Bayerisches Staatsministerium des
Innern, für Sport und Integration

Rede des Bayerischen Staatsministers des Innern,
für Sport und Integration, Joachim Herrmann,

anlässlich der Pressekonferenz zur Vorstellung des
Berichts zur Cybersicherheit in Bayern 2026

am Montag, 31. August 2026 in München

Es gilt das gesprochene Wort!

Anrede!

Einleitende Worte

Ich **freue** mich, auch in diesem Jahr wieder unseren **Bericht zur Cybersicherheit in Bayern 2026** zusammen mit meinen Kollegen **Finanzminister Füracker** und **Justizminister Eisenreich** hier im **Bayerischen Landeskriminalamt** vorstellen zu dürfen.

Allgemeine Cybersicherheitslage

Die **Bedrohungslage im Cyberraum** ist so **virulent und vielschichtig** wie nie zuvor. Viele Cyberangriffe sind heute **bedingt durch geopolitische Spannungen**. Zugleich wirkt der **technologische Fortschritt** wie ein Katalysator. Das ist positiv wie negativ.

KI ist eine der wichtigsten Zukunftstechnologien und **strategische Chance**. Gleichzeitig gehen mit deren Einsatz auch ein enormes **Missbrauchspotenzial** und **steigende Anforderungen** an den **Schutz der IT-Infrastrukturen** einher. Das zeigte uns etwa der Vorfall des **KI-Modells** „**Claude Mythos**“ im Frühjahr dieses Jahres, als das automatisierte Finden von Software-Schwachstellen weltweites Aufsehen erregte.

Cybersicherheitslage Bayern

Nach den Erkenntnissen der bayerischen Cybersicherheitsbehörden blieb auch bereits **2025** die **Cyberbedrohungslage in Bayern** auf einem **hohen Niveau** mit **komplexer werdenden Angriffszenarien**. Neben Wirtschaftsunternehmen gerieten immer häufiger **Behörden und KRITIS-Einrichtungen** ins Visier der zunehmend professionell agierenden Angreifer.

Fallzahlen Cybercrime nach PKS

In den diesjährigen Lagebericht zur Cybersicherheit in Bayern wurden **erstmalig** auch die **Fallzahlen zu Cybercrime** aus der **Polizeilichen Kriminalstatistik** *(PKS)* **aufgenommen**. Für den Berichtszeitraum 2025 weist diese Statistik – einschließlich Auslandstaten – **49.468 erfasste Straftaten im Bereich Cyberkriminalität** aus. Das ist ein **leichter Anstieg** *(+1,7%)* im Vergleich zu 2024 *(48.643).* Wir gehen jedoch **unverändert von einer erheblichen Dunkelziffer** aus.

Die **Bandbreite der Delikte** reicht von **Identitätsdiebstahl** über **Phishing** bis hin zum **Computerbetrug** im Zahlungsverkehr und Onlinehandel. Dabei wird, wie auch in den

Vorjahren, der **überwiegende Teil** *(72 %)* **der Straftaten aus dem Ausland** begangen.

Normative Grundlagen für „aktive Cyberabwehr“

Ich **begrüße** es daher sehr, dass mit dem **Gesetz zur Stärkung der Cybersicherheit** und dem vom Bundeskabinett am 12. August 2026 beschlossenen **Gesetzentwurf zur Reform des Nachrichtendienstrechts** die **normativen Grundlagen** für eine **aktive Cyberabwehr** geschaffen werden sollen. Zentral sind dabei die **neuen digitalen Aufklärungsbefugnisse** für die Sicherheitsbehörden und die Möglichkeit, künftig unter engen Voraussetzungen auch **aktive Schutzmaßnahmen ergreifen** zu können.

DDoS-Angriffe

Gezielte Unterbrechungen der Verfügbarkeit von Internetseiten oder -diensten mittels sogenannter **DDoS-Angriffe** haben in 2025 **weiter** erheblich **zugenommen**. Ein Grund hierfür sind die **geringen Einstiegshürden für cyberkriminelle Akteure**. DDoS-Angriffe werden zunehmend auch von **hacktivistischen Akteuren** mit **politischen Motiven** eingesetzt.

Eine zentrale Rolle spielte die **prorussische Gruppierung NoName057(16)**, einer der **aktivsten Betreiber politisch motivierter DDoS-Kampagnen**. Sie richten sich insbesondere gegen Staaten und Organisationen, die die Ukraine politisch oder militärisch unterstützen.

Ransomware-Angriffe und Phishing

Neben DDoS-Angriffen dominieren in Bayern weiterhin klassische Phänomene wie **Phishing**, um mittels zum Beispiel gefälschter E-Mails an Daten zu kommen, und **Ransomware-Angriffe**. Das Landeskriminalamt registrierte 2025 einen **Anstieg der Ransomwarefälle von 18 % gegenüber 2024** *(2025: 230; 2024: 195)*. Neben **Unternehmen** waren auch **öffentliche Einrichtungen in Bayern** von solchen Angriffen betroffen. Ransomware-Angreifer gehen dabei zunehmend professionell vor und bedienen sich vermehrt sogenannter „Verhandlungsteams“ zur Kommunikation mit den Opfern.

Zudem wird der Phänomenbereich von **wenigen bekannten und etablierten Organisationen** beherrscht. Als **neue Ransomware-**

Gruppierungen in Bayern sind in 2025 „**Safepay**“ und „**Sarcoma**“ aufgetreten. Sie verübten eine Vielzahl von Angriffen. Bei der Gruppierung „**Lockbit**“ dagegen konnte aufgrund der internationalen Ermittlungen ein **deutlicher Rückgang** festgestellt werden.

