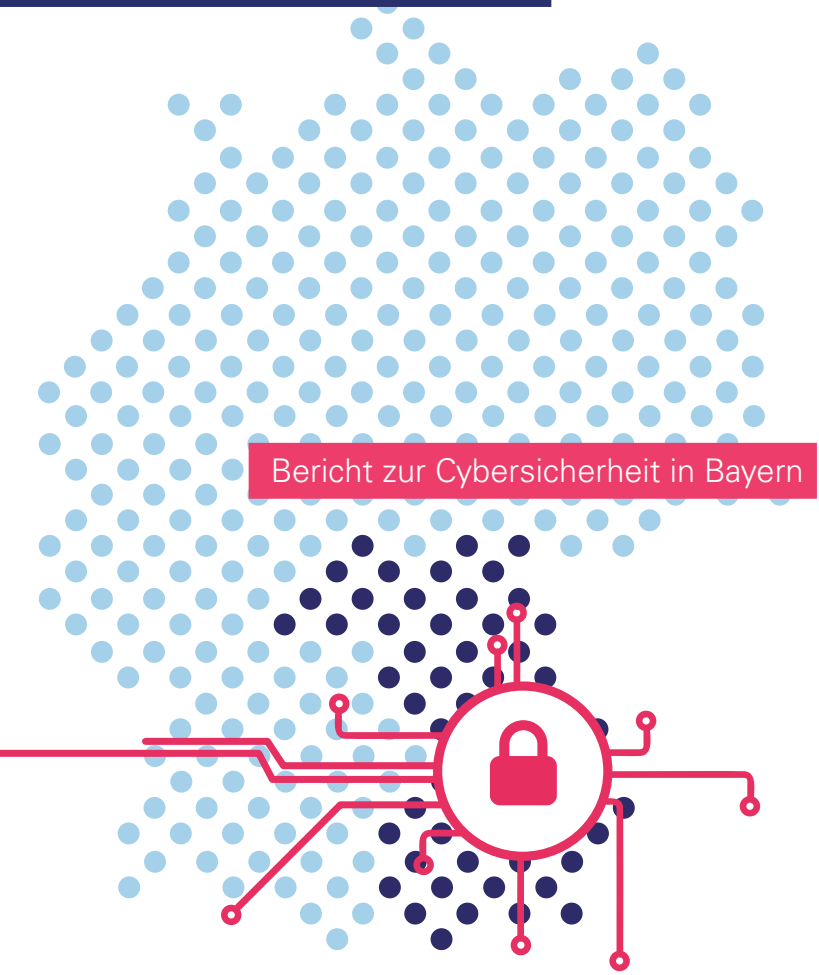
Bayerisches Staatsministerium des
Innern, für Sport und Integration

Bayerisches Staatsministerium der
Finanzen und für Heimat

CYBERSICHERHEIT IN BAYERN 2025



Bericht zur Cybersicherheit in Bayern

VORWORT

Die innere Sicherheit ist eine Grundvoraussetzung für unsere Freiheit und ein seit langem etablierter Markenkern der Politik der Bayerischen Staatsregierung.

Neben dem Schutz vor Gewalt, Verbrechen und Terrorismus, der Gewährleistung der Verfassung sowie dem Bevölkerungsschutz hat sich der Schutz von Staat, Wirtschaft und Gesellschaft vor Bedrohungen aus dem Cyberraum zu einem essenziellen Bestandteil der inneren Sicherheit entwickelt.

> *„Digitalisierung ist der große Megatrend unserer Zeit. Sie durchdringt alle Lebensbereiche. Unser Ziel ist es, auch im Cyberraum ein hohes Sicherheitsniveau für Bayerns Bürger und Unternehmen zu schaffen, die kritischen Infrastrukturen und die Handlungsfähigkeit des Staates zu schützen."*

Aufgrund der Entwicklungssprünge im Bereich der Künstlichen Intelligenz sinken die technischen Einstiegshürden für Täter und Tätergruppierungen, was auch zukünftig den Umfang, die Geschwindigkeit und Schlagkraft von Cyberangriffen erhöhen wird.

Trotz zunehmender Resilienz gegen Cyberangriffe liegt noch immer kein ausreichendes Bewusstsein für Cybergefahren in der Bevölkerung, aber auch bei Unternehmen vor. Gleichzeitig bleibt die Gefährdungslage auf einem anhaltend hohen Niveau. Mit dem Ziel, die Öffentlichkeit in Bayern über die Entwicklung der Bedrohungslage zu informieren und hinsichtlich der Notwendigkeit geeigneter Schutzmaßnahmen zu sensibilisieren, veröffentlichen das Staatsministerium des Innern, für Sport und Integration und das Staatsministerium der Finanzen und für Heimat daher seit 2022 jährlich diesen Bericht zur Cybersicherheit in Bayern.

Als gemeinsamer Lagebericht führt dieser die Erkenntnisse und Einschätzungen der mit Cybersicherheit befassten Stellen zusammen und ordnet die aktuellen Aktivitäten der Behörden und Einrichtungen mit Cybersicherheitsaufgaben entsprechend ein. Deren institutionalisierte Zusammenarbeit in der Cyberabwehr Bayern ermöglicht eine fortlaufende behördenübergreifende Beobachtung und Bewertung der Bedrohungslage.

Die daraus resultierenden Erkenntnisse können wir gemeinsam dazu nutzen, den Gefahren aus dem Cyberraum wirkungsvoll entgegen zu treten und die Cyberabwehr Bayern stetig dem Stand der Technik entsprechend fortzuentwickeln.

Denn weiterhin gilt: In Bayern leben, heißt sicherer leben!

Joachim Herrmann, MdL
Bayerischer Staatsminister
des Innern, für Sport und Integration

Albert Füracker, MdL
Bayerischer Staatsminister
der Finanzen und für Heimat

INHALT

I. AUSGANGSLAGE

Der vorliegende Bericht zieht eine Bilanz für die Zeit vom 01.01.2024 bis zum 31.12.2024 (Berichtszeitraum).

Die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben sehen eine anhaltend hohe Bedrohungslage im Cyberraum. Insbesondere waren im Berichtszeitraum verstärkt öffentliche Stellen, kritische Infrastrukturen und soziale Einrichtungen Ziele von Cyberangriffen.

