Bayerischer Landtag

19. Wahlperiode 02.07.2025 **Drucksache 19/7357**

Antrag

der Abgeordneten **Katharina Schulze, Johannes Becher, Benjamin Adjei, Stephanie Schuhknecht, Barbara Fuchs, Dr. Markus Büchler, Patrick Friedl, Mia Goller, Christian Hierneis, Paul Knoblach, Jürgen Mistol, Ursula Sowa, Martin Stümpfig, Laura Weber, Andreas Birzele, Cemal Bozoğlu, Maximilian Deisenhofer, Gülseren Demirel, Claudia Köhler, Tim Pargent, Toni Schuberl, Florian Siekmann** und **Fraktion (BÜNDNIS 90/DIE GRÜNEN)**

Sachverständigenanhörung über IT-Sicherheit in bayerischen Unternehmen

Der Landtag wolle beschließen:

Der Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung führt eine Sachverständigenanhörung zum Thema „IT-Sicherheit in der bayerischen Wirtschaft “ durch. Im Rahmen der Anhörung soll auf folgende Themenfelder eingegangen werden:

– aktueller Stand und Gefährdungslage

– Notfallunterstützung

– Prävention

In diesem Rahmen sollen insbesondere folgende Fragen von den Sachverständigen beantwortet werden:

1. aktuelle Bedrohungslage und Angriffsarten
   – Wie hat sich die Bedrohungslage für bayerische Unternehmen in den letzten Jahren entwickelt, insbesondere vor dem Hintergrund zunehmender globaler Cyberattacken und geopolitischer Spannungen?
   – Welche Angriffsarten (z. B. Ransomware, Phishing, verteilter Denial-of-Service-Angriff (DDoS) sind aktuell besonders relevant für Unternehmen in Bayern?
2. Stand der IT-Sicherheitsmaßnahmen
   – Wie ist der aktuelle Stand der IT-Sicherheitsmaßnahmen in bayerischen Unternehmen, insbesondere bei kleinen und mittleren Unternehmen (KMU)?
   – Welche typischen Schwachstellen und Defizite bestehen in der Praxis? Wo werden die größten Handlungsbedarfe gesehen?
3. Resilienz und Krisenmanagement
   – Wie gut sind bayerische Unternehmen auf größere Cybervorfälle vorbereitet? Gibt es Notfallpläne und regelmäßige Übungen?
   – Welche Rolle spielt die Zusammenarbeit mit Behörden wie dem Landesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Sicherheit in der Informationstechnik?
4. Wertschöpfung und Lieferketten
   – In welchem Maß sind Lieferketten bayerischer Unternehmen durch Cyberangriffe auf nationale und internationale Zulieferer gefährdet?
   – Wie können IT-Sicherheitsstandards entlang der gesamten Wertschöpfungskette etabliert und durchgesetzt werden?

- Welche Risiken ergeben sich durch die Abhängigkeit bayerischer Unternehmen von internationalen Cloud- und IT-Infrastrukturanbietern?
- Welche Maßnahmen könnten zur Stärkung der digitalen Souveränität und zur Förderung europäischer Alternativen beitragen?
- Wie kann ein durchgängiger Schutz von digitalisierten Wertschöpfungsstufen gewährleistet werden?

5. regulatorische Anforderungen und Umsetzung
   - Inwiefern sind bayerische Unternehmen auf die Umsetzung neuer gesetzlicher Vorgaben wie der NIS2-Richtlinie vorbereitet?
   - Wo bestehen aus Expertinnen- und Expertensicht Unterstützungsbedarfe bei der Einhaltung von IT-Sicherheitsstandards und Zertifizierungen?
6. wirtschaftliche Auswirkungen und Kosten
   - Welche wirtschaftlichen Schäden entstehen durch Cyberangriffe auf Unternehmen in Bayern?
   - Wie bewerten Sie die Kosten-Nutzen-Relation von Investitionen in IT-Sicherheit, insbesondere für KMU?
7. Sensibilisierung, Ausbildung und Fachkräftemangel
   - Wie ist der Stand der Sensibilisierung und Weiterbildung im Bereich IT-Sicherheit in Unternehmen?
   - Gibt es ausreichend qualifiziertes Personal, um die IT-Sicherheit zu gewährleisten? Wo sehen Sie Engpässe?
8. Zukunftsperspektiven und Innovation
   - Welche technologischen Trends (z. B. Künstliche Intelligenz, Cloud-Lösungen) beeinflussen die IT-Sicherheitslage aktuell und künftig?
   - Wie kann Bayern als Wirtschaftsstandort die digitale Souveränität stärken und Abhängigkeiten von internationalen IT-Anbietern verringern?
9. Empfehlungen für die Politik
   - Welche politischen Maßnahmen und Förderprogramme sind aus Expertinnen- und Expertensicht notwendig, um die IT-Sicherheit in bayerischen Unternehmen nachhaltig zu stärken?
   - Wie sollte die Zusammenarbeit zwischen Wirtschaft, Wissenschaft und Behörden weiterentwickelt werden, um die Resilienz gegenüber Cyberbedrohungen zu erhöhen?