Auch **kompromittierte E-Mail-Accounts und Phishing** waren 2025 ein prominenter **Angriffsvektor**. Eine besonders **erfolgreiche Variante** stellte erneut das „**Quishing**“ dar. Um an sensible Daten zu gelangen, wurden hierbei täuschend **echt wirkende Schreiben mit QR-Codes** versandt, die auf betrügerische Seiten verweisen, oder **offizielle QR-Codes mit gefälschten QR-Codes** überklebt.

Hybride Bedrohungen

Neben **finanziellen Motiven** von Cyberkriminellen gewinnen **politisch motivierte Cyberangriffe** und **Informationsmanipulation** durch Desinformationskampagnen zunehmend an Bedeutung. Ausländische Nachrichtendienste möchten damit Informationen beschaffen, Einfluss nehmen oder Sabotage betreiben.

Seit dem Angriffskrieg Russlands auf die Ukraine stellen wir fest, dass die **hybride Bedrohung unserer Gesellschaft** mit dem kulminierten Auftreten von Spionage, Sabotage, Desinformation und Cyberangriffen ein **nie gekanntes Level** erreicht hat. Der **Schutz unserer Bevölkerung vor hybriden Angriffen duldet keinen Aufschub** und muss oberste Priorität haben.

Russische Akteure

Im Bereich der **Cyberspionage** und der **Desinformation** stellt das **Cyber-Allianz-Zentrum Bayern** *(CAZ)* bereits seit Jahren umfangreiche **Operationen staatlicher russischer Akteure** fest. Auch im Jahr 2025 setzte das CAZ – nach den erfolgreichen Analysen in 2024 – die Beobachtung der **russischen Desinformationskampagne** „**Doppelgänger**“ fort. Die bisherigen Erkenntnisse konnten im Bereichtszeitraum erneut **bestätigt** und weiter vertieft werden.

Aktuelle Kampagne „Matryoshka“

Aktuell sind im Kontext der anstehenden **Landtagswahlen in Ostdeutschland** Aktivitäten der sogenannten „**Matryoshka-Kam-**

pagne“ zu beobachten, die eine **Polarisierung zwischen Ost- und Westdeutschland** befördern soll.

Nordkoreanische Cyberakteure

Daneben machten 2025 insbesondere **nordkoreanische Cyberakteure** mit **zwei Kampagnen** auf sich aufmerksam. Mit der Kampagne „**Operation Dream Job**“ werden **gefälschte Stellenangebote** auf Plattformen wie LinkedIn inseriert, um Kontakt zu IT-Experten und Mitarbeitern der Rüstungs- und Technologiebranche herzustellen. **Vermeintliche „Personalvermittler**“ infizieren anschließend die Systeme ihrer Opfer über Dokumente oder Links, die Schadsoftware ausführen, um Systeme auszuspähen und sensible Daten zu stehlen.

Umgekehrt funktioniert die Kampagne „**(Fake) IT Worker**“, bei der sich **nordkoreanische Akteure** als Bewerber **mit gefälschten Identitäten** in westliche Firmen einschleusen möchten.

Cyberspionage China

Daneben stehen Unternehmen verschiedenster Sparten im Fokus **staatlicher chinesischer Cyberspionage**. Dazu gehören insbesondere die **Verteidigungsindustrie** sowie **Forschungseinrichtungen**.

Erfolge der Sicherheitsbehörden

Unsere **Sicherheitsbehörden gehen konsequent gegen Cyberkriminalität vor**. Auch 2025 gelangen ihnen wieder zahlreiche Erfolge, von denen ich zwei Beispiele herausgreifen möchte:

Das Bayerische Landeskriminalamt führte unter Leitung der Zentralstelle Cybercrime Bayern *(ZCB)* erfolgreiche Ermittlungen gegen die **Ransomware-Gruppierung „Phobos**“. Bei einer koordinierten Aktion von **Strafverfolgungsbehörden** aus **14 Ländern** konnten **vier Anführer der Ransomware-Gruppe „8Base**“, dem größten operativen Vertriebspartner des Phobos-Netzwerks, **festgenommen** werden.

Besonders eindrücklich zeigt eine erfolg-

reiche Zusammenarbeit auch die **inter-nationale** „**Operation Stream**“. Hier sind Polizei und Staatsanwaltschaft in Bayern in koordinierter Aktion mit **Europol** und 38 beteiligten Staaten gegen die weltweite **Verbreitung kinderpornografischer Inhalte** vorgegangen. Die internationale Zusammenarbeit führte zur Identifizierung von **über 1.600 Tatverdächtigen** und rund **80 Festnahmen**. In Folge der „Operation Stream“ wurde das BLKA durch Europol mit dem **Europol Excellence Award in Innovation** ausgezeichnet.

Dank und Schlussworte

Ich **danke** allen Beschäftigten der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben sowie Finanzminister **Füracker** und Justizminister **Eisenreich** für ihr **unermüdliches Engagement** für die Cybersicherheit und die Resilienz von Staat, Wirtschaft und Gesellschaft. Durch die **konsequente Nutzung aller** zur Verfügung stehenden **Lageinformationen, regelmäßige Zusammenarbeit** aller Cybersicherheitsbehörden sowie das **proaktive Management**

der Risiken können wir den Gefahren im Cyberraum auch künftig wirkungsvoll begegnen.