Im Vergleich zu den Vorjahren zeigte sich eine deutliche Professionalisierung der Tätergruppen. Zugleich verschoben sich die Motivlagen: Neben finanziellen Interessen waren vermehrt auch mutmaßlich politisch motivierte Cyberangriffe festzustellen.

Um den ständig wachsenden Herausforderungen zu begegnen, hat Bayern in den vergangenen Jahren eine schlagkräftige Cybersicherheitsarchitektur aufgebaut. Neben Maßnahmen, wie beispielsweise die Errichtung des Landesamts für Sicherheit in der Informationstechnik (LSI), zeichnet sich diese insbesondere auch durch die etablierte, institutionalisierte Zusammenarbeit aller Behörden und Einrichtungen mit Cybersicherheitsaufgaben aus. Ein wesentlicher Erfolgsfaktor dabei ist die horizontale und vertikale Vernetzung zu den wichtigen Akteuren beim Bund und in anderen Ländern.

Durch internationale Kooperationen und innovative Ermittlungsmethoden konnten im Berichtszeitraum bedeutende Erfolge bei der Bekämpfung dieser Bedrohungen erzielt werden.

II. ALLGEMEINES LAGEBILD ZUR CYBERSICHERHEIT IN BAYERN

Die Cybersicherheitslage bleibt im Berichtszeitraum weiterhin angespannt.

Neben Erpressungslagen mittels DDoS-Angriffen, Spoofing und Ransomware-Angriffen bestimmten insbesondere Betrugsformen wie CEO-Fraud/Invoice-Fraud, Phishing, Carding oder das Ausnutzen von Schwachstellen in Soft- und Hardware die Cyberbedrohungslage.

Durch den Einsatz von KI sind Cyber-Akteure zwischenzeitlich in der Lage, ohne oder mit nur geringen IT-Kenntnissen ausgefeilte Angriffe zu entwickeln, mit denen sich teilweise auch robuste technische Sicherheitsmaßnahmen überwinden lassen. Insbesondere die Qualität und Quantität von Phishing-Angriffen sind durch den Einsatz von Künstlicher Intelligenz (KI) weiter gestiegen. Niederschwellig verfügbare Deepfake-Technologien ermöglichen es Angreifern, sich täuschend echt als andere Personen auszugeben – sei es in E-Mails, Sprachanrufen oder sogar in Videokonferenzen.

Besorgniserregend ist, dass kleine und mittelständische Unternehmen (KMU) aufgrund schwächerer IT-Sicherheitsvorkehrungen zunehmend zur bevorzugten Zielgruppe der Angreifer werden. Dies erscheint in Hinblick auf die hohe volkswirtschaftliche Relevanz der KMU besonders besorgniserregend.

Auch bayerische Kommunen waren aufgrund der Herausforderungen der fortschreitenden Digitalisierung der öffentlichen Verwaltung im Berichtszeitraum das Ziel verschiedener Cyberangriffe. Die Sicherheitslage bei kommunalen Infrastrukturen sowie deren Resilienz bei erfolgreichen Angriffen haben sich seit Gründung des LSI jedoch deutlich verbessert.

Die abstrakte Gefährdungslage für Behörden, Forschungseinrichtungen, Unternehmen und Kritische Infrastrukturen, Ziel von Cyberspionage oder-sabotageakten zu werden, ist unverändert hoch geblieben.

Darüber hinaus haben sich seit Beginn des russischen Angriffskriegs auf die Ukraine Desinformationskampagnen und andere Bedrohungsformen zu einem integralen Bestandteil hybrider Kriegsführung entwickelt.

Zum Teil sinkende Fallzahlen und Meldungen über die erfolgreiche Zerschlagung internationaler krimineller Strukturen (Take-Downs) durch die Sicherheitsbehörden sind kein Grund zur Entwarnung.

In allen nachfolgend aufgeführten Deliktsfeldern ist von einer erheblichen Dunkelziffer auszugehen. Legt man die Ergebnisse der Dunkelfeldbefragung des Bundeskriminalamts und der Polizei der Länder „Sicherheit und Kriminalität in Deutschland - SKiD 2020[1]“ zugrunde, werden deliktsübergreifend nur 17,9 % der Straftaten angezeigt.

Als mögliche Ursachen für die Nichtanzeige kommen in Betracht, dass kein oder nur geringer Schaden verursacht wurde und/oder die Opfer durch ein öffentliches Bekanntwerden eines Angriffs geschäftsschädigende Reputationsschäden fürchten. Zudem ist zu berücksichtigen, dass der Fokus der Betroffenen regelmäßig überwiegend auf der schnellen Wiederherstellung der Verfügbarkeit der betroffenen IT-Systeme liegt.

1 Die zweite Erhebungswelle SKiD 2024 wird aktuell aufbereitet und ausgewertet. Mit der Veröffentlichung von Ergebnissen ist voraussichtlich im Herbst 2025 zu rechnen.

III. VORHERRSCHENDE PHÄNOMENE

Im Berichtszeitraum bestimmten insbesondere folgende Phänomene die digitale Sicherheitslage in Bayern:

A RANSOMWARE[2]

Ransomware (*von englisch ransom für „Lösegeld"*) ist eine Form von Schadsoftware (Malware), deren Ziel es ist, zunächst unbemerkt in einem Computernetzwerk ausgebracht zu werden, unter Umständen sensible Daten zu exfiltrieren und anschließend zentrale Systeme und Dateien zu verschlüsseln.

Ransomware-Angriffe zählen seit Jahren zu den dominierenden Phänomenen im Bereich Cybercrime. Laut dem „Cybersecurity Threat Report" von Check Point Research entfielen im Berichtsjahr weltweit rund 25 Prozent aller Cyberangriffe auf Ransomware – Tendenz steigend. Die finanziellen Dimensionen solcher Angriffe sind erheblich. Lösegeldforderungen bewegen sich häufig im sechs- bis siebenstelligen Bereich – in Einzelfällen wurden sogar Summen von über zehn Millionen Euro gefordert. Doch nicht nur das Lösegeld selbst verursacht hohe Kosten: Produktionsausfälle, Datenverluste und Wiederherstellungsmaßnahmen schlagen zusätzlich zu Buche.