Begründung:

Eine hohe und verlässliche IT-Sicherheit ist Standortfaktor, Wirtschaftswachstums- und Wettbewerbsfaktor sowie Sicherheitsfaktor zugleich. Die aktuelle Lage der IT-Sicherheit in bayerischen Unternehmen erfordert dringend eine vertiefte parlamentarische Befassung. Mehrere Entwicklungen – sowohl auf globaler als auch auf regionaler Ebene – machen eine Anhörung im zuständigen Ausschuss notwendig und geboten. Dazu gehören zunehmende Cyberangriffe im globalen und regionalen Kontext.

Cyberkriminalität zählt mittlerweile zu den größten Gefahren für Unternehmen in Bayern. Bereits fast ein Viertel der Unternehmen ist Opfer eines erheblichen Cyberangriffs geworden, wie aktuelle Umfragen und die Erfahrungen aus dem Cybersecurity Day 2025 in München zeigen (Cybersecurity Day 2025 in München – Bayerisches Landesportal). Die Angriffe werden immer komplexer und gefährlicher, nicht zuletzt durch den verstärkten Einsatz von Künstlicher Intelligenz durch Cyberkriminelle. Herkömmliche Schutzmechanismen reichen nicht mehr aus, um die aktuellen Bedrohungen abzuwehren.

Zusätzlich hat die globale politische Lage einen Einfluss auf die IT-Sicherheit. Die weltpolitische Lage ist angespannt: Geopolitische Konflikte, insbesondere zwischen Großmächten, führen zu einer Zunahme staatlich unterstützter oder motivierter Cyberangriffe. Staaten setzen Cyberattacken gezielt als Teil ihrer geopolitischen Strategien ein, etwa auf kritische Infrastrukturen oder Unternehmen. Prorussische Hackerkollektive haben jüngst gezielt Behörden in Bayern attackiert, wie der DDoS-Angriff auf mehrere Webseiten der Staatsregierung vor der Münchner Sicherheitskonferenz eindrücklich belegt (Prorussische Hacker bekennen sich zu Angriffen auf Behörden | BR24). Solche Vorfälle verdeutlichen die Verwundbarkeit auch regionaler Strukturen in einem globalisierten digitalen Raum.

Steigende regulatorische Anforderungen, zum Beispiel neue gesetzliche Vorgaben wie die NIS2-Richtlinie der EU sowie nationale Umsetzungen erhöhen den Druck auf Unternehmen, ihre IT-Sicherheit zu stärken und ihre digitale Resilienz nachzuweisen. Besonders KMU sind häufig nicht ausreichend vorbereitet und benötigen gezielte Unterstützung, um den steigenden Anforderungen und Bedrohungen gerecht zu werden.

Die wirtschaftliche und gesellschaftliche Bedeutung von IT-Sicherheit darf nicht unbeleuchtet bleiben: Cyberangriffe verursachen nicht nur direkte wirtschaftliche Schäden, sondern gefährden auch die Wettbewerbsfähigkeit, Innovationskraft und das Vertrauen in den bayerischen Wirtschaftsstandort. Die fortschreitende Digitalisierung aller Wirtschaftsbereiche verstärkt diese Risiken zusätzlich.

Digitalsouveränität, welches auch als Ziel der neuen Bundesregierung festgehalten wird, ist ein weiterer Aspekt von IT-Sicherheit und Resilienz. Die Abhängigkeit von internationalen IT-Lösungen und die mangelnde digitale Souveränität Europas, insbesondere im Hinblick auf die aktuelle US-Politik, machen eine eigenständige Stärkung der IT-Sicherheitsstrukturen in Bayern und Deutschland umso dringlicher.

Die Verschärfung der globalen politischen Lage, die Zunahme und Professionalisierung von Cyberangriffen sowie die wachsenden regulatorischen Anforderungen machen eine umfassende Bestandsaufnahme und Diskussion zur IT-Sicherheit in bayerischen Unternehmen unabdingbar. Eine Anhörung im Ausschuss bietet die Möglichkeit, Expertenwissen zu bündeln, Handlungsbedarfe zu identifizieren und gezielte politische Maßnahmen zum Schutz und zur Stärkung der bayerischen Wirtschaft zu entwickeln. Antworten auf die genannten Fragen decken die wichtigsten Handlungsfelder ab, sensibilisieren Entscheidungsträgerinnen und Entscheidungsträger im Landtag für die Thematik und ermöglichen eine umfassende Bewertung der IT-Sicherheitslage sowie der notwendigen politischen und praktischen Schritte zur Stärkung der digitalen Resilienz in Bayern.