilt auch für die digitale Welt. Aufgrund der starken Vernetzung und von globalen Beziehungen ist diese ein zentraler Baustein für die Erhaltung unseres Lebensstandards und der Grundversorgung sowie für die Bekämpfung der Pandemie selbst. Die Digitalisierung stellt auch die Arbeitsgrundlagen von Unternehmen und Behörden sicher. Aus diesem Grund hatten Cyberattacken im Jahr 2020 noch weitreichendere Konsequenzen und waren teilweise leichter durchführbar.

Social-Engineering

Das Phänomen erfasst Manipulations- und Betrugsversuche, welche unter Vortäuschen falscher Tatsachen menschliche Reaktionen ausnutzen und durch Hilfsbereitschaft oder Angst die Opfer dazu veranlassen, selbstschädigend zu handeln. Die Täter arbeiten oft medienorientiert, weshalb die Kampagnen an die weltweite Pandemie angepasst wurden. Die Zielgruppenspezifität von Phishing-Kampagnen wird durch Corona-Narrative deutlich minimiert, da jeder Bürger unabhängig von seinem beruflichen und gesellschaftlichen Status von der Thematik betroffen ist.

Soforthilfe für Corona

Die Soforthilfeprogramme der Bundesregierung und des Bayerischen Staatsministeriums für Wirtschaft, Landesentwicklung und Energie waren im Jahr 2020 Ziele von Cyberkriminellen mit zwei verschiedenen Phishing-Varianten.

Zum einen wurden gefälschte Soforthilfe-Webseiten eingesetzt, mit denen die Daten der Antragsteller abgegriffen wurden. Bayern war diesbezüglich vergleichsweise wenig betroffen. So blieben die Anzeigen hier in einem niedrigen zweistelligen Bereich. Einzelne Veröffentlichungen von Seiten im Internet konnten durch entsprechende Monitoringaktivitäten des BLKA auch präventiv verhindert werden.

Die zweite Variante umfasste Phishing-E-Mails, die den größten Teil der diesbezüglichen Straftaten ausmachten. Genutzt wurden vorgeblich z.B. von der Bundesagentur für Arbeit oder vom Bayerischen Staatsministerium für Wirtschaft, Landesentwicklung und Energie stammende E-Mails, die Antragssteller dazu auffordern, sensible Daten zum Unternehmen und zu Beschäftigten per E-Mail zu verschicken, um staatliche Zuschüsse wie Kurzarbeitergeld oder Corona-Überbrückungshilfen zu erhalten. Insgesamt wurden ca. 500 derartige E-Mails etwa von den betrügerischen Absendeadressen „corona-zuschuss@stmwi-bayern.de.com“ oder „zuschuss@bmwi.de.com“ bekannt.

Corona-Banking

Auch im Bereich Online-Banking wurde Corona als willkommener Anlass für die Begehung von Betrügereien genutzt. So wurden vermehrt Bankkunden von Betrügern angerufen oder per E-Mail kontaktiert, die sich als Bankmitarbeiter oder Mitarbeiter eines Sicherheits-Teams ausgaben. Um ihre Opfer zu täuschen, spoofen[23] die Anrufer bei dieser Betrugsmasche ihre Rufnummer oder E-Mailadresse, sodass der Anschein erweckt wird, dass es sich tatsächlich um einen Anruf der Bank handelt. Häufig kennen die Täter durch vorherige Ausspähung die aktuellen Kontostände und Umsätze der Opfer und erschleichen sich so deren Vertrauen. In manchen Fällen werden E-Mail und Anruf in Kombination genutzt.
Die Opfer werden aufgefordert, eine oder mehrere TANs zu nennen, die sie in Abhängigkeit von dem genutzten TAN-Verfahren per SMS oder PushTAN-App zugeschickt bekommen oder die sie beim ChipTAN-Verfahren mit Hilfe ihres TAN-Generators erzeugen sollen. Als Vorwand wird eine angebliche Änderung des Sicherheitssystems in Zeiten der Corona-Pandemie genannt. Vielfach erfolgen die betrügerischen Anrufe auch abends oder am Wochenende und damit außerhalb der normalen Geschäftszeiten, damit keine Möglichkeit besteht, unmittelbar mit den vorgespielten Banken Rücksprache zu halten.

Zoombombing

Hierbei verschaffen sich die Täter unberechtigt Zugriff auf Videoschaltkonferenzen. Hunderttausende von Meeting-IDs wurden im April 2020 im Darknet sowie zahlreichen Untergrundforen verkauft.