Die häufig mehrstufigen Angriffe verlaufen in den meisten Fällen weitgehend automatisiert und hochgradig professionell. In der Regel erfolgt dabei eine doppelte Erpressung (Double Extortion):

Zum einen wird angedroht, die zuvor entwendeten Daten zu veröffentlichen oder weiterzuverkaufen, sollte kein Lösegeld gezahlt werden. Zum anderen fordern die Angreifer das Lösegeld für die Wiederherstellung der verschlüsselten Daten und Systeme.

2 Bei Ransomware handelt es sich um Schadsoftware, bei der Daten der Opfer auf deren IT-Systemen verschlüsselt und damit unbrauchbar gemacht werden. Der zur Wiederherstellung benötigte Schlüssel wird im besten Falle nach Zahlung eines Lösegeldes durch die Täter zur Verfügung gestellt.

Dabei geraten längst nicht mehr nur große Unternehmen ins Visier der Angreifer. Zunehmend sind auch mittelständische Betriebe, Bildungseinrichtungen und kommunale Infrastrukturen betroffen.

In den vergangenen Jahren beobachteten die Sicherheitsbehörden in Bayern, ebenso wie das Bundesamt für Sicherheit in der Informationstechnik, die zunehmende Professionalisierung der Szene durch **„Cybercrime-as-a-Service" (CaaS)** als kriminelles Geschäftsmodell. Dieses arbeitsteilige Vorgehen ähnelt dem Outsourcing in der legalen Wirtschaft. Ein besonders relevantes Teilsegment ist das sogenannte **„Ransomware-as-a-Service" (RaaS)**. Hierbei stellen Entwickler ihre vorgefertigten Ransomware-Plattformen gegen eine Beteiligung an den Lösegeldern oder gegen Mietzahlungen zur Verfügung. Die eigentlichen Angriffe werden dann von sogenannten „Affiliates" ausgeführt – zum Teil professionellen, zum Teil nur technisch wenig versierten Kriminellen, die durch das Geschäftsmodell Zugang zu technisch hochentwickelten Angriffswerkzeugen erhalten.

Die bekanntesten Gruppierungen im Bereich Ransomware, die im Berichtszeitraum eine verstärkte Bedrohung für bayerische Organisationen darstellten, sind die auch aus der medialen Berichterstattung bekannten **LockBit** und **Phobos/8Base**.

Auch im vergangenen Jahr waren bayerische Ermittlungsbehörden wiederholt maßgeblich an konzentrierten Maßnahmen gegen internationale Ransomware-Gruppierungen – sog. Take-Downs – beteiligt. Zuletzt wurde hierbei in Zusammenarbeit mit dem FBI die deliktische IT-Infrastruktur der oben genannten Gruppierung „8Base" (Ransomware „Phobos") durch Maßnahmen der Zentralstelle Cybercrime Bayern (ZCB) und des Bayerischen Landeskriminalamts (BLKA), Dezernat 54 – Cybercrime beschlagnahmt.

B SCHWACHSTELLEN[3]

Auch das Berichtsjahr 2024 war erneut geprägt vom Auftreten schwerwiegender Sicherheitslücken in z.T. weitverbreiteten Hard- und Softwareprodukten. Den Angreifern eröffnen sich hier nach wie vor weitreichende und lukrative Angriffsflächen.

Die Cybersicherheitsbehörden beobachten in diesem Phänomenbereich, dass Cyberkriminelle Netzwerkkomponenten inzwischen als besonders lohnenswerte Ziele identifiziert haben. Angreifer konnten beispielsweise über eine Sicherheitslücke in Check Point Security Gateways sensible Daten aus dem lokalen Dateisystem der Systeme auslesen, in ähnlicher Weise konnten Besprechungsinformationen und Metadaten über eine Schwachstelle in Cisco WebEx Meeting Center offengelegt werden. Des Weiteren führte eine schwerwiegende Schwachstelle im Fortinet FortiClient EMS zu erfolgreichen Angriffen auf Einrichtungen, auch im kommunalen Bereich.

Dabei hätte eine Vielzahl der erfolgreichen Angriffe durch das rechtzeitige Einspielen der zur Verfügung stehenden Sicherheitsupdates (Patches) vermieden, zumindest aber erschwert werden können. Dies erfolgt aber in vielen Fällen immer noch zu spät oder gar nicht. Zum Teil liegt das darin begründet, dass Einrichtungen keine eigenen Kontrollmechanismen umsetzen und sich ausschließlich auf die rechtzeitige Umsetzung durch ihre IT-Dienstleister verlassen.

Werden diese Sicherheitslücken bekannt und entsprechende Warnhinweise veröffentlicht, wird kurz darauf häufig eine Zunahme entsprechender Angriffsversuche beobachtet. Bei besonders kritischen Schwachstellen werden Betreiber betroffener Systeme durch OSINT[4]-Recherchen identifiziert und von den Sicherheitsbehörden dann gezielt informiert.

---

3 Schwachstellen entstehen beispielsweise durch Fehler in der Programmierung, durch schwache Default-Einstellungen von IT-Produkten im Produktivbetrieb oder auch durch fehlkonfigurierte Sicherheitseinstellungen.

4 OSINT steht für Open Source Intelligence und bezeichnet die Sammlung und Analyse von öffentlich zugänglichen Informationen zur Gewinnung von Erkenntnissen. Diese Informationen können aus verschiedenen Quellen stammen, wie dem Internet, Presseerzeugnissen, Büchern und anderen öffentlich zugänglichen Datenbanken.

C DATEN- UND IDENTITÄTSDIEBSTAHL

Von Identitätsdiebstahl wird gesprochen, wenn personenbezogene Daten einer natürlichen Person durch Dritte missbräuchlich verwendet werden.

Moderne „Stealer"-Malware und Keylogger haben sich in ihrer Funktionalität erheblich weiterentwickelt. Sie sind mittlerweile in der Lage, sensible Informationen wie Zugangsdaten, Kundendatenbanken und sogar unternehmensinterne Geschäftsgeheimnisse nahezu unbemerkt auszulesen und weiterzuleiten.

