Bayerischer Landtag

19. Wahlperiode

Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung

37. Sitzung

Donnerstag, 27. November 2025, 10:19 bis 13:17 Uhr

Anhörung

„IT-Sicherheit in der bayerischen Wirtschaft“

Inhalt

Sachverständige

Holger Blumberg
Head of Group IT Architecture & Governance, KRONES AG

Thomas Boele
Director Engineering – Landesbehörden, Check Point Software Technologies GmbH

Bernd Geisler
Präsident des Landesamts für Sicherheit in der Informationstechnik (LSI) Bayern

Marc Luczak
Leiter Informationssicherheit, BMW Financial Services

Norbert Radmacher
Präsident des Bayerischen Landeskriminalamtes (LKA)

Josef Schinabeck
Vizepräsident des Bayerischen Landesamts für Verfassungsschutz (LFV)

Prof. Dagmar Schuller
Vizepräsidentin der Industrie- und Handelskammer (IHK) für München und Oberbayern

Prof. Dr. Haya Schulmann
Lehrstuhl des Institute of Computer Science an der Goethe Universität Frankfurt

Fragenkatalog

1. Aktuelle Bedrohungslage und Angriffsarten

   a) Wie hat sich die Bedrohungslage für bayerische Unternehmen in den letzten Jahren entwickelt, insbesondere vor dem Hintergrund zunehmender globaler Cyberattacken und geopolitischer Spannungen? Welche Branchen waren besonders betroffen?

   b) Welche Cyberangriffsarten (z. B. Ransomware, Phishing, verteilter Denial-of-Service Angriff (DDoS), Advanced Persistent Threats-Angriffe (ATPs)) oder Social Engineering sind aktuell besonders relevant für Unternehmen in Bayern?

   c) Wie können die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben die bayerischen Unternehmen bei der Abwehr und Bewältigung von Cyberangriffen unterstützen?

2. Stand der IT-Sicherheitsmaßnahmen

   a) Inwieweit ist der aktuelle Stand der IT-Sicherheitsmaßnahmen in bayerischen Unternehmen, insbesondere bei kleinen und mittleren Unternehmen (KMU) und im Bereich der kritischen Infrastruktur transparent?

   b) Welche typischen Schwachstellen und Defizite bestehen bei den Unternehmen? Wo werden die vordringlichen Handlungsbedarfe gesehen?

3. Resilienz und Krisenmanagement

   a) Wie gut sind bayerische Unternehmen auf größere Cybervorfälle vorbereitet? Gibt es beispielsweise Notfallpläne, Quick-Response-Teams (QRTs) und regelmäßige Übungen?

   b) Wie bewerten Sie die Notfallversorgung im Stromausfall (z. B. auch via Dieselgeneratoren) speziell bei Rechenzentren in Bayern?

   c) Welche Erfahrungen gibt es mit der Wiederherstellung nach erfolgreichen Angriffen (Recovery-Zeit, Datenverluste)?

   d) Liegen Erkenntnisse vor, inwieweit der kurzfristige Wegfall grundlegender digitaler Dienste von Drittstaatsanbietern wie Cloud-Diensten in den Notfallplänen/Business Continuity -Plänen der bayerischen Unternehmen durch geeignete Vorkehrungen berücksichtigt wird?

4. Lieferketten, digitale Resilienz und digitale Souveränität

   a) Wie können einheitliche IT-Sicherheitsstandards entlang der gesamten Wertschöpfungskette etabliert und durchgesetzt werden?

   b) Inwieweit bestehen Abhängigkeiten für bayerische Unternehmen von internationalen Cloud- und IT-Infrastrukturanbietern und ggf. welche Risiken ergeben sich hierdurch?

   c) Welche Maßnahmen könnten zur Stärkung der digitalen Souveränität und zur Förderung europäischer Alternativen beitragen?

5. Regulatorische Anforderungen und Umsetzung

   a) Welche gesetzlichen Vorgaben zur Einhaltung von IT-Sicherheit, insbesondere zu Standards und Zertifizierungen, bestehen für bayerische Unternehmen?

   b) Welche Herausforderungen bestehen für bayerische Unternehmen aus Expertinnen- und Expertensicht bei der Umsetzung? Wo bestehen ggf. Unterstützungsmöglichkeiten durch staatliche Stellen?

   c) Welche möglichen Nachteile ergeben sich für die Wettbewerbsfähigkeit bayerischer Unternehmen im Bereich IT- und Cybersicherheit durch nationale oder europäische Regulierung (z. B. zusätzliche Bürokratie)?

6. Wirtschaftliche Auswirkungen und Kosten

   a) Welche wirtschaftlichen Schäden entstehen durch Cyberangriffe auf Unternehmen in Bayern? Inwieweit kam es dadurch bisher zu spürbaren Einschränkungen der laufenden Produktion?

   b) Welche Dunkelziffer ist bei gemeldeten Schäden realistisch anzunehmen?

   c) Wie bewerten Sie die Kosten-Nutzen-Relation von Investitionen in IT-Sicherheit, insbesondere für KMU?

   d) In welchen wirtschaftlichen Nischen im Bereich Cybersicherheit haben bayerische IT-Unternehmen besondere Stärken oder Chancen in der internationalen Arbeitsteilung?

7. Sensibilisierung, Ausbildung und Fachkräftemangel

   a) Wie ist der Stand der Sensibilisierung und Weiterbildung im Bereich IT-Sicherheit in Unternehmen?

   b) Gibt es ausreichend qualifiziertes Personal, um die IT-Sicherheit in Unternehmen zu gewährleisten? Wo sehen Sie etwaige Engpässe und deren Ursachen?

   c) Wie kann die Aus- und Weiterbildung von IT-Sicherheitsfachkräften an bayerischen Hoch- und Berufsschulen verbessert werden?

8. Zukunftsperspektiven und Innovation

   a) Welche technologischen Trends (z. B. Künstliche Intelligenz, Cloud-Lösungen) beeinflussen die IT-Sicherheitslage aktuell und künftig?

   b) Wie kann Bayern als Wirtschaftsstandort die digitale Souveränität stärken und Abhängigkeiten von internationalen IT-Anbietern verringern?

9. Empfehlungen für die Politik

   a) Inwieweit kann die Politik bayerische Unternehmen dabei unterstützen, ihre IT-Sicherheit weiter zu stärken?

   b) Wie werden aktuell verfolgte Maßnahmen auf Bundes- und Landesebene dahingehend bewertet?

   c) Wo werden Potenziale gesehen, die Zusammenarbeit von Staat, Wirtschaft und Forschung zur Erhöhung der Resilienz gegen Cyberbedrohungen weiter zu verbessern?

Anlagen

(Beginn: 10:19 Uhr)

Vorsitzende Stephanie Schuhknecht (GRÜNE): Ich begrüße Sie herzlich zu unserer heutigen Anhörung. Wie immer wird die Anhörung per Livestream übertragen. Die Stenografen schreiben heute außerhalb des Saals mit, und damit das gut gelingt, bitte ich alle Redner, direkt in das Mikrofon zu sprechen. Das Protokoll zu dieser Anhörung wird später auf der Internetseite des Landtags veröffentlicht.

Eine Aufnahmegenehmigung für Presse, Funk, Fernsehen und Fotografen wird gemäß § 140 der Geschäftsordnung erteilt, sofern sich kein Widerspruch regt. – Das sehe ich nicht. Dann ist das so beschlossen.

Ich möchte noch darauf hinweisen, dass das Essen im Plenarsaal nicht zugelassen ist. Das sage ich einfach nur, damit das jeder gehört hat.

