



Sie befinden sich hier: [Startseite](#) > [Presse](#) > **Pressemitteilungen**

Pressemitteilungen

Cybersecurity Day 2025 in München

29. Januar 2025

+++ Cyberkriminalität hat sich zu einer der größten Gefahren für Unternehmen entwickelt. Bayern will insbesondere kleinere und mittlere Unternehmen dabei unterstützen, sich bestmöglich vor Cyberangriffen zu schützen und vorbereitet zu sein. Das bayerische Innen- sowie Justizministerium, luden deshalb heute gemeinsam mit der IHK für München und Oberbayern zum Cybersecurity Day 2025 in München ein. Das Motto: ‚Gelebte Cybersicherheit im Unternehmen – Strategie, Technik und Mensch‘. +++

Beim Cybersecurity Day informierten zahlreiche Expertinnen und Experten aus Wissenschaft, Wirtschaft, Polizei, Justiz, Verfassungsschutz, aus dem Bereich des Datenschutzes, dem Landesamt für Sicherheit in der Informationstechnik sowie dem Bundesamt für Sicherheit in der Informationstechnik über mögliche Maßnahmen und Unterstützungsangebote gegen Cyberkriminalität.

In einer Reihe von Gesprächen diskutierten die Vertreter der bayerischen Staatsregierung mit Expertinnen und Experten aus Wirtschaft und Wissenschaft über verschiedene Aspekte der Cybersicherheit. Innenstaatssekretär Sandro [Kirchner](#) merkte dazu an: „Unzureichende Sicherheitsvorkehrungen können fatale Folgen haben. Ein wirksamer Schutz gegen Cyberangriffe und eine starke Cyberresilienz in Unternehmen müssen für Entscheidungsträger deshalb oberste Priorität haben. Zum besseren Schutz vor Cyberangriffen bauen Polizei, Verfassungsschutz und Datenschutz ihre Beratungsangebote für die Wirtschaft kontinuierlich aus. Im Ernstfall ist durch unsere „Quick Reaction Teams“ bei der Bayerischen Polizei die jederzeitige Reaktionsbereitschaft qualifizierter Einsatzkräfte gewährleistet. Aber auch eine vertrauensvolle Zusammenarbeit von Sicherheitsbehörden und Wirtschaft ist unerlässlich. Nur gemeinsam können wir den Herausforderungen der Zukunft entgegentreten.“

Bayerns Justizminister [Eisenreich](#): „Zwischen August 2023 und August 2024 ist der Schaden durch Cyberattacken für die deutsche Wirtschaft laut Bitkom auf einen neuen Rekordwert von etwa 179 Milliarden Euro angestiegen, etwa 30 Milliarden mehr als im Vorjahreszeitraum. Wir wollen heute dafür sensibilisieren, dass jedes Unternehmen zur Zielscheibe werden kann. Auch kleinere und mittlere Unternehmen sind gefährdet und müssen sich vor Cyberangriffen schützen. Die Angriffe können im Extremfall ganze Existenzen vernichten.“

IHK-Vize-Präsidentin Prof. Dagmar M. [Schuller](#) betonte, dass die Unternehmen angesichts der großen Bedrohungslage noch mehr Sicherheitsmaßnahmen ergreifen müssen. „Noch immer haben erst weniger als die Hälfte der Firmen einen Notfallplan zum Umgang mit erfolgreichen Cyberangriffen. Besonders bei kleinen Unternehmen zeigen sich viele Lücken in der Prävention“, zitiert die IHK-Vize-Präsidentin die aktuelle IHK-Digitalisierungsumfrage. Andererseits nehmen Unternehmen ihre Mitarbeitenden mittlerweile etwas mehr in den Fokus: 64 Prozent führen IT-Sicherheitsschulungen durch und fast drei Viertel haben Nutzungsrichtlinien festgelegt. Laut Umfrage ist bereits fast ein Viertel der Unternehmen Opfer eines erheblichen Cyberangriffs geworden, unterstreicht Schuller. „Eine erfolgreiche Cyberabwehr ist damit ein elementarer Standortfaktor und gemeinsame Aufgabe von Wirtschaft und Staat“, so Schuller weiter.