Besonders der Zugriff auf geschäftlich genutzte E-Mail-Konten stellt ein lohnendes Ziel für Cyberkriminelle dar. Kompromittierte oder täuschend echt imitierte E-Mail-Adressen von Führungskräften oder Finanzverantwortlichen dienen dabei als ein initiales Einfallstor für entsprechende Angriffe mit Schadsoftware. Die Angreifer nutzen diese Zugänge auch gezielt, um betrügerische Überweisungen zu veranlassen oder umfangreiche Phishing-Kampagnen innerhalb der Organisation zu starten. Im Berichtszeitraum ist eine signifikante Zahl an gemeldeten Betrugsversuchen, die diesem Muster folgen, zu verzeichnen.

D PHISHING[5]

Phishing hat sich längst als eine der wirksamsten Methoden von Cyberkriminellen etabliert. Durch den gezielten Einsatz künstlicher Intelligenz hat sich die Qualität und Überzeugungskraft von Phishing-Kampagnen zuletzt nochmals massiv gesteigert. KI-gestützte Textgeneratoren ermöglichen es Tätern, täuschend echte E-Mails zu verfassen, die nicht nur sprachlich fehlerfrei, sondern auch auf die individuellen Lebensumstände ihrer Zielpersonen abgestimmt sind. Mit Einsatz von KI können

5 Unter dem Begriff Phishing (Neologismus von fishing, engl. für ‚Angeln') versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es z.B. an persönliche Daten einer Person zu gelangen oder sie z.B. zur Ausführung einer schädlichen Aktion zu bewegen. In der Folge werden dann beispielsweise Kontoplünderung oder Identitätsdiebstahl begangen oder eine Schadsoftware installiert.

die Texte anhand öffentlich zugänglicher Informationen – etwa aus sozialen Netzwerken, beruflichen Profilen oder Online-Publikationen – weiter personalisiert werden. So entstehen sehr authentisch wirkende Nachrichten, die selbst geübte Empfänger täuschen können. Mit den erbeuteten Zugangsdaten können weitere Straftaten vorbereitet oder begangen werden.

Im Berichtszeitraum war zudem ein bemerkenswerter Trend, das sogenannte „Quishing" (eine Wortkreuzung aus QR-Code und Phishing), zu beobachten. Dabei versendeten Täter massenhaft vermeintlich offizielle Bankanschreiben, versehen mit QR-Codes, die zur Installation angeblicher Sicherheitssoftware aufforderten. Tatsächlich führten die Codes jedoch zu täuschend echt gestalteten Phishing-Webseiten, über die Zugangsdaten abgegriffen wurden. Die professionelle Aufmachung und der Versand auf dem klassischen Postweg verliehen den Schreiben zusätzliche Glaubwürdigkeit und führten zu einer entsprechend hohen Erfolgsquote.

E CARDING

Unter dem Begriff „Carding" werden betrügerische Aktivitäten zusammengefasst, bei denen gestohlene Zahlungsinformationen widerrechtlich verwendet werden, um unautorisierte Transaktionen durchzuführen, wobei es sich meist um Kredit- und Debitkartendaten handelt.

Im Berichtszeitraum verlagerten Cyberkriminelle ihren Fokus zunehmend auf die Nutzung digital erbeuteter Kartendaten. Sie setzen dabei gestohlene Informationen aus Datenlecks, Phishing-Kampagnen oder kompromittierten Benutzerkonten ein, um damit gezielt Online-Einkäufe zu tätigen (sog. Card Not Present Fraud) – oft in hoher Frequenz und über automatisierte Systeme, so dass große Schäden entstehen.

F PAYMENT DIVERSION FRAUD

Eine Form des digitalen Betrugs ist das gezielte Umleiten von Zahlungsströmen durch gefälschte Kommunikation („Payment Diversion Fraud" oder „Invoice Fraud"). Die Täter nutzen gestohlene Identitäten und betreiben geschicktes Social Engineering, um sich als Geschäftspartner auszugeben. Bezugnehmend auf gemeinsame Projekte oder offene Rechnungen täuschen sie Änderungen bei den Zahlungsmodalitäten, meist neue Bankverbindungen, vor. Dabei agieren die

Betrüger nach erfolgter Zahlung sehr schnell, so dass der Betrug meist erst auffällt, wenn Gelder längst ins Ausland weitertransferiert wurden. Aufgrund der Kombination aus überzeugender Tarnung, zeitlichem Vorsprung und den im Geschäftsverkehr oft hohen Summen sind die entstehenden Schäden oft immens.

Im Berichtszeitraum wurden von der Bayerischen Polizei 617 derartiger Fälle verzeichnet. Nach 2023 (380), 2022 (310) und 2021 (130) bedeutet das einen erneuten deutlichen Anstieg der Fallzahlen.

G CYBERCRIME-AS-A-SERVICE[6] – CYBERKRIMINALITÄT ALS DIENSTLEISTUNG

Das Geschäftsmodell „Cybercrime-as-a-Service" hat sich als fester Bestandteil der digitalen Unterwelt etabliert. Zentrales Element der kriminellen Infrastruktur sind dabei illegale Exploit-Marktplätze. Auf diesen Plattformen werden Sicherheitslücken – insbesondere sogenannte Zero-Day-Schwachstellen – gehandelt, welche den Herstellern noch unbekannt und daher besonders lukrativ für Angreifer sind. Gefragt sind vor allem Schwachstellen in weit verbreiteten Business-Anwendungen und Cloud-Diensten, die häufig in KMU zum Einsatz kommen.

Die Vielzahl erfolgreicher Angriffe auf Remote-Zugangslösungen und Cloud-Umgebungen bei KMU kann auf diese Entwicklung zurückgeführt werden.

H CYBERSPIONAGE UND CYBERSABOTAGE

Den Fachkräftemangel in der IT-Branche nutzen die Nachrichtendienste totalitärer Staaten zunehmend, um Unternehmen zu infiltrieren. Diese Infiltration erfolgt im Zuge regulärer Bewerbungen vermeintlicher „IT-Fachkräfte" auf ausgeschriebene Stellen.

Insbesondere Organisationen aus sicherheitsrelevanten Bereichen, wie Verteidigung, Verwaltung und Forschung, stehen im Visier der Täter. Die hoch professionellen Angreifer legen zur Täuschung gefälschte Referenzen vor, oft unterstützt durch Drittparteien, die Identitätsprüfungen manipulieren und als Mittelsmänner z.B. bei der Zahlungsabwicklung auftreten.