Entschuldigt für die heutige Sitzung ist Herr Dr. Stefan Ebner. Herr Josef Schmid wird von Herrn Joachim Konrad und Herr Walter Nussel von Herrn Martin Wagle vertreten. Kommt Gabi Schmidt auch in diese Runde dazu?

(Kerstin Schreyer (CSU): Nein. Die anderen kommen auch nicht. Sie waren nur im Ausschuss.)

– Okay. Dann wissen wir Bescheid. – Ich möchte jetzt herzlich unsere heutigen Sachverständigen begrüßen.

Herr Holger Blumberg, Head of Group IT Architecture & Governance, KRONES AG, Herr Thomas Boele, Direktor Engineering – Landesbehörden, Check Point Software Technologies GmbH, Herr Bernd Geisler, Präsident des Landesamts für Sicherheit in der Informationstechnik (LSI) Bayern, Herr Marc Luczak, Leiter Informationssicherheit, BMW Financial Services, Herr Norbert Radmacher, Präsident des Bayerischen Landeskriminalamtes, Herr Josef Schinabeck, Vizepräsident des Bayerischen Landesamts für Verfassungsschutz, Frau Prof. Dagmar Schuller, Vizepräsidentin der Industrie- und Handelskammer (IHK) für München und Oberbayern, und Frau Prof. Dr. Haya Schulmann, Lehrstuhl des Institute of Computer Science an der Goethe Universität Frankfurt, schön, dass Sie sich die Zeit genommen haben und uns heute Ihre Expertise zur Verfügung stellen. Das ist für uns sehr wertvoll.

Ich bin sehr gespannt auf die kommenden Stunden, die wir gemeinsam verbringen. Wie immer wird es so sein, dass Sie zu Beginn die Möglichkeit haben, eine Stellungnahme von fünf Minuten abzugeben. Dafür rufe ich Sie in der Reihenfolge des Alphabets auf. Bei der Einhaltung dieser fünf Minuten werde ich streng sein, weil wir sehr viele sind und uns sonst die Zeit schon zu Beginn davonläuft. Im Anschluss gibt es dann die Möglichkeit für die Kollegen, Fragen zu stellen, und wir werden versuchen, das in Blöcken gut abzuarbeiten.

Warum kommen wir heute zusammen? Ich glaube, jeder hat in der letzten Zeit bei sich im direkten Umfeld Cyberattacken mitbekommen und auch, welche Auswirkungen das auf den Betrieb von Unternehmen, von Institutionen hat und wie lange es teilweise dauert, bis man danach wieder voll arbeitsfähig ist. Bitkom hat erst in einer letzten Studie einen Betrag von ungefähr 200 Milliarden Euro Schadenssumme für Deutschland angegeben, was das alleine 2025 verursacht hat.

In der aktuellen geopolitischen Situation müssen wir damit rechnen – ich denke, das ist uns allen bewusst –, dass sich diese Attacken verstärken, weil es natürlich nicht nur Cyberkriminelle gibt, sondern auch diejenigen, die staatlich – sage ich jetzt einmal – im Auftrag handeln. Insofern freue ich mich, dass wir heute über den

aktuellen Stand, die Gefährdungslage in Bayern, aber auch über die möglichen Notfallunterstützungen und Präventionsmöglichkeiten sprechen werden.

Wir starten jetzt diesen Austausch, und ich erteile das Wort Herrn Blumberg für die KRONES AG das Wort. Bitte schön.

SV Holger Blumberg (KRONES AG): Vielen Dank. – KRONES hat mehr als 20.000 Arbeitsplätze um den ganzen Globus verteilt. Ich habe bei der KRONES AG in den letzten 14 Jahren die IT verantwortet. Heute bin ich aber noch in einer weiteren Rolle hier. Als Mitglied im Kreis der IT-Leiter des Arbeitgeberverbands bayme spreche ich als Vertreter meiner Kollegen und möchte auch diese Situation darstellen.

Wie ist die aktuelle Bedrohungslage? Unser Unternehmen wird permanent angegriffen. Wir haben permanent Angriffe und sind permanent dabei, uns zu verteidigen. Ich glaube, es ist auch keine Frage des Ob, sondern eine reine Frage des Wann und in welcher Dimension man angegriffen wird. Ich denke, die Kollegen werden dazu gleich noch Zahlen liefern. Es ist – das muss man ganz klar sagen – eine permanente Bedrohungslage. Zudem wird mit der entstehenden KI-Technologie die Kreativität und die Bedrohungslage größer. Es gibt versteckte Angriffe, und die Unterscheidung, ob man zum Beispiel eine Mail von einem Menschen oder von einer Maschine bekommt, wird immer schwieriger.

Wie ist der Stand der Sicherheitsmaßnahmen in Unternehmen? Unser Unternehmen mit mehr als 20.000 Arbeitsplätzen leistet sich 400 IT-Spezialisten. Wir haben ein dediziertes Team, um die IT zu schützen. In einem sogenannten Security Operations Center überwacht es 24/7 unsere IT. Das ist das, was sich ein großes Unternehmen, was wir uns – wir sind großer Mittelstand – leisten können.

Ich spreche jetzt aber auch einmal für meine Kollegen aus dem kleinen Mittelstand. Mein Beispiel ist ein mittelständisches Unternehmen aus der Oberpfalz mit 200 Mitarbeitern. Dort wird die IT von einem Mitarbeiter betreut. Dieser Mitarbeiter kann seine IT nicht 24/7 schützen. Er ist erst einmal dafür da, die IT im Unternehmen am Laufen zu halten, und er ist nicht in der Lage, diesen Standard zu leisten, wie ihn wir uns als ein größeres Unternehmen oder zum Beispiel BMW leisten kann. Hier besteht ein großer Handlungsbedarf, zu schauen, wie man das verbessert.

Ich möchte jetzt das Thema Resilienz und Lieferketten ansprechen. Wir alle sind abhängig von großen amerikanischen Unternehmen, was die Cloudplattformen anbelangt. Es gibt zwar Initiativen, miteinander Plattformen in Europa aufzubauen, aber wir müssen auch realistisch sein. Zum Beispiel gibt es für Maschinenbauunternehmen für spezielle Anwendungen – Konstruktionswerkzeuge, CAD-Systeme – eigentlich keine europäischen Anbieter. Vor allem gibt es auch für kleinere Systeme keine Anbieter. Das heißt, es besteht eine Abhängigkeit gerade von großen amerikanischen Unternehmen.

Wenn man über Sicherheitssoftware redet, würde ich sagen, dass man heute von zwei Ländern abhängig ist. Das eine Land sind die USA. Das andere Land ist Israel; es kommt auch sehr viel Sicherheitstechnologie aus Israel.

Sehr am Herzen liegt mir das Thema Regulatorik. Einerseits finde ich es gut, dass auf europäischer Ebene die NIS-2-Richtlinie erlassen wurde, die einen Standard definiert, wie man in einem Unternehmen IT-Sicherheit zu organisieren hat. Wenn ich mir andererseits aber anschaue, wie so etwas implementiert wird, dann ist das gerade für ein kleines Unternehmen eine große Herausforderung.

Ich komme wieder zurück zu meinem Kollegen, der eine One-Man-Show in seinem Unternehmen ist. Er muss sicherstellen und dokumentieren, dass er die IT entsprechend dieser Richtlinie erfüllt. Jetzt tut sich die Tür für eine ganze Menge Berater auf, die – das habe ich seinerzeit auch bei der Datenschutz-Grundverordnung gesehen – den kleinen Unternehmen natürlich helfen. Was passiert aber aus meiner Sicht? Das Geld geht eigentlich eher an zum Teil auch fadenscheinige Berater und in diesen Unternehmen noch nicht einmal mehr in die Technologie. Insofern halte ich die Regulatorik für diese kleinen Unternehmen für sehr kritisch, während große Unternehmen wie wir das stemmen können.