Staatssekretär Martin Schöffel (Finanzen und Heimat) sprach mit Prof. Dr. Claudia Eckert, der Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit, über technische Aspekte. Schöffel: „Beim Schutz der staatlichen IT-Systeme ist der Freistaat dank der versierten IT-Experten am Landesamt für Sicherheit in der Informationstechnik (LSI) bestens aufgestellt! Neben technischen Aspekten gilt es, auch ein solides Sicherheitsbewusstsein zu schaffen, um die IT-Sicherheit nachhaltig zu stärken! Das LSI hat dafür ein neues Beratungsangebot geschaffen, das vor allem kleine und mittelständische Unternehmen im KRITIS-Bereich und Kommunen bei der Umsetzung der NIS-2-Richtlinie unterstützen und somit zur Steigerung der IT-Sicherheit in ganz Bayern beitragen soll.“

Justizminister Eisenreich tauschte sich mit Johannes Hackstette, Head of Digital Enablement bei Siemens Energy über die Schlüsselrolle von Mitarbeiterinnen und Mitarbeitern bei der Cybersicherheit aus. Der Minister: „Ein unbedachter Klick eines Mitarbeiters oder einer Mitarbeiterin kann zu einem schweren Sicherheitsvorfall führen, der das Unternehmen am Ende Millionen kostet. Die bayerische Justiz setzt im Kampf gegen Cybercrime innovative Ermittlungswerkzeuge ein. Doch das wirksamste Mittel sind und bleiben wachsame Mitarbeiterinnen und Mitarbeiter.“

Hintergrund:

Bayern hat seine Strukturen für eine moderne Strafverfolgung im Cyberraum kontinuierlich verstärkt.

- Bereits vor zehn Jahren gründete die Justiz Bayern die in Bamberg angesiedelte Zentralstelle Cybercrime Bayern (ZCB). Ermittlungsschwerpunkte der ZCB liegen u. a. im Kampf gegen sexuellen Missbrauch von Kindern und Kinderpornografie, in der strafrechtlichen Verfolgung von Cyberangriffen sowie im Kampf gegen illegales Cybertrading (Betrug mit angeblich lukrativen, tatsächlich aber nicht existenten Finanzinstrumenten) und gegen den Handel mit verbotenen Waren auf Internet-Plattformen.
- Bei der ZCB werden alle Verfahren zu Cyberattacken auf Unternehmen mit Sitz in Bayern gebündelt, insbesondere die sogenannten Ransomware-Fälle.
- Die ZCB setzt innovative Werkzeuge wie den „BigPhish“, ein Tool, das frühzeitig neu-registrierte Phishing-Domains im Internet aufspüren soll, ein.
- Die ZCB fungiert zudem als zentrale Ansprechstelle für alle bayerischen Staatsanwaltschaften. Die Spezialermittler der ZCB unterstützen in technisch schwierigen Fällen die Staatsanwältinnen und Staatsanwälte in der Fläche. Bei allen 22 Staatsanwaltschaften und den drei Generalstaatsanwaltschaften in Bayern wurden IT-Sonderdezernate eingerichtet bzw. IT-Ansprechpartner bestellt.
- Zum 1. Oktober 2022 wurde bei der ZCB eine Taskforce „Cyberangriffe auf Unternehmen und Einrichtungen“ eingesetzt.
- Aktuell hat die bayerische Polizei mehr als 400 Spezialisten für die Bekämpfung von Cybercrime eingesetzt. Dabei handelt es sich um rund 300 speziell aus- und fortgebildete Ermittler, davon 200 ausgebildete IT-Kriminalisten, sowie um rund 100 IT-Forensiker, die durch Sicherung und Aufbereitung der digitalen Spuren die Ermittlungen unterstützen. Jede Kriminalpolizeiinspektion verfügt über eigene Kommissariate zur Verfolgung schwerwiegender Cybercrime-Delikte.
- Darüber hinaus werden bei jeder Polizeiinspektion sogenannte Schwerpunktsachbearbeiter für den Bereich Cybercrime eingesetzt.
- Zudem hat der Freistaat bei allen Landespolizeipräsidien und dem Landeskriminalamt sogenannte „Quick-Reaction-Teams“ eingerichtet, um schnellstmöglich am Einsatzort digitale Spuren zu sichern.

[Pressemitteilung auf der Seite des Herausgebers](#)

Inhalt

Datenschutz

Impressum

Barrierefreiheit

