Herrmann, Füracker und Eisenreich stellen den Bericht zur Cybersicherheit in Bayern 2026 vor: Anhaltend hohe Bedrohungslage / Behörden und KRITIS verstärkt im Visier der Angreifer / Künstliche Intelligenz bei Cyberattacken immer wichtiger, …

31.8.2026 - | Bayerische Staatsregierung

Bayerns Innenminister Joachim Herrmann, Finanzminister Albert Füracker und Justizminister Georg Eisenreich haben heute den Bericht zur Cybersicherheit in Bayern 2026 vorgestellt. Demnach ist die Bedrohungslage im Cyberraum so vielschichtig wie nie zuvor und die Angriffsszenarien werden immer komplexer. Neben Wirtschaftsunternehmen gerieten im letzten Jahr immer häufiger Behörden und KRITIS-Einrichtungen ins Visier der zunehmend professionell agierenden Angreifer. Im Jahr 2025 wurden mehr als 49.400 Fälle von Cybercrime bei der Bayerischen Polizei angezeigt – die Dunkelziffer liegt vermutlich um ein Vielfaches höher. Innenminister Herrmann betonte: „Der Schutz unserer Bevölkerung, der Wirtschaft und unseres Staates vor Cyberkriminalität muss besondere Priorität haben. Durch die konsequente Nutzung aller zur Verfügung stehenden Lageinformationen, die regelmäßige und enge Zusammenarbeit aller Cybersicherheitsbehörden und das proaktive Management der Risiken sind wir für die Herausforderungen im Cyberraum gut aufgestellt."

Dem Cyberlagebericht zufolge wird Künstliche Intelligenz zu einem immer wichtigeren Werkzeug für Cyberattacken – sie ermöglicht es, niederschwellig und ohne großes Vorwissen Angriffe durchzuführen. Zudem wurde im letzten Jahr beobachtet, dass vermehrt politische Motive bei der Cyberkriminalität zu beobachten sind. „Sogenannte DDoS-Angriffe zur gezielten Unterbrechung von Webseiten haben erheblich zugenommen, sie werden immer häufiger auch von hacktivistischen Akteuren mit politischen Motiven eingesetzt. Politisch motivierte Cyberangriffe und Desinformationskampagnen gewinnen ebenfalls zunehmend an Bedeutung. Sie stellen für ausländische Nachrichtendienste ein effektives Mittel dar, um Informationen zu beschaffen, Einfluss zu nehmen oder Sabotage zu 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", so **Herrmann**. Darüber hinaus dominieren in Bayern weiterhin klassische Phänomene wie Phishing, insbesondere auch das sogenannte „Quishing", bei dem gefälschte QR-Codes zum Einsatz kommen, sowie Ransomwareangriffe durch etablierte Gruppen. Das Bayerische Landeskriminalamt registrierte 2025 einen Anstieg der Ransomwarefälle von 18 Prozent gegenüber 2024 (2025: 230 Fälle, 2024: 195 Fälle), die neben Unternehmen auch öffentliche Einrichtungen betroffen haben.

Finanzminister Albert Füracker betonte: „Die zunehmende Bedrohung im Bereich Cybersicherheit ist real und macht auch vor bayerischen Behörden nicht Halt. In 2025 hat das Landesamt für Sicherheit in der Informationstechnik – kurz LSI – insgesamt 105 DDoS-Angriffe auf staatliche Webseiten registriert. Im Cyber Defence Center des LSI wurden 2025 zudem rund 6.000 sicherheitsrelevante Vorfälle bearbeitet – das sind zehn Prozent mehr als noch im Vorjahr. Dank der

hervorragenden Expertise unserer IT-Experten am LSI sowie einer frühzeitigen Erkennung und schnellen Reaktion kam es in allen Fällen weder zu Schäden noch zu einem Datenabfluss. Das zeigt einmal mehr: Bayern ist hier sehr gut aufgestellt! Wir nehmen die Entwicklungen dennoch sehr ernst und agieren weiterhin bestmöglich. Im engen Schulterschluss mit den bayerischen Cybersicherheitsbehörden sowie auf Landes- und Bundesebene geben wir tagtäglich unser Bestes, damit unsere Behörden auch künftig sicher und handlungsfähig bleiben und das Vertrauen der Bürgerinnen und Bürger in den Staat unerschütterlich steht."