Noch etwas zur Regulatorik: Der Cyber Resilience Act – ein EU-Erlass, der uns verpflichtet, unsere Produkte in der Zukunft updatefähig und dokumentiert zu halten –, gibt uns im europäischen Markt sicherlich gute Standards vor. Wir als Unternehmen treffen aber im außereuropäischen Markt auf Wettbewerber aus Asien, die diese Standards nicht erfüllen müssen. Dadurch haben wir einen Wettbewerbsnachteil. Insofern müssen wir als Wirtschaftsstandort Europa überlegen, wenn wir eine Regulatorik haben, wo sie uns hilft und wo sie Wettbewerbsnachteile schafft.

Zusammenfassend: Ich würde mir speziell für kleinere Unternehmen weniger Regulatorik im Bereich NIS-2 und Cyber Resilience Act wünschen, weil ich glaube, dass das in die falsche Richtung geht. Es wird nicht mehr Sicherheit eingeführt, sondern es wird nur stärker dokumentiert, dass versucht wird, sicher zu sein.

Mein Wunsch an die Politik wäre, gerade den kleinen Unternehmen mit Förderungen und entsprechenden Programmen zu helfen. Wenn ein großes Unternehmen wie die KRONES oder ein noch größeres Unternehmen wie BMW Sicherheitstechnologie einkauft, werden Skaleneffekte genutzt. Wir bekommen, wenn ich zum Beispiel mit dem Unternehmen meines Nachbarn hier verhandele, ganz andere Rabatte als das kleine Unternehmen aus der Oberpfalz, das 50 Lizenzen kauft. Dieses Unternehmen bekommt das nicht und hat also auch beim Einkauf der Technologie große Nachteile.

Wir haben hier einen Handlungsbedarf, wie wir so etwas lösen. Mein Appell an Sie in der Politik ist deshalb, zu schauen, wie man das fördern kann und vielleicht auch Rahmenbedingungen schafft, damit gerade die kleinen Unternehmen in diesem Bereich besser unterstützt sind.

SV Thomas Boele (Check Point Software Technologies GmbH): Ich bin seit etwas über 30 Jahren im Business bei verschiedenen Unternehmen und bin jetzt bei der Check Point, also auf der Herstellerseite. Unser Unternehmen ist 32 Jahre alt. Das heißt, wir haben über diese Zeit schon einiges gesehen, was in diesen Bereichen passiert.

Ich nehme hier jetzt einmal das Delta zu meinem Vorredner. Wir sind uns sicherlich alle darüber im Klaren, dass die Bedrohungslage anhaltend hoch ist und täglich interessanter wird. Das Wort KI wurde erwähnt. Dort haben wir natürlich auch sehr starke Fortschritte. Das Thema ist, dass man Phishing-Mails nicht mehr sauber zu übersetzen braucht, weil das die KI für einen macht. Man kann auch relativ einfach vollkommen automatisierte Angriffe fahren, ohne sehr viel zu orchestrieren. Das macht es für die möglichen Opfer natürlich schwierig.

Es gibt die unterschiedlichsten Angriffsarten. Am teuersten sind in der Regel die Ransomwareangriffe. Dabei werden Daten verschlüsselt, und es wird ein Ransom, ein Lösegeld gefordert. Dann werden die Daten noch einmal zusätzlich verkauft und in anderen Bereichen genutzt. Das nennt sich Doubel oder Triple Extortion. Jeder hat sicherlich auch schon einmal den Begriff Quantencomputing gehört. Dabei geht es darum: Man holt sich Daten und entschlüsselt sie, sobald sie fertig

sind. Das heißt, man kann davon ausgehen, dass da in der Zukunft noch Dinge passieren werden.

In vielen Bereichen ist erwähnenswert, wie der Stand der Sicherheitsmaßnahmen ist. Bei Großunternehmen ist das – da kann ich mich meinem Vorredner anschließen – kein Thema. Dort sind die Budgets vorhanden. Dort kann man auch die Gehälter zahlen, die heute im Bereich Cybersecurity aufgerufen werden. Im öffentlichen Bereich wird das extrem schwierig, weil man in diesen Bereichen Gehaltsstrukturen hat, die man relativ schwierig verändern kann. Dort muss man mit beschränkten Ressourcen arbeiten, um das absichern zu können. Das ist sicherlich, ebenso wie in dem kleinen Bereich der KMUs oder Mittelständler, gefährlich.

Eine Antwort in diesem Bereich ist, sich einen starken Partner, einen Managed Security Service Provider zu suchen, um einfach auf eine zentralisierte Expertise zugreifen zu können und auch kleineren Unternehmen diese Möglichkeit zu erschließen. Wenn ein KMU seinen größten Schatz, seine Daten, verliert und vielleicht wochenlang nicht arbeiten kann, dann ist das relativ schnell mit einer Bankrotterklärung verbunden. Wir haben das schon in vielen Bereichen gesehen und schauen, dass wir die Leute entsprechend unterstützen können.

Es ist auch noch etwas anderes wichtig. Wir haben das Wort Regulierung gehört. Eine Überregulierung ist gefährlich und kann in vielen Bereichen Innovationen ersticken. Wir haben sicherlich einen AI Act hier. Auf der einen Seite ist es wichtig und vernünftig, sinnvoll damit umzugehen. Auf der anderen Seite gibt es Länder, denen es vollkommen egal ist, was passiert; sie entwickeln das weiter. Letztendlich erhöhen wir damit unsere Abhängigkeiten. Man sollte sich also sehr genau überlegen, wie man diese Gesetze fasst und entsprechend umsetzen kann.

Ein Weiteres ist, diese Dinge so zu bauen, dass sie flexibel sind, weil der technologische Fortschritt nicht aufzuhalten ist. In vielen Bereichen wurden Datensicherheitsgesetze in den Sechzigern erlassen und vielleicht in den Neunzigern angepasst. Stichwort "Briefgeheimnis, § 202 Strafgesetzbuch" – ein wichtiges Thema –: Hier ist das Problem, dass die meisten Angriffe nach wie vor über E-Mails kommen. Wenn man dort nicht hineinschauen kann, um zu beurteilen: "Ist das gefährlich?", weil man sonst das Briefgeheimnis verletzt, hat man eine Zeitbombe im Netzwerk.

Es ist wirklich wichtig, dass Sie als Gesetzgeber darüber nachdenken, wie man solche Sachen flexibel gestalten kann, um zum technologischen Fortschritt einen Gegenpol aufbauen und sagen zu können: "Okay, die Gegenseite schläft nicht, aber ich mache entsprechend weiter". Es ist auch mein innigster Wunsch an Sie, dass Sie dort offen sind.

Zum Thema "Resilienz und Krisenmanagement": Hier ist es wichtig, zu üben, damit man versteht, wie man eine K-Fall-Übung macht. Was passiert, wenn meine Systeme ausfallen? Wo bekomme ich Systeme her, mit denen ich arbeitsfähig werde? Wie kann ich dort arbeiten, wenn meine zentrale IT ausgefallen ist? Man kann sich Sachen überlegen, aber muss auch üben. Das ist dem ähnlich, wenn man früher in der Schule einen Feueralarm gemacht hat. Beim Militär ist es genauso. Wenn man nicht übt, weiß man nicht, was im K-Fall passiert. Gott bewahre, dass so etwas passiert, aber im IT-Sicherheitsbereich muss man dann auch wissen, was passiert und dort rangehen.

Des Weiteren hören wir – das ist ebenfalls wichtig – sehr oft den Begriff "digitale Souveränität". Die Definition dafür ist im einfachsten Fall: Ich möchte die Herrschaft über meine Daten haben.