Die Zugangsdaten konnten keinem speziellen Datenleak[24] zugeordnet werden, sondern wurden durch sog. Credential Stuffing[25] erbeutet. Der finanzielle Aspekt steht dabei nicht im Fokus der Täter, sondern deren Ziel begrenzt sich auf das Stören der Videoschaltkonferenzen. Die Störung kann unterschiedliche Ausmaße annehmen; häufig wurden Teilnehmer und Moderatoren beleidigt und volksverhetzende Inhalte verbreitet, in vereinzelten Fällen kam es sogar zu einer Übertragung von Kinderpornografie. Die Dienstleister reagierten auf die Vorfälle mit Warteräumen und Passwörtern für Videokonferenzen, um so unberechtigte Teilnahmen zu erschweren.

Offene Krisenkonferenz in Bayern

Die virtuellen Konferenzräume des bayerischen Gesundheitsministeriums wurden zweitweise ohne Zugangsschutz betrieben. So konnte das Online-Magazin „C't" unbemerkt an einer internen Krisensitzung teilnehmen. Hierzu war lediglich die Adresse des virtuellen Raums von Nöten. Dieses Sicherheitsmanko wurde daraufhin behoben.

[23] Bei Anruf-Spoofing verwendet der Anrufer absichtlich eine falsche Anrufer-ID, um über seine eigene Identität zu täuschen. Meistens wird hierfür ein VoIP (Voice over Internet Protocol) oder ein IP-Telefon genutzt.
[24] Ein Datenleak ist ein ungewollter Abfluss von sensiblen Daten.
[25] „Credential Stuffing" ist eine Methode, bei der Zugangsdaten aus älteren Datenabschöpfungen bei verschiedenen Diensten getestet werden, ob auch dort mittels dieser Zugangsdaten eine unautorisierte Anmeldung erfolgen kann.

4.12 Hotline der Bayerischen Polizei für IT-Notfälle

Der Ministerrat hat in seiner Sitzung vom 26. Februar 2019 beschlossen, ein vom Staatsministerium für Digitales vorgelegtes Maßnahmenpaket zur Stärkung der Cybersicherheit umzusetzen. Hierzu zählte auch ein Pilotprojekt zur Erprobung einer polizeilichen Hotline für IT-Notfälle, die es den Bürgerinnen und Bürgern ermöglichen soll, schneller in Kontakt mit staatlichen Stellen zu treten. Insbesondere vor dem Hintergrund einer drohenden Datenflüchtigkeit müssen die erforderlichen Informationen schnell bei den zuständigen Stellen und den Betroffenen sein. Durch die Hotline für IT-Notfälle soll dafür Sorge getragen werden, dass (auch technisch weniger versierte) Nutzer eine einfache Möglichkeit bekommen, bei Datenangriffen Hilfe zu erhalten. Start der Erprobungsphase war der 01.08.2019. Das Pilotprojekt war zunächst für die Dauer eines Jahres angesetzt. Die Besetzung der Hotline erfolgt grundsätzlich mit zwei Polizeivollzugsbeamten zu den üblichen Bürozeiten (Mo. – Do.: 08.00 – 16.00 Uhr; Fr.: 08.00 – 14.00 Uhr). Außerhalb dieser Servicezeiten erfolgt eine Bandansage zu den Erreichbarkeiten bzw. weiteren Kontaktmöglichkeiten (LSI, BSI, CAZ, LDA, LfD). Die Hotline-Rufnummer lautet 089/1212-4400.

Vor Entgegennahme des Anrufs wird - ähnlich wie beim polizeilichen Notruf - eine Bandansage vorangestellt, in der dem Anrufenden die Zuständigkeit der Hotline geschildert wird. Erst im Anschluss daran erfolgt eine Weitervermittlung des Anrufs an den Sachbearbeiter. Nach Entgegennahme des Anrufs erfolgt durch den Sachbearbeiter der Hotline die Aufnahme der Personalien des Mitteilers (Vorname, Familienname, Geburtsname, Geburtstag, Geburtsort, Familienstand, Beruf, Wohnort und Staatsangehörigkeit) und die Bewertung des vorgetragenen Sachverhalts. Der Anrufer erhält im Falle einer Straftat den Hinweis, sich zur Anzeigenerstattung zu seiner örtlich und sachlich zuständigen Polizeidienststelle zu begeben. Er wird darauf hingewiesen, dass ein persönliches Erscheinen mit einem Ausweisdokument zur Legitimation unumgänglich ist. Ferner wird ihm mitgeteilt, an welche Dienststelle er sich wenden sollte und dass diese von Seiten des BLKA über den Anruf informiert wird. Im Anschluss wird der Sachverhalt in einer E-Mail verschriftet und im Falle einer Straftat zielgerichtet weitergeleitet.

