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 2025

am Mittwoch, 12. November 2025 in München

Es gilt das gesprochene Wort!

Anrede!

Einleitende Worte

Ich **freue** mich, dass ich unseren **Bericht zur Cybersicherheit in Bayern 2025** wieder gemeinsam mit **Staatsminister Eisenreich** und **Staatsminister Füracker** vorstellen kann, dieses Mal hier im **Bayerischen Landeskriminalamt**.

Bedeutung der Cybersicherheit für die Innere Sicherheit

Der **Schutz** von **Staat**, **Wirtschaft** und **Gesellschaft** vor **Bedrohungen aus dem Cyberraum** hat sich in den letzten Jahren zu einem **essenziellen Bestandteil der Inneren Sicherheit** entwickelt. Wir treten den **Gefahren aus dem Cyberraum wirkungsvoll entgegen**. Dazu nutzen wir die aus der **gemeinsamen Lagearbeit** unserer Behörden und Einrichtungen mit Cybersicherheitsaufgaben resultierenden Erkenntnisse. Außerdem entwickeln wir die **Fähigkeiten und Befugnisse** der Sicherheitsbehörden bedarfsgerecht **fort**.

Cybersicherheitslage

Eine wichtige Erkenntnis ist: Die **Bedrohungslage im Cyberraum** ist auf einem

anhaltend hohen Niveau. Diese Feststellung deckt sich auch mit

- den **Einschätzungen des Bundeskriminalamts** und
- dem **Bundesamt für Sicherheit in der Informationstechnik** sowie
- der **Agentur der Europäischen Union für Cybersicherheit**.

PKS und Dunkelfeld

Nach der Polizeilichen Kriminalstatistik wurden in Bayern im zurückliegenden Berichtszeitraum **über 48.000 Fälle von Cybercrime** zur Anzeige gebracht. Dabei spiegelt diese Zahl **nur das Hellfeld** wider – die **tatsächliche Anzahl** von Straftaten im Bereich Cybercrime ist vermutlich noch **um ein Vielfaches höher**.

Verschiebung der Motivlagen

Zudem zeigte sich im Vergleich zu den Vorjahren eine **deutliche Professionalisierung der Tätergruppen**. Zugleich haben sich die **Motivlagen verschoben:** Neben **finanziellen Interessen** waren vermehrt auch mutmaßlich **politisch motivierte**

Cyberangriffe festzustellen. Vor dem **Hintergrund des aktuellen politischen Weltgeschehens ist das** nur eine logische Konsequenz.

DDos-Angriffe

In diesem Zusammenhang kamen etwa die **Überlastungsangriffe**, sogenannten **Distributed-Denial-of-Service** *(DDoS)***-Attacken**, zum Einsatz. Neben Cyberkriminellen setzen auch **fremde Nachrichtendienste** und **staatlich gesteuerte Akteure** diese zunehmend als Mittel zur **politischen Einflussnahme** ein.

Einschlägige Gruppen riefen wiederholt **über soziale Medien** zu **Cyberangriffen** auf **Unterstützerstaaten der Ukraine** auf. In der Folge kam es global zu einer **Vielzahl von Überlastungsangriffen** *(DDoS)*, von denen **auch Einrichtungen in Bayern** betroffen waren. Dank etablierter Schutzmechanismen blieben diese **Angriffe bislang ohne** nachhaltige **Wirkung**.

Desinformations-kampagnen

Eine **weitere wichtige Erkenntnis** ist: **Desinformationskampagnen** haben sich seit Beginn des russischen Angriffskriegs gegen die Ukraine 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.

Mit den **Entwicklungssprüngen in der Künstlichen Intelligenz** *(KI)* gehen **enorme Chancen** einher, aber auch das **erhöhte Riskio** einer missbräuchlichen Verwendung. Cyber-Akteure sind durch den Einsatz von KI in der Lage, **mit nur geringen IT-Kenntnissen** ausgefeilte, meist mehrstufige **Angriffe** zu entwickeln. Damit lassen sich schlimmstenfalls auch **robuste technische Sicherheitsmaßnahmen überwinden**.