Ein anderer Punkt ist – das ist natürlich auch ein Wunsch –, dass man darüber nachdenkt, wie man das Seed Funding für interessante Unternehmen hinbekommt. In den meisten Fällen gehen sie nach Kalifornien oder in andere Bereiche, weil es dort Geld gibt. Man sollte wirklich darüber nachdenken: "Wo sind meine Kronjuwelen, und wie kann man diese erste initiale Finanzierung aufbauen, um Kreativität weiterzubilden?" Denn die meisten interessanten Securityunternehmen, die es in Deutschland gibt, sind verkauft. Sie sind in England, in den USA oder in anderen Ländern.

Das eine, das sicherlich auch politisch gesteuert werden kann, ist also: Wo setze ich Fördermittel ein? Das andere ist: Wie sorgt man dafür, dass man einen vernünftigen Nachwuchs bekommt? Da sollte man sicherlich an den Schulen anfangen, denn hier ist in vielen Bereichen – das habe ich auch bei meiner Tochter gesehen –Technologiefeindlichkeit vorhanden.

Die Möglichkeiten heute sind mannigfaltig. Man kann alles tun, weil die Technologie verfügbar ist.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Herr Boele, die fünf Minuten sind vorbei, auch wenn Sie gerade ein neues Thema begonnen haben.

SV Thomas Boele (Check Point Software Technologies GmbH): Okay. Ich habe genannt, was wichtig ist, und ich habe auch meine Wünsche genannt.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Wir können sicher nachher zu dem Bildungsthema noch ausführlicher sprechen. – Als Nächster hat Herr Geisler das Wort. Bitte schön.

SV Bernd Geisler (LSI): Vielen Dank. – Ich darf heute als Präsident das Landesamt für Sicherheit in der Informationstechnik vertreten. Wir sind die IT-Sicherheitsbehörde des Freistaats Bayern, und ich möchte in meinem Eingangsstatement zunächst die Rolle des LSI einordnen, damit Sie für die nachfolgenden Fragen ein wenig einen Hintergrund haben, wofür wir zuständig und wofür wir eben nicht zuständig sind.

Das LSI kümmert sich mit derzeit rund 160 Mitarbeitern – diese Zahl hat mich durchaus überrascht – seit 2017 um den aktiven Schutz der staatlichen IT-Systeme, und wir unterstützen Kommunen und öffentliche Betreiber kritischer Infrastrukturen bei der Absicherung ihrer Systeme durch Beratung sowie weitere Angebote. Unsere Aufgaben sind in Artikel 42 ff. des Bayerischen Digitalgesetzes hinterlegt.

Insbesondere trägt das LSI dafür Sorge, dass die Sicherheit an den Schnittstellen des Bayerischen Behördennetzes zu anderen Netzen sichergestellt ist. Außerdem unterstützen wir sämtliche Stellen, die an das Behördennetz angeschlossen sind, bei der Erkennung und bei der Abwehr von Angriffen. Dazu entwickeln wir sicherheitstechnische Mindeststandards für alle an das Bayerische Behördennetz angeschlossenen Stellen und überprüfen die Einhaltung dieser Standards.

Eine Aufgabe des LSI ist auch, Informationen zu aktuellen Sicherheitsrisiken zu sammeln und relevante Stellen regelmäßig über die aktuelle Sicherheitslage zu informieren. Als Kontaktstelle zum BSI gehört es zu den Aufgaben des LSI, die zuständigen Aufsichtsbehörden bayerischer Betreiber kritischer Infrastrukturen über relevante Sicherheitsvorkommnisse zu informieren.

Das LSI kann staatliche und kommunale Stellen, Betreiber kritischer Infrastrukturen und weitere Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen in Fragen der IT-Sicherheit beraten und unterstützen. Die Polizei, die Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz können wir bei der

Wahrnehmung ihrer gesetzlichen Aufgaben technisch unterstützen, insbesondere bei der Durchführung von technischen Untersuchungen oder der Datenverarbeitung. Das LSI hat dabei keine Aufsichts- oder Kontrollbefugnisse für bayerische Unternehmen, sondern wir bieten eine kostenfreie Unterstützung auf Anfrage für Betreiber kritischer Infrastrukturen und Unternehmen mit mehrheitlich staatlicher Beteiligung an.

Betreiber kritischer Infrastrukturen haben unterhalb der jeweiligen im BSI-Gesetz definierten Schwellenwerte keine Melde- oder Berichtspflicht von IT-Sicherheitsvorfällen an das BSI und an uns. Deshalb liegt uns kein vollständiger Überblick über die aktuelle Sicherheitslandschaft bayerischer Unternehmen vor.

Das LSI erhält allerdings Kenntnis von Strukturen und Vorfällen in den Unternehmen in Bayern, die sich aktiv an das LSI wenden bzw. die Leistungen des LSI – Beratung etc. – in Anspruch nehmen. Zudem erhält das LSI Kenntnis von akuten noch anhaltenden Vorfällen mit einem möglichen Ausfall der kritischen Dienstleistung bei bayerischen Betreibern kritischer Infrastrukturen, die über den in der BSI-Kritisverordnung festgelegten jeweiligen Schwellenwerten liegen. – Damit habe ich vielleicht ein wenig Zeit hereingeholt.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Herzlichen Dank. – Vielen Dank auch für die Zeit, die Sie uns an dieser Stelle schenken. Wir werden Sie nachher aber sicher noch ausführlich befragen. Als Nächster hat Herr Luczak das Wort. Bitte schön.

SV Marc Luczak (BMW Financial Services): Sehr verehrte Frau Vorsitzende, sehr geehrte Abgeordnete, liebe Gäste! Ich möchte Sie heute aus der Perspektive der BMW Financial Services mitnehmen. Dort bin ich sei knapp fünf Jahren der Leiter für die Informationssicherheit.

Was ist im Moment die aktuelle Lage, und welche Gegenmaßnahmen sind getroffen? Wir haben verschiedene Angriffsvektoren im Bereich der IT-Sicherheit, IT-Bedrohungslage. Wenn man das einmal clustert, sind das grob drei Stück.

Eine Motivationsart ist monetär. Das ist der typische Erpressungstrojaner, also eine Schadsoftware. Da muss man tatsächlich – was man sich vor einigen Jahren nicht hätte träumen lassen – mit den Erpressern diskutieren, um gegebenenfalls einen Code wieder freizukaufen und so zum Beispiel einen Schaden in der Datenbank abzuwenden.

Dann gibt es die Motivationsart, die einen Informationsvorteil, also einen klaren Wettbewerbsvorteil beschaffen soll. Aus meiner Sicht ist das noch etwas gefährlicher. Hier handelt es sich auch um Trojaner, die aber versteckt auf Applikationen, auf Datenbanken liegen und dort bewusst Informationen und Daten abgreifen. Der Vorteil dabei ist klar; der Wettbewerber möchte sich bestimmte Informationen holen. Früher hätte man das Industriespionage genannt. Das ist heute nichts anderes.

Die dritte Motivationsart ist das reine Zerstören. Typisch sind hier die DDoS-Maßnahmen, die es gibt. Man will im Endeffekt Daten zerstören. Die Motivationslage dahinter ist eigentlich auch jedem klar.

Warum skizziere ich das? Alle diese Bedrohungslagen fügen sich zusammen in Gegenmaßnahmen.

Es ist eine Kombination an vielen Gegenmaßnahmen. Die Vorredner haben die Regulatorik angesprochen. Wir in der BMW Financial Services haben das ISMS

recht gut ausgebaut. Das ist ein Vorteil von großen Unternehmen. Wir haben an die 40 Maßnahmen implementiert. Das sind banale Dinge wie das USB-Port-Blocking, Data Loss Prevention. Wir haben E-Mail-Encryption, Access Management usw. Das alles sind Maßnahmen, die diese Bedrohungslagen abwehren oder zumindest aufklären sollen.