---

6 Cybercrime-as-a-Service (kurz: „CaaS") 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 schlagen.

Das Leistungsspektrum der eingesetzten IT-Fachkräfte reicht von Webentwicklung bis hin zu Anwendungen mit künstlicher Intelligenz. Zum Schutz ihrer wahren Identität nutzen sie VPN-Dienste und manipulierte Bewerbungsbilder. Dabei sind vollständig ortsunabhängige Arbeitsmodelle häufig die Grundvoraussetzung, um in das Opferspektrum der „Bewerber" zu fallen.

Die für die vermeintlich erbrachte Arbeitsleistung gezahlten Einkünfte fließen häufig direkt in die Finanzierung des jeweiligen Regimes. Für die betroffenen Unternehmen stellen diese verdeckten Anstellungen ein erhebliches Risiko dar: Spionage und Datendiebstahl, Erpressung, gezielte Betriebsstörung.

Auch bayerische Unternehmen gerieten ins Visier solcher Kampagnen. Allerdings wurde im Berichtszeitraum keine bestätigte Kompromittierung bekannt.

I DESINFORMATIONSKAMPAGNEN, HACKTIVISMUS UND WEITERE HYBRIDE BEDROHUNGEN

Seit Beginn des russischen Angriffskriegs gegen die Ukraine Anfang 2022 haben sich Desinformationskampagnen zu einem integralen Bestandteil hybrider Kriegsführung entwickelt. Pro-russische Akteure setzen gezielt auf die Manipulation öffentlicher Meinung und das systematische Untergraben des gesellschaftlichen Vertrauens in staatliche Institutionen – auch in Deutschland. So riefen einschlägige Gruppen wiederholt über soziale Medien zu Cyberangriffen auf Unterstützerstaaten der Ukraine auf. In der Folge kam es bundesweit zu einer Vielzahl von Überlastungsangriffen (Distributed Denial of Service – DDoS), von denen auch bayerische Behörden betroffen waren. Diese blieben dank etablierter Schutzmechanismen bislang ohne nachhaltige Wirkung.

Ein besonders anschauliches Beispiel für eine breit angelegte Desinformationsoperation ist die sogenannte „Doppelgänger"-Kampagne, die ab März 2024 vom Bayerischen Landesamt für Verfassungsschutz beobachtet wurde. Ziel war die gezielte Verbreitung pro-russischer und antiwestlicher Narrative über gefälschte Nachrichtenbeiträge. Die Urheber der Kampagne nutzten massenhaft Fake-Accounts auf gängigen Social-Media-Plattformen wie X (vormals Twitter) und Facebook. Dort wurden täuschend echte Beiträge gestreut, häufig als Antwort auf virale Inhalte mit hoher Reichweite – ungeachtet ihrer thematischen Relevanz.

Die Botschaften waren professionell aufbereitet: Eine plakative Überschrift, ergänzender Text, ein Bild und ein Link zu einer gefälschten Nachrichtenseite, die der Optik renommierter Medienhäuser nachempfunden waren.

Zur Steigerung der Glaubwürdigkeit wurden echte Zitate namhafter Nachrichtenagenturen aus dem Kontext gerissen und propagandistisch umgedeutet. Die Kampagne bediente dabei sowohl wiederkehrende als auch aktuelle Themen: etwa die Kritik an westlicher Militärhilfe für die Ukraine, die Darstellung westlicher Demokratien als führungsschwach oder das bewusste Schüren von Misstrauen gegenüber Regierungen. Auch kurzfristige Ereignisse wurden in Echtzeit für die eigene Agenda instrumentalisiert.

J DDOS[7]-ANGRIFFE (DISTRIBUTED DENIAL OF SERVICE)

Auch im Jahr 2024 standen Distributed-Denial-of-Service (DDoS)-Attacken im Mittelpunkt der Zusammenarbeit der Sicherheitsbehörden im Handlungsfeld Cybersicherheit.

Dabei zeigte sich im Vergleich zu den Vorjahren bei den DDoS-Attacken eine deutliche Professionalisierung dieser Tätergruppen. Zugleich verschoben sich hier auch die Motivlagen: Neben finanziellen Interessen waren vermehrt politisch motivierte Cyberangriffe festzustellen, was die Herausforderungen für die Sicherheitsbehörden erheblich erhöhte. Durch internationale Kooperationen und innovative Ermittlungsmethoden konnten im vergangenen Jahr jedoch auch bedeutende Erfolge bei der Bekämpfung dieser Bedrohungen erzielt werden.

7 Unter Distributed Denial of Service (DDoS)-Angriffen versteht man die mutwillige Beeinträchtigung eines Internetdienstes durch eine Flut von Anfragen, mit dem Ziel, diesen durch die Menge der Anfragen zu überlasten und so im schlimmsten Fall vollständig zusammenbrechen zu lassen. Hierfür kommt eine Vielzahl unterschiedlicher Systeme in einem großflächig koordinierten Angriff zum Einsatz. Durch die hohe Anzahl der gleichzeitig angreifenden Rechner sind die Angriffe besonders wirksam. Ein DDoS-Angriff ist daran zu erkennen, dass er deutlich mehr Ressourcen als der normale Netzwerkverkehr beansprucht.

IV. MASSNAHMEN

Die dynamische Bedrohungslage im Cyberraum sowie die zunehmende Professionalisierung der Täter und Tätergruppierungen erfordert auch auf Seiten der Sicherheitsbehörden sowohl eine Intensivierung der individuellen Anstrengungen als auch ein starkes behördenübergreifendes Zusammenwirken. Die kooperative und komplementäre Zusammenarbeit der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben ist insbesondere mit folgenden Maßnahmen gewährleistet:

A PRÄVENTION & CYBERSICHERHEITSBERATUNG

Die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben ergreifen umfassende Präventionsmaßnahmen, um Sicherheitsrisiken im Cyberraum zu minimieren. Die Maßnahmen schützen dabei nicht nur die staatliche Infrastruktur, sondern richten sich auch gezielt an Körperschaften, Unternehmen und Bürger.

Die unterschiedlichen, aufeinander abgestimmten Präventionsangebote von Polizei, Justiz und Verfassungsschutz für den Bereich Wirtschaft und Gesellschaft werden auf Grundlage der obigen Lageerkenntnisse fortlaufend bedarfsgerecht weiterentwickelt.