Nach mehr als einem Jahr Pilotbetrieb ist bei näherer Betrachtung der insgesamt eher niedrigen Anruferzahlen (durchschnittlich eine mittlere einstellige Zahl von Anrufen pro Tag) festzustellen, dass bei ca. 45% aller Gespräche ein Cybercrime-Delikt mitgeteilt wurde. Die restlichen Anrufe hatten Cybercrime-Präventionsberatungen zum Gegenstand, betrafen die Zuständigkeit anderer Behörden oder lagen außerhalb der Zielrichtung der IT-Notfall-Hotline. Ein IT-Notfall, der besondere polizeiliche Sofortmaßnahmen bedurft hätte, wurde bislang über die Hotline nicht mitgeteilt.

Als Ergänzung bzw. mögliche spätere Alternative zu dem Betrieb der Telefonhotline wird aktuell die Möglichkeit der Einrichtung eines sog. Chatbots[26] fachlich und technisch geprüft.

[26] Bei einem Chatbot handelt es sich um eine textbasierte Dialoganwendung, welche das Chatten einer Person mit einem technischen System erlaubt. Die meisten Chatbots greifen dabei auf eine vorgefertigte Datenbank, die sog. „Wissensdatenbank“, mit Antworten und Erkennungsmustern zurück.

5 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 sollen. In diesem Kontext fällt der Kriminalprävention im Phänomenbereich Cybercrime ein besonderer Stellenwert zu, da hier insbesondere im gewerblichen Bereich ein einzelner unbedachter Mausklick zu sehr weitreichenden wirtschaftlichen Schäden führen kann. Der Auftrag der Polizei besteht deshalb neben einer konsequenten Strafverfolgung auch 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 insbesondere:

- den Schutz der Bürgerinnen und Bürger sowie von Unternehmen, Behörden und gesellschaftlichen Akteuren vor Straftaten aus dem Phänomenbereich der Cyberkriminalität (Cybercrime und Tatmittel Internet)
- Information und Sensibilisierung 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 der objektiven und subjektiven Sicherheit im Umgang mit dem Internet sowie mit neuen Medien im privaten und gewerblichen Bereich

Dies bedarf einer fachlichen und organisatorischen Differenzierung der Cybercrime-Präventionsberatung nach Zielgruppen.

5.1 Bürgerinnen und Bürger

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

Neue Medien

Die Hauptzielgruppe des Präventionsbereichs neue Medien sind Kinder und Jugendliche an weiterführenden Schulen und in Vereinen, 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 die Vermittlung von Informationen zu bekannten Vorgehensweisen von Kriminellen im Bereich der Sozialen Medien.

Internetkriminalität

Zielgruppe dieses Präventionsbereichs sind alle Internetnutzer.
Ziele sind 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 (www.polizei-beratung.de), Themenwochen wie „Sicheres Internet“ mit Antenne Bayern und die EU-Initiative „Klicksafe.de“. Auch in den Sozialen Medien werden durch die Polizei Warnmeldungen zu häufigen oder neu auftretenden Vorgehensweisen gesteuert. In Bezug auf Fake-Seiten in Zusammenhang mit Corona-Soforthilfen wurde z. B. folgender Post auf allen Social-Media-Kanälen der Bayerischen Polizei veröffentlicht.

Warnmeldung auf der Facebook-Seite des BLKA

5.2 Gewerbetreibende, kleine und mittelständische Unternehmen (KMU)

Ziel der Prävention bei dieser Zielgruppe ist die Umsetzung grundsätzlicher Verhaltensweisen und Schutzmaßnahmen zur IT-Sicherheit sowie das Erkennen der Notwendigkeit eines eigenen IT-Sicherheitskonzeptes. Damit sollen Straftaten oder Vorbereitungshandlungen im gewerblichen Bereich, die dem Deliktsbereich Cybercrime (im engeren Sinne) zuzuordnen sind oder bei denen das Tatmittel Internet eingesetzt wird, wie z.B. DDoS- und Ransomware-Angriffe, möglichst effektiv verhindert werden.