Die Regulatorik: Ja, ich bin ein Freund von Regulatorik, aber nicht von einer Überregulatorik. Schauen wir es uns einmal an. Wir haben die ISO 27001. Wir haben das TISAX. Wir haben den DORA als neue EU-Verordnung, den Resilience Act. Das alles ist wunderbar. Wir haben aber auch die intrinsische Motivation, unsere Schutzobjekte zu schützen.

Unsere Schutzobjekte sind im Endeffekt, wenn man das einmal clustert, Kundendaten, Konstruktionsdaten und das Financial Reporting. Das alles sind hochkritische Daten, die im Endeffekt geschützt werden müssen. Ob man dafür Regulatorik benötigt, möchte ich einmal dahingestellt lassen. Häufig ist das auch ein Dokumentationsaufwand.

Große Unternehmen: Ja, wir haben den großen Vorteil, dass wir ein Incident Response Team für die Cyberabwehr haben. Vor einigen Jahren haben wir auch ein zweites Rechenzentrum, eine sogenannte Co-Location in Aschheim gebaut, um eine gewisse Redundanz unserer kritischen Prozesse herzustellen. Das können wir uns nur deshalb leisten, weil wir über ein Budget verfügen und wir das Ganze mit großen Teams eben auch vom Vorstand aus priorisiert bekommen.

Es ist aber auch ein wenig dem Finanzprodukt geschuldet, denn Sie wissen: Ein Finanzprodukt hat immer etwas mit Vertrauen zu tun, und ein Reputationsschaden ist das Größte, was uns passieren könnte. Sprich: Wenn Kundendaten in großer Form verloren gingen, zöge das logischerweise einen Reputationsschaden nach sich.

Ich komme auf das Thema Zukunftsaussichten zu sprechen und möchte dazu meinen Chef Oliver Zipse, Vorsitzender des Vorstands der BMW AG, zitieren:

> "Wir haben ein klares Ziel, dass in absehbarer Zeit jeder unserer Prozesse von KI unterstützt wird."

Jawohl, ich teile dieses Ziel. Wer sich heute nicht mit KI beschäftigt, ist morgen abgehängt. Davon bin voll überzeugt. Dennoch muss man auch sehen: Das birgt Gefahren. Wir haben es bei meinen Vorrednern gehört: KI wird auch auf der anderen Seite eingesetzt. KI ist dafür da, dass man auch hochkomplexe und voluminös große Angriffe in der Cybersicherheit gewährleisten kann. Dementsprechend müssen wir die Abwehrmaßnahmen definieren.

KI: Natürlich, die Digitalisierung schafft Effizienzen in Prozessen, kann die Qualität von Prozessen steigern. Da bin ich völlig dabei. Die höheren Risiken dadurch darf man aber nicht außer Betracht lassen.

Wir haben das Thema Cloud, das ebenfalls angesprochen wurde. Viele große Unternehmen – wir sind auch in einem Verbund – sind cloudabhängig. Im Moment gibt es nur die zwei gängigen US-Cloudanbieter AWS und Azure. Das könnte in der, ich sage einmal, geopolitischen Lage jetzt irgendwann ein Problem werden, zumal man heute bestimmte Fragen – Wer hat den Zugriff auf die Daten in der Cloud? An wen werden sie weitergegeben? – nicht so eindeutig beantwortet bekommt. Daher: Es besteht eine gewisse Abhängigkeit von US-amerikanischen Anbietern. Dem stehe ich kritisch gegenüber.

Was ist unsere Empfehlung oder der Wunsch an die Politik? Es klang gerade an. Wir haben, wie alle Unternehmen, mit der Gewinnung von Nachwuchs zu kämpfen, und zwar mit der Gewinnung von Experten. Die IT-Sicherheit ist ein sehr komplexes Feld, und ich bin manchmal ein wenig verdutzt: Jeder hat eine gewisse Affinität – Social Media –, jeder nutzt heute ein Laptop, ein Handy. Wir müssen junge Leute dazu motivieren, an den Hochschulen IT, Informatik, Cybersicherheit bis hin zur Forensik zu studieren.

Das sind hoch spannende Themenfelder – zwar vielleicht nicht für jeden –, und wir müssen diese Studiengänge und die Aus- und Weiterbildung attraktiver machen. Dementsprechend können wir und gerade auch die kleinen und mittelständischen Unternehmen dann aus einem großen Fundus von Experten profitieren.

SV Norbert Radmacher (LKA): Frau Vorsitzende, werte Damen und Herren Abgeordnete! Ein herzliches grüß Gott und vielen Dank für die Möglichkeit, als Präsident des Landeskriminalamts heute zu diesem Thema sprechen zu dürfen. Als Zentralbehörde für die Kriminalitätsbekämpfung sind wir natürlich auch für die Bekämpfung von Cyberkriminalität zuständig. Das bedeutet für uns zum einen die repressive Dimension und zum anderen die Dimension der Prävention, die bei uns gelebt wird, die von den Kolleginnen und Kollegen wahrgenommen wird.

Die Zahl der Cyberangriffe – wir haben es schon gehört – ist auf einem hohen Niveau, und die Komplexität nimmt zu. Der verursachte Schaden ist enorm. Die IT-Sicherheit hat deshalb nicht nur eine technische, sondern auch eine wirtschaftspolitische und damit eine gesamtgesellschaftliche Dimension.

Wir brauchen in diesem Themenbereich ein verstärktes Sicherheitsbewusstsein, verlässliche rechtliche Rahmenbedingungen und organisatorische Maßnahmen sowie eine enge Zusammenarbeit zwischen den öffentlichen Behörden, der Politik und der Wirtschaft. Insofern begrüßen wir sehr, dass heute diese Anhörung stattfindet. Außerdem brauchen wir eine Sensibilisierung für die Sicherheitsrisiken, eine Förderung von Sicherheitstechnologien und eine Förderung der Vernetzung zwischen den Akteuren innerhalb der Sicherheitsarchitektur, um diesen Bedrohungen gemeinsam effektiv zu begegnen.

Das Ganze stellt einen entscheidenden Faktor für die bayerische Wirtschaft dar. Als Polizei ist uns das bewusst, und wir bieten eine sehr professionelle Partnerschaft an.

Cyberkriminalität ist eine der dynamischsten und komplexesten Bedrohungslagen für Unternehmen, Behörden und letztlich für die Bürgerinnen und Bürger in Bayern. Die Täter agieren professionell, international und arbeitsteilig. Besonders auffällig sind gezielte Angriffe auf informationstechnische Systeme und die darin enthaltenen Daten. Das wurde auch schon von den Vorrednern angesprochen.

Eines der beiden Phänomene, die uns am meisten beschäftigen, ist die digitale Erpressung durch Verschlüsselungssoftware, Ransomware. Es sind aber auch DDos-Attacken zu beobachten. Wir stellen fest, dass diese Angriffe nicht nur große Konzerne treffen, sondern sie treffen insbesondere kleine und mittlere Unternehmen, die oftmals über begrenzte Schutzressourcen verfügen. Gleichzeitig beobachten wir eine wachsende Überschneidung von Cybercrime, Wirtschaftsspionage und staatlich gesteuerter Einflussnahme. Dabei stellen wir fest, dass viele Unternehmen ein hohes Schutzniveau haben. Insgesamt ist die Landschaft aber heterogen.