Ransomware als dominierendes Phänomen

Wir verzeichnen auch nach wie vor zahlreiche **Cyberangriffe mittels Ransomware**, also einer Schadsoftware zur Verschlüsselung von Daten zur Lösegelderpressung, die zu erheblichen **finanziellen Belastungen bei** den Betroffenen – sowohl Firmen als auch Privatpersonen – führen. **Lösegeldforderungen** bewegen sich häufig **im sechs- bis siebenstelligen Bereich**. Daneben schlagen bei Firmen **Produktionsausfälle**, **Datenverluste** und **Wiederherstellungsmaßnahmen** zusätzlich zu Buche.

Maßnahmen

Gegen diese vielfältigen Herausforderungen im Cyberraum haben wir uns bestmöglich gewappnet und die **Rahmenbedingungen** für unsere Cybersicherheitsbehörden **auf allen Ebenen bedarfsgerecht ausgebaut** und **internationale Kooperationen** weiter verstärkt.

Unter anderem wurde bei der Polizei ein **flächendeckendes Netzwerk hochspezi-**

alisierter Fachkommissariate und -dezernate eingerichtet. Sie übernehmen die Ermittlungen bei Cyberangriffen und stehen den Bürgerinnen und Bürgern, Unternehmen, Behörden und Organisationen in Bayern kompetent zur Seite.

Sogenannte „**Quick-Reaction-Teams**“ *(QRT)* **stehen rund um die Uhr an sieben Tagen der Woche zur Verfügung** und können bei Cyber-Angriffen gegen Unternehmen und Organisationen im Freistaat unverzüglich die erforderlichen Maßnahmen vor Ort initiieren.

Prävention

Auch **Prävention** ist natürlich ein wichtiger Baustein, um **Sicherheitsrisiken** im Cyberraum zu **minimieren**. **Polizei**, **Justiz** und **Verfassungsschutz** haben ihre umfangreichen, aufeinander abgestimmten **Präventionsangebote** für den Bereich **Wirtschaft und Gesellschaft** auf Grundlage der Lageerkenntnisse fortlaufend **weiterentwickelt**.

Neben diesen **strukturellen und präventiven Maßnahmen** sind auch der ständige **Auf- und Ausbau von Fachkompetenzen** und die **Etablierung innovativer Ermittlungsmethoden** bei den Sicherheitsbehörden wichtige Elemente der bayerischen Cybersicherheitspolitik.

Erfolge der Sicherheitsbehörden

Und sie zeigen Wirkung: Bayerische Sicherheitsbehörden konnten auch im vergangenen Jahr wieder **bedeutende Erfolge** bei der **Bekämpfung** von **Cyberkriminalität**, **Cyberspionage und -sabotage** erzielen. So konnte eine der bekanntesten internationalen **Ransomware-Gruppierungen**, „**8Base**“, **zerschlagen** und ihre Webpräsenzen im Darknet stillgelegt werden. Allein in Deutschland fanden **mindestens 365 nachgewiesene Angriffe** durch die Gruppierung statt. Im Zuge der Ermittlungen gelang es, **insgesamt 240 Firmen aus 30 Ländern** vor einer Verschlüsselung **zu warnen**.

Außerdem konnte das **Landesamt für Verfassungsschutz** dank seiner **hohen technischen und fachlichen Expertise** eine breit angelegte Desinformationskampagne aufdecken. Damit wurde verhindert, dass sich durch **gefälschte Nachrichtenbeiträge** gezielt **pro-russische und antiwestliche Narrative** verbreiten.

Schlusswort/ Überleitung

Wir werden auch weiterhin die **Fähigkeiten unserer Sicherheitsbehörden zum Wohl unserer Bürgerinnen und Bürger weiterentwickeln**.

Ich darf nun das Wort an **Finanzminister Füracker** übergeben, der näher auf die **Herausforderungen und Maßnahmen** bei **staatlicher Informationstechnik** eingeht.