Präventionsmaßnamen in diesem Bereich sind zum Beispiel Vorträge und Beratungsgespräche bei Interessenvertretungen, wie Industrie- und Handwerkskammern und Industrieverbänden oder Aufbau und Pflege eines regionalen wie überregionalen Informations- und Beratungsnetzwerkes im gewerblichen Bereich, insbesondere durch intensive Kontakte zu Unternehmen, (IT-)Ansprechpartnern und IT-Dienstleistern. Die überregionale Koordination von Cybercrime-Präventionsmaßnahmen, speziell für den Bereich gewerblicher Zielgruppen sowie die zeitgleiche Abstimmung mit und anlassbezogene Einbindung von benachbarten Behörden (z.B. LSI[27], BayLfV[28]) ist hierbei essentiell. Die anlassbezogene Steuerung von Warnmeldungen zu aktuellen Phänomenen wird ebenso mit benachbarten Behörden (z.B. LSI, BSI[29]) abgestimmt.

[27] Landesamt für Sicherheit in der Informationstechnik
[28] Bayerisches Landesamt für Verfassungsschutz
[29] Bundesamt für Sicherheit in der Informatik

5.3 KRITIS, Sub-KRITIS und Großunternehmen

Ziel der Prävention ist hier ebenso wie bei den KMU die Umsetzung grundsätzlicher Verhaltensweisen und Schutzmaßnahmen zur IT-Sicherheit sowie das Erkennen der Notwendigkeit eines eigenen IT-Sicherheitskonzeptes.

Bedarfsträger in diesem Bereich beschränken sich auf
KRITIS (Kritische Infrastrukturen): Organisationen, Unternehmen und Institutionen mit hoher Bedeutung für das Funktionieren des Gemeinwesens, durch deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden und die durch das BSI auf Grundlage der BSI-KritisVerordnung entsprechend klassifiziert wurden. Diese Unternehmen sind gemäß dem IT-Sicherheitsgesetz ohnehin verpflichtet, Schutzmaßnahmen gegen Cyberangriffe zu ergreifen und unterliegen einem regelmäßigen Monitoring.

Sub-KRITIS: Organisationen, Unternehmen und Institutionen, welche die KRITIS-Definition erfüllen, jedoch hinsichtlich ihrer Größe die Schwellenwerte der BSI-KritisVerordnung nicht erreichen.

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

Ziel der Cybercrime-Prävention in den Bereichen KRITIS, Sub-KRITIS und Großunternehmen ist vor allem die Vermeidung von Versorgungsengpässen und die Aufrechterhaltung der öffentlichen Sicherheit sowie der Schutz von Unternehmen, Organisationen und Institutionen mit hoher Bedeutung für das Funktionieren des Gemeinwesens. Dies wird durch die bereits unter 5.2 genannten Maßnahmen und Methoden und zusätzliche Angebote wie Konzeption, Planung und Durchführung von Krisenstabsübungen und Planspielen bei bayerischen KRITIS- und Sub-KRITIS-Bedarfsträgern erreicht.
Im Rahmen dieses Präventionsauftrags wurden im Jahr 2020 insgesamt 73 Beratungsgespräche und Vorträge mit der bayerischen Wirtschaft durch die Zentrale Ansprechstelle Cybercrime des BLKA (ZAC) durchgeführt.

5.4 Digitale Prävention in Zeiten von Corona

In Zeiten der Coronapandemie können keine Präsenzveranstaltungen wie persönliche Beratungsgespräche oder Präventionsvorträge durchgeführt werden. Der Bedarf an polizeilichen Präventionsmaßnahmen im Bereich Cybercrime nimmt jedoch von Seiten der Unternehmen – gerade auch vor der verstärkt auftretenden Home-Office Situation und der damit verbundenen technischen Umsetzung – rapide zu. Um dem Bedarf dennoch gerecht zu werden und dem Präventionsauftrag der ZAC des BLKA nachzukommen, wurde das Projekt „Digitale Prävention für Unternehmen und Behörden“ bestehend aus drei Modulen ins Leben gerufen, die nachfolgend erläutert werden:

Das erste Modul „**Online Seminare**“ bildet die klassischen Präventionsvorträge in digitaler Form ab. Die während des Vortrages auftretenden Fragen der Teilnehmer können über einen Chat parallel zum Vortrag beantwortet werden.

Das zweite Modul „**Präventionsvideos**“ soll den einzelnen Bedarfsträgern in den Unternehmen einen schnellen und kompakten Überblick über einzelne Themengebiete wie

ausgewählte Phänomene oder Krisenmanagement verschaffen.