Technische Lösungen alleine reichen oft nicht aus. Auch organisatorische Vorsorge, regelmäßige Schulungen und geübte Notfallprozesse sind wichtig. Aus unserer

Sicht zeigt sich: Zahlreiche erfolgreiche Angriffe hätten durch Präventionsmaßnahmen und oftmals durch einfache Maßnahmen wie konsequente Passwortsicherheit, Netztrennung oder Updates verhindert werden können. Wir müssen resilient werden, um die entsprechende Funktionsfähigkeit gewährleisten zu können. Wichtig dafür sind Tests, aber auch Krisenübungen, die wir Ihnen gerne als Partner anbieten.

Eine Botschaft möchte ich hier bewusst senden: Wir sind natürlich für die Repression zuständig. Wir sind aber auch präventiv Partner für die Wirtschaft.

Wir haben bei mir im Haus die sogenannte ZAC, die Zentrale Ansprechstelle Cybercrime. Sie tritt an Verbände, an Unternehmen heran und wird beratend präventiv tätig. Sie bietet dort Vorträge und Schulungen, aber zum Beispiel auch Planspiele an, um den Ernstfall konkret zu üben und zu schauen: Sind die organisatorischen Maßnahmen richtig, die ich vorgesehen habe?

Außerdem haben wir ihnen Fähigkeiten rund um die Uhr zur Verfügung gestellt. Wir haben in Bayern sogenannte QRTs – das sind Quick Reaction Teams, die über die ganze bayerische Fläche verteilt sind –, die ihnen bei einem akuten Angriff beratend und natürlich ermittelnd – das ist ja unsere originäre Aufgabe – zur Seite stehen. Für uns ist wichtig, diese QRT-Teams und die entsprechende Hotline, die zur Verfügung steht, weiter bekannt zu machen und für diese Einheiten zu werben, die 24/7 an 365 Tagen im Jahr im Ernstfall ausrücken, um die jeweiligen Unternehmen in der Erstlage zu unterstützen und dann auch die Ermittlungen erfolgreich führen.

Sie fragten nach Empfehlungen für Sie als Gesetzgeber, für die Politik. Dazu würde ich gerne fünf Themenbereiche benennen. Das ist die Stärkung der Prävention; ich hatte das bereits angesprochen. Wünschenswert für uns sind auch verbindliche Sicherheitsstandards und ein strukturierter Informationsaustausch. Außerdem müssen wir in Forschung und Innovation investieren. Sehr klug ist immer, insgesamt in das Personal und in den Sachhaushalt der bayerischen Polizei zu investieren.

Abschließend möchte ich sagen: Cybersicherheit ist eine Kernaufgabe unseres Bereichs, und wir bieten Ihnen an, hier ein professioneller Partner zu sein.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Herzlichen Dank. – Ich möchte jetzt die Besuchergruppe auf der Empore begrüßen, die auf Einladung der Kollegin Toso hier ist. Schön, dass Sie da sind. Sie haben vielleicht mitbekommen, dass wir heute ein etwas sperriges Thema haben; es geht um Cybersicherheit für bayerische Unternehmen. Das heißt aber nicht, dass das ein unwichtiges Thema ist, sondern es beschäftigt uns sehr stark, weil es auch große Schadenssummen verursacht. Insofern hoffe ich, dass Sie aus dieser Debatte etwas mit nach Hause nehmen können. – Jetzt hat Herr Schinabeck das Wort. Bitte schön.

SV Josef Schinabeck (LFV): Sehr geehrte Frau Vorsitzende, sehr geehrte Mitglieder des Ausschusses, sehr geehrte Damen und Herren! Vielen Dank für die Einladung und dafür, dass ich heute zum Thema IT-Sicherheit in der bayerischen Wirtschaft sprechen darf.

Ich möchte zunächst ein paar Sätze zum Bayerischen Landesamt für Verfassungsschutz sagen. Wir sind grundsätzlich unter anderem für die Beobachtung extremistischer Bestrebungen und für die Spionageabwehr zuständig. Folglich sind wir im Bereich Cyberabwehr nur dann zuständig, wenn die Angriffe von fremden Staaten ausgehen, also wenn Spionage- oder Sabotageaktivitäten anderer Länder dahinterstecken. Für rein kriminelle Aktivitäten oder eine Konkurrentenausspähung haben wir keine Zuständigkeit. Wir sind auch keine Strafverfolgungsbehörde und unterliegen nicht dem Legalitätsprinzip.

Das eröffnet uns die Möglichkeit, dass wir unseren Hinweisgebern absolute Vertraulichkeit zusichern, woran wir uns gebunden fühlen. Außerdem war das der Grund, warum unsere Einheit bei ihrer Gründung im Jahr 2013 nicht als Cyber-Abwehrzentrum, sondern als Cyber-Allianz-Zentrum benannt wurde; es war von Anfang an auf Kooperation mit den Wirtschaftsunternehmen ausgelegt. Mit der Errichtung dieses Cyber-Allianz-Zentrums sollte der Fokus in der Spionageabwehr auf den Cyberbereich gelegt werden, denn es war schon damals absehbar, dass sich Spionageaktivitäten zunehmend in den virtuellen Raum verlagern.

Um Wiederholungen zu vermeiden, möchte ich gerne ein paar Ausführungen zu 1. c) des Fragenkatalogs machen. Wie können die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben die bayerischen Unternehmen bei der Abwehr und Bewältigung von Cyberangriffen unterstützen?

Ein wesentlicher Baustein bei der Bekämpfung ausländischer Cyberspionageaktivitäten ist der gegenseitige Informationsaustausch sowohl im polizeilichen als auch im nachrichtendienstlichen Bereich. So können Unternehmen rechtzeitig gewarnt und Angriffe abgewehrt werden. Eine Strafverfolgung ist in diesem Bereich eher selten der Fall, weil die Haupttäter in aller Regel im Ausland sitzen und für die bayerische Justiz kaum greifbar sind.

Im Interesse einer bestmöglichen Abwehr von Cyberangriffen wurde mit Ministerratsbeschluss vom November 2019 eine neue zentrale Informations- und Koordinationsplattform für bayerische Behörden mit Cybersicherheitsaufgaben geschaffen, die sogenannte Cyberabwehr Bayern, kurz: CAB. Teilnehmer der CAB sind das Cyber-Allianz-Zentrum Bayern im Landesamt für Verfassungsschutz, die zentrale Ansprechstelle für Cybercrime im Landeskriminalamt, die Zentralstelle Cybercrime der Generalstaatsanwaltschaft in Bamberg, das Landesamt für Sicherheit in der Informationstechnik, das Landesamt für Datenschutzaufsicht und der Landesbeauftragte für den Datenschutz.

Die zentrale Aufgabe der Cyberabwehr Bayern ist ein enger und vor allem schneller Austausch zwischen den teilnehmenden Behörden in Bayern zu cyberrelevanten Informationen. Hierfür finden regelmäßige und anlassbezogene Lagebesprechungen statt. Die teilnehmenden Behörden werden so schnellstmöglich über relevante Sicherheitsvorfälle informiert und können rasch über erforderliche Maßnahmen entscheiden.

Die Informationen der Cyberabwehr Bayern werden regelmäßig in einem Lagebild zur Cybersicherheitslage Bayern gebündelt. Ein umfassendes behördenübergreifendes Cyberlagebild ist die Voraussetzung für die qualifizierte Bewertung der Cybersicherheitslage in Bayern und für die zielgerichtete Veranlassung angemessener Maßnahmen darauf. Zur Gewährleistung des Betriebs unterhält die Cyberabwehr Bayern ein Cyber-Lagezentrum. Dieses Cyber-Lagezentrum ist beim Bayerischen Landesamt für Verfassungsschutz angesiedelt.