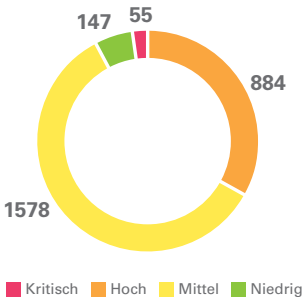
Beim BLKA besteht die Zentrale Ansprechstelle Cybercrime (ZAC), die unter der Hotline 089/1212-3300 erreichbar ist und Unternehmen sowie Institutionen als kompetenter Ansprechpartner zur Verfügung steht. Als einer der Schwerpunkte hat sich im Bereich der ZAC die Präventionsarbeit herauskristallisiert. So führte die ZAC im Berichtszeitraum 73 Präventionsveranstaltungen durch, in denen die Teilnehmer der verschiedenen Institutionen hinsichtlich der aktuellen Gefahren sensibilisiert und potentielle Lösungsmöglichkeiten dargelegt wurden. Das Credo ist hier „Hilfe zur Selbsthilfe“ und das Heben des Themas IT-Sicherheit auf die höchsten Führungsebenen. Explizit für diese Hierarchieebenen bietet die ZAC die Möglichkeit, eventuelle Szenarien im Rahmen eines interaktiven Planspiels oder einer Krisenstabsübung (im Bereich KRITIS) zu üben. Weiterhin konnten in zahlreichen Fällen Unternehmen aufgrund von Erkenntnissen aus laufenden polizeilichen Ermittlungsverfahren rechtzeitig vor einer unmittelbar bevorstehenden Verschlüsselung gewarnt werden.

Das LSI informiert weiterhin mit seinem kostenlosen Warn- und Informationsdienst tagesaktuell über die neuesten Gefährdungslagen und Risiken. In Warnmeldungen werden konkrete Anhaltspunkte zu dem jeweiligen Sicherheitsrisiko bzw. den bereits ermittelten Angriffen genannt. Im Berichtszeitraum wurden insgesamt 2664 neue Meldungen zu Schwachstellen veröffentlicht, darunter 55 als kritisch

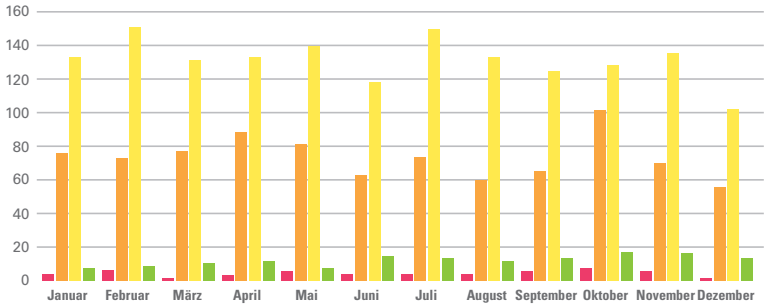
eingestufte. Die jeweilige Kritikalität dieser Meldungen ist in den nachfolgenden Grafiken aufgeschlüsselt.

Grundsätzlich konnte die Sicherheitslage der Kommunen in Bayern, also die Abwehr sowie deren Resilienz bei erfolgreichen Angriffen auch durch die zahlreichen Angebote des LSI für die Kommunen in den letzten Jahren deutlich verbessert werden. Insbesondere ist das LSI-Siegel „Kommunale IT-Sicherheit" ein geeignetes und praxisorientiertes Mittel, um IT-Sicherheit vor Ort zu stärken.

Warnmeldung nach Kritikalität



Warnmeldung nach Monat



Zusätzlich werden technische Orientierungshilfen und Unterlagen für ein Notfallmanagement, laufende Angriffswellen und andere Bedrohungen bereitgestellt. Das LSI bietet einen kostenfreien Online-Mitarbeitersensibilisierungskurs für die öffentliche Verwaltung – Staat und Kommunen – und konkrete technische Beratung zu allen Fragen der IT-Sicherheit.

Ein weiterer wichtiger Punkt ist die Kooperation mit der Forschung. Ein Beispiel ist das gemeinsame Forschungsprojekt „Herausforderungen für die Cybersicherheit durch Künstliche Intelligenz" (HeCKI) des LSI und der OTH Amberg-Weiden,

dessen Ziel es ist, Risiken und neuartige Bedrohungen durch künstliche Intelligenz zu analysieren und darauf aufbauend innovative Lösungen zu entwickeln.

Das Cyber-Allianz-Zentrum Bayern (CAZ) im Bayerischen Landesamt für Verfassungsschutz engagierte sich im Jahr 2024 mit zahlreichen Informations- und Sensibilisierungsveranstaltungen. Neben Warnungen vor Ausspähungsaktivitäten ausländischer Dienste standen insbesondere Cyberangriffe auf kritische Infrastrukturen im Fokus. Die konstant hohen Fallzahlen unterstreichen den fortbestehenden Bedarf an zielgerichteter Prävention.

B BEWÄLTIGUNG VON VORFÄLLEN

Straftaten in Zusammenhang mit Cyberkriminalität können bei jeder Polizeidienststelle in Bayern angezeigt werden. Beginnend mit Schwerpunktsachbearbeitern bei den lokalen Polizeiinspektionen bis hin zu hochspezialisierten Ermittlern und IT-Forensikern bei den Kriminalpolizeidienststellen sowie beim BLKA stehen auf allen polizeilichen Ebenen kompetente Ansprechpartner für Cyberkriminalität zur Verfügung.

Mit den im Jahr 2021 installierten Cybercrime „Quick-Reaction-Teams" (QRT) gewährleistet die Polizei eine Rund-um-die-Uhr-Verfügbarkeit qualifizierter Fachkräfte, um zeitnah auf die teilweise existenzbedrohenden Gefahren für die Unternehmen reagieren zu können. Durch den Einsatz der QRT kann der betroffenen Institution Unterstützung im technischen Bereich, z.B. bei der Netzwerkseparierung und im Rahmen eventueller Verhandlungen mit den Tätern gewährt werden. Die QRT kamen im Berichtszeitraum bayernweit in 172 Fällen zum Einsatz.

Die Bürgerhotline der Bayerischen Polizei für IT-Notfälle (089/1212-4400) wurde im Berichtszeitraum 998-mal von Bürgerinnen und Bürgern in Anspruch genommen. 531 Telefongespräche hatten Cybercrime-Straftaten zum Inhalt. In 209 Fällen konnte der Anrufer präventiv beraten werden.