Der „**Workshop**“ als drittes und letztes Modul widmet sich einem Teilbereich des Awareness-Vortrags. Ziel ist es, mit einem hohen Anteil an Eigeninitiative der Teilnehmer den Inhalt eines gewöhnlichen Vortrags selbst zu erarbeiten und so einen nachhaltigeren Lerneffekt zu erzielen.

Die „Digitale Prävention im Bereich Cybercrime“ soll auch zukünftig, losgelöst vom Coronavirus, ergänzend zur Anwendung kommen, um die generelle Reichweite der Präventionsmaßnahmen des BLKA zu erhöhen.

6 Zukünftige **Entwicklung**

Superwahljahr 2021

Das Jahr 2021 gilt als sogenanntes „Superwahljahr“. Neben der Bundestagswahl im kommenden Herbst finden auch Landtagswahlen in Baden-Württemberg, Berlin, Mecklenburg-Vorpommern, Rheinland-Pfalz, Sachsen-Anhalt und Thüringen statt.

Dadurch ist „Wahlsicherheit“ ein bedeutendes Thema bei den für Cybersicherheit zuständigen Behörden. Meldungen in Zusammenhang mit den zurückliegenden Wahlen in den USA legen nahe, dass Wahlen ein Ziel – vor allem aus dem Ausland gesteuerter – Einflussnahmen sein können.

Deep Fakes

In der heutigen Zeit sind „Fake News“ ein weit verbreiteter Begriff. Schon ein auf falschen Tatsachen basierender Artikel oder ein simpler Tweet kann rufschädigend wirken. „Deep Fakes“ werden Dateien genannt, die mit Hilfe von künstlicher Intelligenz aus einem Datenpool an Informationen täuschend echt wirkende Bilder, Videos oder Audios herstellt, die nicht real sind. Diese Technologie verbessert sich rasant und wird immer einfacher zugänglich. Auf diese Weise können Kriminelle Videos – z.B. von Politikern – herstellen und damit versuchen ein falsches Meinungsbild zu verbreiten.

Zu rechnen ist dabei, neben klassischen Bedrohungen wie Spam- oder Ransomware-Kampagnen auch mit gezielten Angriffsversuchen. Diese bergen die Gefahr, dass sensible Informationen oder manipulierte Inhalte veröffentlicht werden, um Einfluss auf den öffentlichen Meinungsbildungsprozess zu nehmen und somit Wahlergebnisse zu beeinflussen („Hack and Leak“).

Quick Reaction Teams (QRT)

Bisherige Erfahrungen mit Cybercrime-Angriffen auf bayerische Unternehmen haben gezeigt, dass insbesondere Ransomware-Attacken häufig eine existenzielle Bedrohung für deren wirtschaftlichen Fortbestand darstellen. Hieraus ergeben sich für die Polizei besondere Herausforderungen, die regelmäßig über die polizeilichen Standardmaßnahmen zur Gefahrenabwehr und Strafverfolgung hinausgehen und allein durch die Zentrale Ansprechstelle Cybercrime des BLKA als zentraler Ansprechpartner der Bayerischen Polizei für alle bayerischen Unternehmen, Behörden, Verbände, Vereine und sonstigen Institutionen nicht zu bewältigen sind. Zur Etablierung gemeinsamer, bayernweit einheitlicher Mindeststandards für eine schnelle, professionelle und ganzheitliche polizeiliche Reaktion auf derartige Cyberangriffe werden künftig sogenannte QRT (Quick Reaction Teams) in allen Polizeipräsidien und dem Landeskriminalamt eingeführt.

Bekämpfung von Rechtsextremismus und Hasskriminalität im Netz

Im Internet und insbesondere in den sozialen Medien ist eine zunehmende Verrohung der Kommunikation zu beobachten. So äußern sich Internetnutzer immer öfter - vor allem gegenüber Personen des öffentlichen Lebens - in diffamierender Weise, die in vielen Fällen gegen das geltende deutsche Strafrecht verstößt. Betroffene sehen sich häufig einem extrem aggressiven verbalen Auftreten, Beleidigungen, Einschüchterungen oder sogar der Androhung von Straftaten bis hin zum Mord ausgesetzt.