Ein weiterer wesentlicher Baustein ist – das sagten auch bereits meine Vorredner – die Präventionsarbeit; der Schutz der bayerischen Wirtschaft und Wissenschaft ist Teil des gesetzlichen Auftrags des BayLfV im Bereich der Spionageabwehr. Der regelmäßige Kontakt mit Firmen, wissenschaftlichen Einrichtungen und Verbänden ist dabei ein wesentlicher Baustein des Cyber-Allianz-Zentrums als vertraulicher Ansprechpartner für Unternehmen und Forschungseinrichtungen.

Die Kontakte erfolgen zum einen anlassbezogen; das heißt, aufgrund von vorliegenden Informationen über konkrete Bedrohungen. Zum anderen erfolgen sie in allgemeiner Form durch Vorträge, Messebesuche oder der Organisation von Tagungen wie dem kürzlich von uns in München veranstalteten Wirtschaftsschutz-

tag mit rund 100 teilnehmenden Firmenvertretern. – Soweit meine Ausführungen. Danke schön.

SVe Prof. Dagmar Schuller (IHK): Sehr geehrte Frau Vorsitzende, sehr geehrte Mitglieder des Ausschusses, meine sehr verehrten Damen und Herren! Ich bin Vizepräsidentin der IHK für München und Oberbayern, Professorin für angewandte KI und Unternehmerin im Hightechbereich. Daher kann ich Ihnen aus der Praxis sehr viele Inputs und Informationen geben, wie die Lage bei kleineren und mittleren Unternehmen aussieht.

Die IHK München und Oberbayern vertritt rund 400.000 Unternehmen. Der überwiegende Teil davon ist eben klein und mittelständisch, und – wir haben es vorher schon von Herrn Blumberg und anderen Vorrednern gehört – diese kleinen und mittelständischen Unternehmen sind besonders gefordert, wenn es um das Thema Cybersicherheit und -angriffe geht. Wir beobachten hier sehr stark ein eher reaktives als präventives Verhalten. Das heißt, zuerst passiert erst einmal etwas, und danach kümmert man sich darum, wie man mit diesem Problem umgehen kann.

Wir haben jedes Jahr Digitalisierungsumfragen. Unsere letzte Digitalisierungsumfrage aus dem Jahr 2024 – die Digitalisierungsumfrage 2025 läuft gerade – zeigt, dass rund 23 % der bayerischen Unternehmen schon Opfer von mindestens einem relevanten Cyberangriff waren. Die Dunkelziffer ist vermutlich deutlich höher.

Standardmaßnahmen sind bereits auch in sehr vielen kleinen und mittelständischen Unternehmen etabliert. Schauen wir uns aber anhand der IT-Notfallpläne an, wie die Abgrenzung tatsächlich ist. Besonders bei Kleinunternehmen mit bis zu ungefähr 20 Mitarbeitern ist festzustellen, dass nur knapp ein Drittel über solche Pläne verfügt. Demgegenüber sind fast drei Viertel der Unternehmen mit mehr als 250 Mitarbeitern mit solchen Plänen ausgestattet. Das sind nur einige Zahlen, um Ihnen das etwas zu verdeutlichen.

Seitens der IHK arbeiten wir mit Webinaren und Positionspapieren sehr stark daran, präventiv Maßnahmen zu unterstützen und zu informieren. Präventive Maßnahmen bedeuten aber auch, sich ausprobieren und Experimente machen zu können.

Wir haben auch das von den Vorrednern schon gehört: Wir haben Unterstützungsangebote im bayerischen Bereich durch die ZAC, die sehr, sehr hilfreich sind, aber auch an anderer behördlicher Stelle ist ein sehr gutes umfangreiches Angebot vorhanden. Allerdings ist es manchmal so, dass die Unternehmen über dieses Angebot noch nicht ausreichend Bescheid wissen. Für uns heißt das, dass wir daran arbeiten müssen, zielgruppenorientierte Angebote noch stärker zu etablieren, und das bedeutet eben auch: ausprobieren, experimentieren.

Wenn Sie in der Forschung sind, dann müssen Sie, wenn Sie weitere Ergebnisse erzielen wollen, tatsächlich Maßnahmen ergreifen, um Verbesserungen in Ihrem Kenntnisstand zu erlangen. Da kommen wir auch zu dem Thema der Regulatorik, das schon öfter angesprochen wurde, und zu dem Thema der positiven Fehlerhaltung.

Was wir sehr oft haben – das ist manchmal vielleicht ein kleiner Nachteil – hinsichtlich der behördlichen Sicht: Man hat möglicherweise Angst, Fehler zuzugeben. Sie müssen aber auch verstehen: Hinter jedem kleinen und mittelständischen Unternehmen stehen Menschen, und Cyberattacken sind sehr stark menschlich orientiert, menschlich zentriert. Sehr oft heißt es auch: Der Mensch ist zum Beispiel in einem Unternehmen das schwächste Glied in dieser Angriffskette. Gleichwohl könnte man umgekehrt sagen: Der Mensch ist im Gegenzug der Stärkste, um

diese Angriffe abzuwehren, wenn man die Kenntnis hat und wenn man die Möglichkeit hat, die Tools effizient einzusetzen.

Noch einmal zurück zum Thema Regulatorik: Wenn wir hier einzelne Gesetze ansprechen – da sind Sie besonders gefordert, meine sehr verehrten Damen und Herren –, dann ist das im Bereich der Digitalisierung eine gute Maßnahme, die aber optimiert werden kann, wenn man das Ganze holistisch betrachtet. Sie können zum Beispiel Datenschutz, KI-Verordnung oder einzelne Möglichkeiten nicht mehr singulär betrachten, wenn Sie einen effizienten Schutz und eine effiziente digitale Souveränität gewährleisten wollen.

Das heißt, wir müssen hier stärker an einer Vernetzung, stärker an einem Austausch arbeiten. Wir müssen noch viel mehr Möglichkeiten für Reallabore schaffen, in denen wir eine gesicherte Möglichkeit haben, bestimmte Fälle auszuprobieren, Erkenntnisse zu erarbeiten und diese dann in den Transfer und in die Translation umzusetzen. Dazu gehört, dass gerade bei öffentlichen Ausschreibungen heimische Unternehmen, die über diese Informationen verfügen und über den Kenntnisstand der hiesigen Industrie, Zugang bekommen, den sie oft manchmal aufgrund bestimmter anderer Lagen nicht bekommen können.

Weiter ist es wesentlich, die IT-Sicherheit in Open Source Software zu unterstützen. Open Source Software wird sehr oft gerade im KI-Bereich verwendet, um weiter zu experimentieren. Wenn wir hier einen zusätzlichen Sicherheitslayer schaffen, haben wir auch schon wieder viel gewonnen. Außerdem sollten wir die ethische Schwachstellenforschung nicht außer Acht lassen.

Das heißt, Datennutzung bietet uns im Grunde genommen auch sehr viel Datenschutz und in Zukunft hoffentlich ein gutes Maß für verbesserte Cyberangriffabwehr.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Herzlichen Dank. – Für die Fragerunde nehme ich gerne schon Wortmeldungen auf. Bevor wir aber in diese Fragerunde einsteigen, hat Frau Prof. Dr. Schulmann, das Wort. Bitte schön.

SVe Prof. Dr. Haya Schulmann (Goethe Universität Frankfurt): Danke. – Sehr geehrte Abgeordnete, sehr geehrte Damen und Herren! Ich danke Ihnen für die Einladung zu dieser Anhörung. Am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE führen wir regelmäßig umfangreiche empirische Studien durch. Wir vermessen systematisch die von außen sichtbare IT-Infrastruktur in Deutschland – Behörden, Hochschulen, Unternehmen, kritische Infrastrukturen. Die Ergebnisse zeigen, wo die Verwaltung, die Wirtschaft und die Forschung verwundbar sind und was sich dagegen tun lässt.