Bei dem Verdacht eines Cyberangriffs mit nachrichtendienstlichem Hintergrund steht das CAZ als vertraulicher Ansprechpartner für Unternehmen, Hochschulen, Forschungseinrichtungen und KRITIS zur Verfügung.

Neben technischen und präventiven Maßnahmen ist auch eine konsequente Strafverfolgung entscheidend für die Eindämmung der Cyberkriminalität. In komplexen und schwerwiegenden Fällen von Cybercrime, dazu zählen insbesondere Cyberangriffe auf Unternehmen und öffentliche Einrichtungen, ermittelt die im Jahr 2015 gegründete ZCB bei der Generalstaatsanwaltschaft Bamberg. Die ZCB verfügt über

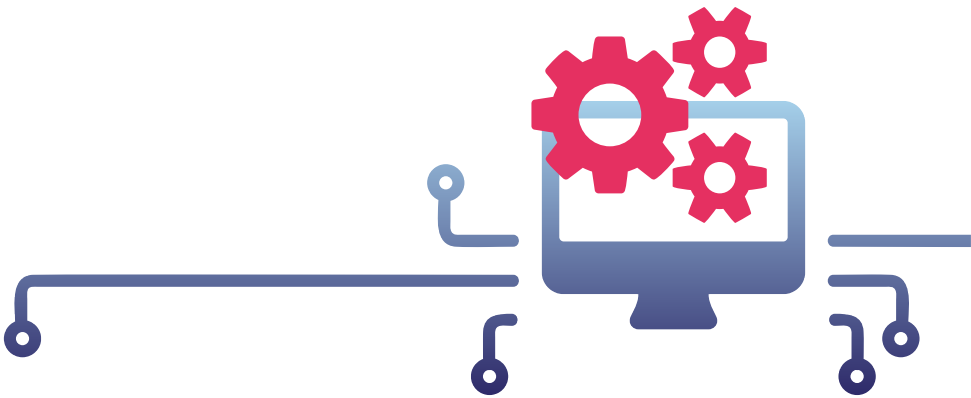
spezialisierte Einheiten für die Bereiche Cybertrading, Angriffe auf Unternehmen und öffentliche Einrichtungen sowie den Betrieb krimineller Handelsplattformen und sog. Fake-Shops. Trotz des in der Regel sehr konspirativen Vorgehens konnten bereits mehrere große Tätergruppen identifiziert und strafrechtlich belangt werden. Daneben erfolgt weiterhin die kontinuierliche Nutzung und Mitwirkung an innovativen Ermittlungs-Tools, etwa dem genannten Phishing-Seiten-Detektor BigPhish, dem DarkWeb Monitor und dem Kryptoanalyse-Tool Graphsense. Eine Forschungskooperation mit dem Austrian Institute of Technology (AIT) dient der Weiterentwicklung des KI-gestützten Fake-Shop-Detektors für den Ermittlungsalltag.

Die Sensibilisierung potenzieller Opfer erfolgt auch durch Vorträge und Informationsveranstaltungen, wie etwa beim „Cybersecurity Day", den die IHK für München und Oberbayern gemeinsam mit dem Bayerischen Staatsministerium des Innern, für Sport und Integration sowie dem Bayerischen Staatsministerium der Justiz ausrichtet.

IT-Sicherheitsvorfälle im Aufgabenbereich des LSI werden im Cyber Defence Center (CDC) des LSI aufgenommen und durch die IT-Sicherheitsexperten des Bayern-CERTs bearbeitet. Bei größeren Vorfällen, sog. Major Incidents, wird eine Task Force eingerichtet, die sich ausschließlich um die Eindämmung, Behandlung und forensische Analyse des jeweiligen Vorfalls kümmert.

Die IT-Sicherheitsexperten des LSI unterstützen auch bei Vorfällen in Kommunen oder Unternehmen der kritischen Infrastruktur. Hierbei ist eine enge Abstimmung mit der Bayerischen Polizei ein entscheidender Erfolgsfaktor.

Gleichzeitig zeigten Projekte zur Verbesserung der Datensicherheit in Unternehmen, wie z. B. „Cyberfestung" oder der Ausbau kommunaler IT-Sicherheitsstrukturen, wie praxisnahe Prävention funktionieren kann.



C BEHÖRDLICHE IT-SICHERHEIT

Das allgemeine Cybersicherheitsniveau soll in der EU mithilfe der sogenannten „NIS-2-Richtlinie" (Richtlinie (EU) 2022/2555) weiter gesteigert werden. Die NIS-2-Richtlinie definiert dazu Maßnahmen, die von Bund und Ländern umzusetzen sind. Mit dem 2017 eingerichteten LSI und den gesetzlichen Regelungen zu angemessener Informationssicherheit war Bayern hierfür bereits hervorragend aufgestellt. Die Umsetzung der NIS-2-Richtlinie stellte daher in der bayerischen Staatsverwaltung keine Herausforderung dar und wurde fristgerecht abgeschlossen. Das LSI nimmt im Zuge dessen die Aufgaben einer Aufsichts- und Meldebehörde für IT-Sicherheit in Bayern wahr, wobei das Bayern-CERT im LSI als operatives „Computer Security Incident Response Team" (CSIRT) agiert. Im Rahmen der Umsetzung der NIS-2-Richtlinie hat das LSI zudem auch die Verfügbarkeit seiner Dienste erweitert und ist mit dem „digitalen Ersthelfer" bei akuten IT-Vorfällen nun 24/7 erreichbar. Das LSI unterstützt damit betroffene Stellen in kritischen Lagen bei der Erstbewertung und Einleitung von Gegenmaßnahmen rund um die Uhr.

Das LSI stellt für Kommunen bereits ein Übungspaket mit einem einfachen Leitfaden zur Durchführung sog. „Table-Top-Übungen" bereit, mit dem sich in mehreren Szenarien zu fiktiven, aber realitätsnahen Bedrohungen, Notfallübungen durchführen lassen.

Mit der Zukunftskommission #Digitales Bayern 5.0 arbeiten Freistaat und Kommunen unter Federführung des Staatsministeriums der Finanzen und für Heimat gemeinsam daran, die digitale Transformation der Kommunalverwaltungen weiter voranzutreiben. Hierbei werden in enger Zusammenarbeit auch neue Maßnahmen vereinbart, um die IT-Sicherheit in den bayerischen Kommunen flächendeckend zu steigern und damit eine nachhaltige Digitalisierung sicherzustellen.

