



Sie befinden sich hier: [Startseite](#) > **Cybersecurity Day in München / Auch kleine und mittlere Unternehmen müssen sich vor Cyberkriminellen schützen / Gemeinsamer Aktionstag von Innen- und Justizministerium sowie der IHK für München und Oberbayern**

Cybersecurity Day in München / Auch kleine und mittlere Unternehmen müssen sich vor Cyberkriminellen schützen / Gemeinsamer Aktionstag von Innen- und Justizministerium sowie der IHK für München und Oberbayern

26. Januar 2023

Cyberangriffe auf deutsche Unternehmen häufen sich: Allein in den vergangenen zwei Jahren fügten Cyberkriminelle der deutschen Wirtschaft einen Gesamtschaden von jeweils mehr als 200 Milliarden Euro zu. **Bayerns Innenminister Joachim Herrmann, Justizminister Georg Eisenreich** und der **IHK-Präsident für München und Oberbayern, Prof. Klaus Josef Lutz**, luden deshalb heute (26. Januar) zum **Cybersecurity Day** in München ein.

Motto: „**Bayerische Unternehmen sicher im Netz**„. Bayerns **Justizminister Eisenreich**: „Jedes Unternehmen kann zur Zielscheibe von Hackern werden. Auch kleine und mittlere Unternehmen sind gefährdet und müssen sich vor Cyberkriminellen schützen. Die Angriffe aus dem Netz können im Extremfall ganze Existenzen vernichten. Mit dem Cybersecurity Day wollen wir für das Thema sensibilisieren und kleine und mittlere Unternehmen dabei unterstützen, sich besser gegen Angriffe aus dem Internet zu rüsten.“

Innenminister Herrmann betonte: „Cybersicherheit wird ein immer wichtigerer Wettbewerbsvorteil für die Wirtschafts- und Innovationskraft bayerischer Unternehmen. Denn mit der zunehmenden Vernetzung steigt auch die digitale Verwundbarkeit. Ausgefeilte Cyberangriffe, Cyberspionage und Cybersabotage sowie zunehmend auch Desinformation verursachen Milliarden Schäden und bedrohen letztlich auch unsere Demokratie. Der wirksame Schutz gegen Cyberangriffe sowie die Stärkung der Cyberresilienz müssen daher oberste Priorität haben.“

IHK-Präsident Lutz: „Besonders kleine und mittlere Unternehmen brauchen noch viel mehr Aufklärung und Unterstützung, um sich vor Cyberangriffen zu schützen und für den Fall der Fälle gut vorbereitet zu sein. Im schlimmsten Fall steht die Existenz auf dem Spiel. Nur eine entschlossene Prävention kann das immense Potenzial für Schäden durch Cyber-Angriffe verringern. IT-Sicherheit muss noch viel mehr zur Chefsache werden.“

Als führender Industrie- und Forschungsstandort bietet der Freistaat mit seinen leistungsstarken Unternehmen besonders attraktive Angriffsziele.

Eisenreich: „Durch den völkerrechtswidrigen Angriffskrieg Russlands auf die Ukraine hat das Thema eine neue Aktualität erfahren. Cyberangriffe bedrohen in zunehmendem Umfang die Sicherheit von Unternehmen, Behörden und kritischer Infrastruktur, zum Beispiel durch Hackerangriffe, Erpressungsversuche oder kriminelle Zugriffe auf Daten. Ich habe daher im vergangenen Oktober bei