Justizminister Georg Eisenreich erklärte: „Der Kampf gegen Cybercrime ist eine zentrale Herausforderung unserer Zeit. Die bayerische Justiz hat mit der Zentralstelle Cybercrime Bayern (ZCB) bereits vor elf Jahren eine schlagkräftige Einheit geschaffen, die weltweit mit wichtigen Akteuren kooperiert. Daneben ist Bayern auch rechtspolitisch aktiv. Die Justizministerkonferenz hat bereits im vergangenen Jahr auf Initiative des Freistaats einen besseren strafrechtlichen Schutz gegen hybride Bedrohungen gefordert. Bei Cyberdelikten setzt sich Bayern zudem für eine Anhebung der Strafrahmen ein, damit Cyber-Straftäter eine adäquate Antwort des Rechtsstaates erhalten."

Aus den Erkenntnissen aus dem Cyberlagebericht entwickeln Polizei, Justiz und Verfassungsschutz ihre Präventionsangebote für den Bereich Wirtschaft und Gesellschaft kontinuierlich weiter. So bietet beispielsweise die Zentrale Ansprechstelle Cybercrime (ZAC) des Bayerischen Landeskriminalamtes vielfältige Beratungsangebote für Unternehmen und Organisationen an, um sich gegen Cyberangriffe zu wappnen. Auch der fortlaufende Auf- und Ausbau von Fachkompetenzen und die Etablierung innovativer Ermittlungsmethoden, wie etwa KI-Tools zur Auswertung umfassenden Bild- und Videomaterials, bei den Sicherheitsbehörden sind wichtige Bestandteile der bayerischen Cybersicherheitspolitik.

Die bayerischen Sicherheitsbehörden gehen konsequent gegen Cyberkriminalität vor und konnten auch 2025 wieder zahlreiche Erfolge erzielen. So wurden etwa bei einer koordinierten Aktion von Strafverfolgungsbehörden aus 14 Ländern vier Anführer der Ransomware-Gruppe „8Base", dem größten Vertriebspartner der Gruppierung „Phobos", festgenommen. Im Rahmen der internationalen „Operation Stream" gegen die weltweite Verbreitung kinderpornografischer Inhalte konnten darüber hinaus mehr als 1.600 Tatverdächtige festgestellt und rund 80 Festnahmen vollzogen werden. Bei dieser groß angelegten internationalen Operation arbeiteten Polizei und Staatsanwaltschaft in Bayern eng mit Europol und 38 beteiligten Staaten zusammen.

Der Freistaat Bayern hat mit dem Landesamt für Sicherheit in der Informationstechnik bereits 2017 als erstes Bundesland eine eigenständige Behörde für IT-Sicherheit gegründet. Das Cyber Defence Center des LSI analysiert täglich rund 2,7 Milliarden Datensätze und blockierte 2025 zusammen mit dem IT-Dienstleistungszentrum (IT-DLZ) bereits beim Empfang rund 838 Millionen verdächtige E-Mails. Da Cyberangriffe zunehmend schneller und komplexer werden, entwickelt das LSI seine Abwehrmechanismen kontinuierlich weiter. Zudem setzt das LSI bereits erfolgreich KI-gestützte Analysen ein, um neue Schadsoftware schnell zu erkennen. Auch sein Beratungsangebot für staatliche und kommunale Behörden baut das LSI kontinuierlich aus, beispielsweise wurde 2025 das Siegel „Kommunale IT-Sicherheit" in der Version 4.0 weiterentwickelt.

Im Rahmen der „Cyberabwehr Bayern" arbeiten die bayerischen Cybersicherheitsbehörden bereits seit sechs Jahren eng und vertrauensvoll zusammen. Diese Kooperation werden die Behörden auch weiter fortsetzen, um die Resilienz gegen Cyberangriffe in Staat, Wirtschaft und Gesellschaft weiter auszubauen.

https://www.bayern.de/herrmann-fueracker-und-eisenreich-stellen-den-bericht-zur-cybersicherheit-in-bayern-2026-vor-anhaltend-hohe-bedrohungslage-behoerden-und-kritis-verstaerkt-im-visier-der-

angreifer-kuenstliche-int