Mit der Einführung des Netzwerkdurchsetzungsgesetzes (NetzDG) wurde im Jahr 2017 ein wichtiger Baustein zur Bekämpfung der Hasskriminalität im Netz geschaffen. Anbieter von sozialen Netzwerken werden mit diesem Gesetz verpflichtet, Beschwerden wegen rechtswidriger Inhalte zu prüfen und diese ggf. zeitnah zu löschen.

Das Maßnahmenpaket der Bundesregierung zur „Bekämpfung des Rechtsextremismus und der Hasskriminalität“ sieht außerdem die Einführung einer Meldepflicht für bestimmte Telemediendienstanbieter (TMDA) nach dem Netzwerkdurchsetzungsgesetz vor. So müssen auch bestimmte strafbare Inhalte, die den TMDA im Rahmen von Nutzerbeschwerden bekannt werden, an das Bundeskriminalamt (BKA) gemeldet werden, um eine adäquate Strafverfolgung zu ermöglichen.

Der Gesetzesentwurf wurde vom Deutschen Bundestag bereits im Juni 2019 verabschiedet, nach Ausfertigung des Gesetzes durch den Bundespräsidenten und der Veröffentlichung im Bundesgesetzblatt wird das Gesetz im Laufe des Jahres 2021 in Kraft treten.

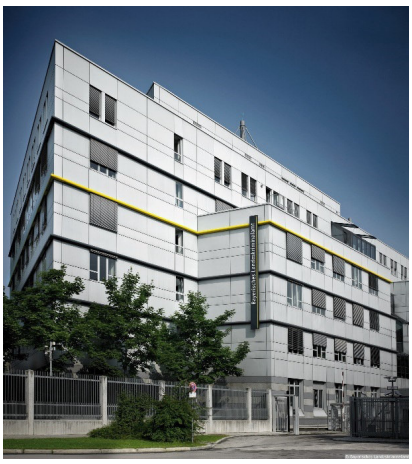
7 Fazit

Die Corona-Pandemie zeigt einmal mehr, dass Straftäter insbesondere im Deliktsbereich Cybercrime sehr agil auf gesellschaftliche Entwicklungen reagieren und diese für ihre kriminellen Ziele ausnutzen. Dabei werden ohne Rücksicht auf individuelle und gesellschaftliche Schäden alle Ziele angegriffen, die einen möglichst hohen kriminellen Gewinn versprechen. So wird die Resilienz von Privatpersonen und von Unternehmen gegenüber Cyberstraftaten fortwährend auf die Probe gestellt.

Dies gilt umso mehr, da die nach wie vor andauernde Pandemie die zunehmende Digitalisierung des Alltags weiter und schneller vorantreibt und somit quantitativ wie qualitativ gesteigerte Möglichkeiten für Cyberkriminelle entstehen. Die Gesellschaft nutzt vermehrt das Internet bzw. digitale Angebote für den Arbeitsalltag und die Freizeitgestaltung, finanzielle Transaktionen werden vermehrt online vorgenommen und der Handel mit Kryptowährungen wird mutmaßlich weiter ansteigen. Cyberkriminelle könnten dies künftig noch intensiver ausnutzen und vermehrt Online-Geschäfte und diesbezügliche virtuelle Zahlungssysteme attackieren.

Die Gefährdungslage im Bereich Cybercrime bleibt damit weiterhin auf einem sehr hohem Niveau und Cybersicherheit ist gegenwärtig wichtiger denn je zuvor. Um einer weiteren Steigerung dieses Bedrohungs- und Schadenspotenzials wirksam entgegenzutreten, kommt es maßgeblich auf eine Schärfung des Gefahrenbewusstseins bei den Nutzern des Internets und auf die Stärkung der digitalen Eigenverantwortung sowohl bei Privatpersonen als auch bei Unternehmen und deren Beschäftigten an. Dies bezieht sich sowohl auf persönliche Verhaltensweisen und Vorsichtsmaßnahmen als auch auf den konsequenten Einsatz von technischen Sicherungsmöglichkeiten wie z. B. regelmäßige Softwareupdates, Einsatz von Virenscannern und Firewalls oder regelmäßige Systemsicherungen.

Darüber hinaus sind die für Cybersicherheit zuständigen Behörden gefordert, ihre gemeinsamen Anstrengungen bei der Verhütung von Gefahren und Bekämpfung von Straftaten aus dem Bereich Cybercrime weiterhin auf hohem Niveau zu halten bzw. soweit möglich noch weiter zu intensivieren.



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
04/2021

Bildnachweis
BLKA
Unsplash.com

www.polizei.bayern.de