der Zentralstelle Cybercrime Bayern eine Taskforce für Cyberangriffe auf Unternehmen und Einrichtungen eingerichtet. Zudem fungiert dessen Leiter, Oberstaatsanwalt Christian Schorr, als persönlicher Ansprechpartner für Unternehmerinnen und Unternehmer.“ **Herrmann:** „Zum besseren Schutz und zur Stärkung der Abwehrfähigkeit gegen Cyberangriffe stellt der Freistaat zahlreiche Angebote zur Verfügung. Hierzu gehören neben vielzähligen präventiven Beratungsangeboten die ‚Hotline für IT-Notfälle‘ beim bayerischen Landeskriminalamt oder ganz neu auch ein sogenannter Chatbot, der seit Ende September 2022 auf den Seiten der Bayerischen Polizei rund um die Uhr Antworten auf die wichtigsten Fragen zur Cybercrime geben soll. Zudem ist das Landesamt für Verfassungsschutz ein wichtiger und vertraulicher Ansprechpartner, wenn es um Cyberangriffe mit mutmaßlich nachrichtendienstlichem Hintergrund geht.“

Beim Cybersecurity Day informierten zahlreiche Experten aus Wissenschaft, Wirtschaft, Polizei, Verfassungsschutz, Justiz und Datenschutzaufsicht in Vorträgen und Workshops über die aktuelle Bedrohungslage und die möglichen Maßnahmen und Unterstützungsangebote gegen Hacker, Erpresser und Spione. Unter anderem schilderte **Dr. Patric Spethmann, der für Cybersicherheit zuständige Vorstand bei Marc O’Polo**, die Erfahrungen mit einem Cyberangriff auf das Stephanskirchner Modeunternehmen. **Oberstaatsanwalt Christian Schorr** von der **Zentralstelle Cybercrime Bayern** beleuchtete das Thema Cybersicherheit aus der Sicht eines Strafverfolgers. Die **Kriminalhauptkommissare Andreas Nath und Andreas Brosche** von der **Zentralen Ansprechstelle Cybercrime** präsentierten ein interaktives Planspiel zum Thema Ransomware. **Elisabeth Greiner vom Cyber-Allianz-Zentrum Bayern (CAZ)** und der **Vizepräsident des Bayerischen Landesamtes für Datenschutzaufsicht Andreas Sachs** informierten über wirksame Strategien zum Schutz vor Kriminalität und Spionage.

Justizminister Eisenreich: „Potenzielle Täter müssen eine adäquate Antwort des Rechtsstaates erhalten. Dafür brauchen unsere Gerichte und Staatsanwälte moderne Gesetze, die in Berlin gemacht werden müssen.“ Viele Tatbestände im Bereich Cyberkriminalität stammen noch aus den 80er Jahren und liegen mit Freiheitsstrafen von maximal drei Jahren im Bagatellbereich. Auch die Ermittlungsbefugnisse werden den Bedürfnissen unserer Ermittlerinnen und Ermittlern im digitalen Zeitalter nicht gerecht. **Eisenreich:** „Ich werde mich weiter dafür einsetzen, das Strafrecht an die aktuellen Herausforderungen anzupassen.“

Hintergrund:

- Bayern hat 2015 mit der Gründung der Zentralstelle Cybercrime Bayern (ZCB) die Strukturen für eine moderne Strafverfolgung auch im Cyberraum geschaffen. 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. Das Team der ZCB besteht aus 22 Spezialstaatsanwältinnen und Spezialstaatsanwälte sowie vier IT-Forensikerinnen und Forensikern.
- 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.
- Aktuell hat die bayerische Polizei mehr als 400 Spezialisten in der Bekämpfung von Cybercrime eingesetzt. Dabei handelt es sich um rund 300 speziell aus- und fortgebildete Ermittler, davon 196 ausgebildete IT-Kriminalisten, sowie um rund 100 IT-Forensiker, die durch Sicherung und Aufbereitung der digitalen Spuren die Ermittlungen unterstützen. Jede Kriminalpolizeiinspektion verfügt mittlerweile über eigene Kommissariate zur Verfolgung schwerwiegender Cybercrime-Delikte.
- Zudem hat der Freistaat bei allen Landespolizeipräsidien und dem Landeskriminalamt sogenannte „Quick-Reaction-Teams“ eingerichtet, um schnellstmöglich am Einsatzort digitale Spuren zu sichern.