D BEHÖRDENÜBERGREIFENDE ZUSAMMENARBEIT

Ein regelmäßiger und schneller Austausch von Informationen und Erkenntnissen ist wesentlicher Erfolgsfaktor bei der Bewältigung von Cybersicherheitsvorfällen. Innerhalb Bayerns wurden hierfür mit der Errichtung der Cyberabwehr Bayern (CAB) bereits zum Jahresanfang 2020 der notwendige organisatorische Rahmen geschaffen.

Mit der Entsendung von bayerischen Verbindungsbeamten aus der CAB in das Nationale Cyber-Abwehrzentrum (Cyber-AZ) besteht nun außerdem eine wichtige Scharnierfunktion zum Bund. Ausgehend von den in der Pilotphase identifizierten Mehrwerten für die Arbeit der CAB ist es ein wichtiges Anliegen, diese horizontale Vernetzung zu verstetigen. Ebenso ist die ZCB als einer der Vertreter der Länderstaatsanwaltschaften nun dauerhaft beim Cyber-AZ vertreten.

Ein weiterer Meilenstein hinsichtlich des Informationsaustausches ist die vom LSI initiierte, bayerische kommunale „Sharing Community", die auf dem Open-Source-Tool MISP basiert. Hierüber können maschinenlesbar Angriffsindikatoren automatisch ausgetauscht werden, um laufende Kampagnen frühzeitig zu identifizieren und Abwehrmaßnahmen zu optimieren.

Neben dem Ausbau eigener Kompetenzen im Bereich IT-Sicherheit wurde auch die übergreifende Zusammenarbeit mit verlässlichen Partnern weiter intensiviert. Die neue Allianz zwischen dem LSI, Hessens CyberCompetenceCenter (Hessen3C) und der Cybersicherheitsagentur Baden-Württemberg (CSBW) stellt dabei einen Meilenstein in der operativen und strategischen Zusammenarbeit der drei Länder dar. Durch intensiven Wissensaustausch und gemeinsame Fortbildungsmaßnahmen sowie gemeinsamen Austausch mit der Fachöffentlichkeit unterstützen sich die IT-Sicherheitsexperten der Partnerländer gegenseitig, um Cyberbedrohungen wirksam zu bekämpfen und Angreifern einen Schritt voraus zu sein.

V. AUSBLICK

Die Cybersicherheitslage bleibt angespannt – in Bayern, Deutschland und in Europa. Angriffe werden gezielter, technischer und internationaler. Staatliche und kriminelle Akteure nutzen Schwachstellen in exponierten Systemen, oft bevor sie überhaupt öffentlich bekannt sind. Gleichzeitig verwischen die Grenzen zwischen Spionage, Sabotage und Erpressung. Was früher lokal begann, wirkt heute global.

Die Entwicklung im Bereich der generativen KI unterstreicht einmal mehr die Notwendigkeit, die Möglichkeiten von KI auch zur Verkleinerung der Angriffsflächen zum Einsatz zu bringen. Aber auch die Schutzmaßnahmen müssen so weiterentwickelt werden, dass sie KI-generierte Angriffe zuverlässig erkennen und abwehren können.

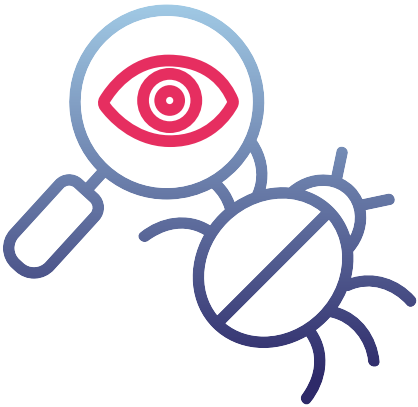
Die Antwort darauf kann nur im engen Schulterschluss gelingen. In Bayern bündeln zahlreiche Stellen ihre Kräfte zu einer schlagkräftigen und effektiven Cyberabwehr: Polizei, Justiz, Verfassungsschutz, Datenschutz- und Sicherheitsbehörden arbeiten gemeinsam daran, die digitale Widerstandskraft des Freistaats fortlaufend zu stärken. Dabei geht es nicht nur um das technische Abwehren von Angriffen, sondern auch um Aufklärung, Prävention, Strafverfolgung und Resilienzstärkung.

Die Vielzahl an Angriffen im Berichtszeitraum zeigt deutlich, wie groß das Risiko Ziel von Cyberangriffen zu werden mittlerweile ist. Dennoch lässt sich ein gemeinsamer Nenner feststellen: Durch frühzeitige Erkennung, technische Gegenmaßnahmen, klare Kommunikation und die Unterstützung spezialisierter Behörden können viele Angriffe begrenzt oder erfolgreich abgewehrt werden. Konsequentes Handeln, enge Zusammenarbeit und technische Kompetenz sind weiterhin entscheidend, um die Resilienz der öffentlichen Infrastruktur zu sichern.

WEITERFÜHRENDE INFORMATIONEN

BAYERISCHE CYBERSICHERHEITSSTRATEGIE 2.0

CYBERSICHERHEIT IN BAYERN 2024



Impressum

Herausgeber: Bayerisches Staatsministerium des Innern, für Sport und Integration
Odeonsplatz 3, 80539 München
www.innenministerium.bayern.de

Bayerisches Staatsministerium der Finanzen und für Heimat
Odeonsplatz 4, 80539 München
info@stmfh.bayern.de, www.stmfh.bayern.de

Bildrechte: AdobeStock/vectorwin
Grafik: Saskia Kölliker
Stand: Oktober 2025
Druck: Landesamt für Digitalisierung, Breitband und Vermessung,
Alexandrastraße 4, 80538 München
Gedruckt auf umweltzertifiziertem Papier (PEFC, FSC)

Das Bayerische Innenministerium im Internet:

www.innenministerium.bayern.de

www.x.com/BayStMI

www.instagram.com/BayStMI

www.facebook.com/BayStMI

www.youtube.de/BayerischesInnenministerium

„Let's talk Innenpolitik" mit Joachim Herrmann – unser Podcast auf allen großen Plattformen