Was beobachten wir? Die IT in Deutschland, in Bayern wächst. Es gibt immer mehr Systeme, immer mehr Vernetzungen, immer mehr Dienste. Was sehen wir aber nicht? Wir sehen keine Zeichen für eine strukturelle Modernisierung der IT-Architekturen im großen Stil. Die Systeme werden mehr, aber die grundlegenden Probleme bleiben.

Dabei zeigt sich ein klares Muster. Große Organisationen sind tendenziell besser als kleine Organisationen aufgestellt. Sie haben zwar insgesamt mehr Schwachstellen, weil sie auch mehr IT haben, aber die Dichte der Schwachstellen pro System ist geringer. Der Grund dafür ist die Professionalisierung: klare Zuständigkeiten, verbindliche interne und externe Standards, ein automatisierter Prozessor, Werkzeuge und spezialisiertes Personal.

Ein weiterer Befund ist, dass sektorale Sicherheitsorganisationen wirken. Wo es Regulierungen, koordinierende Stellen und zentral angebotene Sicherheitslösungen gibt, sehen wir weniger heterogene IT und bessere Ergebnisse. Das LSI leistet hier übrigens sichtbar sinnvolle Arbeit.

Aus unseren Daten lassen sich vier Hauptursachen für Sicherheitsprobleme ableiten. Diese vier Faktoren finden wir in praktisch jeder der von uns untersuchten Organisationen unabhängig von der Branche oder Größe; das ist auch kein Bauchgefühl, sondern das können wir mit Daten belegen.

Erstens. Legacy – veraltete und vergessene IT: Organisationen bauen ständig neue Systeme auf, die IT wächst, aber alte Systeme werden nicht abgeschaltet. Zurück bleiben verwaiste Server, vergessene Domains, Registereinträge, ungewartete Testsysteme. Diese Altlasten sind häufig der Einstiegspunkt für Angreifer.

Zweitens. Digitale Lieferketten: Eine moderne IT besteht aus Hunderten von Komponenten verschiedener Hersteller, Websiten laden Skripte von Dutzenden externen Quellen. Wenn nur eine dieser Komponenten kompromittiert wird, sind alle betroffen, die sie nutzen. Dieses Risiko wird systematisch unterschätzt und selbst in großen Unternehmen nicht ausreichend adressiert.

Drittens. Fehlende oder falsch konfigurierte Sicherheitsmechanismen: Bewährte Sicherheitsmechanismen existieren für Clients, für Servernetze, für Infrastruktur wie E-Mail-Sicherheit, Verschlüsselung, Multi-Faktor-Authentisierung und vieles andere. Sie werden aber nicht oder fehlerhaft eingesetzt. In unseren Messungen fehlen diese Mechanismen bei 40 % bis 90 %; das hängt von der Branche und dem Mechanismus der untersuchten Systeme ab.

Viertens. Unzureichendes IT-Management: Wir finden regelmäßig Administrationszugänge, die aus dem Internet erreichbar sind, unnötig offene Ports, Systeme, die ihre Softwareversionen preisgeben, Dienste ohne Zugangskontrolle. Das sind keine exotischen Schwachstellen, sondern das ist fehlendes Grundhandwerk.

Was folgt daraus, und wie kann Bayern die Sicherheit verbessern? Der Schlüssel liegt in der Professionalisierung des IT-Managements. Das bedeutet verbindliche Standards, klare Organisationsstrukturen, definierte Verantwortlichkeiten. Sicherheit muss als Primärziel behandelt werden, sie ist kein Nebenaspekt. Das gilt auch für die Herstellerauswahl. Entscheidungen sollen nach rationalen Sicherheitskriterien und nicht nach ideologischen Sekundärkriterien fallen. Ob eine Lösung Open Source ist oder von einem bestimmten Anbieter stammt, ist weniger relevant als die Frage, ob sie sicher betrieben werden kann.

Kleinere Einheiten – Kommunen, Mittelstand, kleinere Hochschulen – können diese Professionalisierung nicht alleine leisten. Sie brauchen Unterstützung. Das LSI sollte hier gestärkt werden.

Für die verschiedenen Sektoren braucht es allerdings auch spezifische Ansätze, Mindeststandards, eine Zertifizierung von Herstellern, Dienstleistern und eine koordinierte Unterstützung. Das alles sollte jedoch nicht zentral im LSI sein, weil die Sektoren informationstechnisch sehr unterschiedlich sind. Ein Krankenhaus hat andere Anforderungen und eine andere IT-Infrastruktur als ein Energieversorger.

Wo nötig, sollten Standards gesetzlich festgeschrieben werden. Eine Freiwilligkeit alleine reicht nicht. Das zeigen unsere Daten deutlich.

Lassen Sie mich zum Schluss einen strategischen Punkt, nämlich die digitale Souveränität ansprechen. Einseitige Abhängigkeiten gegenüber wenigen Ländern sind ein Sicherheitsrisiko; es geht um Erpressbarkeit, um Datensouveränität, um den

schleichenden Verlust eigener Kompetenzen. Autarkie ist dafür aber keine Lösung. Sie ist bei unserer knappen Ressourcenlage – Arbeitskräfte, natürliche Ressourcen und Geld – unerreichbar und wäre auch kontraproduktiv, denn Innovation entsteht in globalen Partnerschaften und nicht in Abschottung.

Die richtige Strategie ist risiko- und chancenbasiert. Eigene Lösungen brauchen wir dort, wo die Risiken besonders groß sind – etwa bei kritischen Infrastrukturen, deren Ausfall dramatische Folgen hätte –, und wir brauchen sie dort, wo die Chancen besonders groß sind, dass Deutschland Innovationsführer wird und wir unsere Zukunft als Industrienation, unseren Wohlstand sichern können.

Künstliche Intelligenz – das ist ein gutes Beispiel – erfordert Fokus statt Gießkanne und eine gezielte Förderung von Forschung, Innovation und Transfer. – Vielen Dank für Ihre Aufmerksamkeit.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Danke schön. – Vielen Dank für diese interessanten Einblicke. Ich habe jetzt vier Kolleginnen und Kollegen auf der Rednerliste. Das sind Benjamin Adjei, Tobias Beck, Florian von Brunn und Kerstin Schreyer. Wenn es möglich ist, richten Sie Ihre Fragen bitte direkt an eine Expertin oder einen Experten – ich weiß, dass die Fragen manchmal mehrere betreffen –, damit wir sozusagen einigermaßen geordnet durch dieses Verfahren kommen. – Herr Köhler, Sie würde ich für die zweite Fragerunde aufnehmen. – Wir beginnen jetzt bei Herrn Adjei. Bitte.

Abg. Benjamin Adjei (GRÜNE): Vielen Dank für die sehr breiten und tiefgehenden Informationen. Ich glaube, sie helfen uns allen sehr gut weiter.

Herr Blumberg, Sie haben die Förderprogramme angesprochen und dass sich Unternehmen eine staatliche Unterstützung wünschen würden. In welcher Form würden Sie sich das wünschen? Wie sollte das ausgestaltet sein, dass das vor allem auch bei kleineren Unternehmen ankommt und Wirkung entfaltet und das nicht nur Mitnahmeeffekte bedeutet? Geht es um Schulungen, um Hardwarebeschaffung, um Dienstleistungen oder Ähnliches? Wie sollte so etwas ausgestaltet sein?

Herr Geisler, ich möchte das Thema Kommunen ansprechen, obwohl wir heute eher über die Wirtschaft sprechen, denn Kommunen sind natürlich auch ein relevanter Faktor beim Thema "grundlegende IT-Sicherheit". Wir haben das Bayerische Behördennetz. Meines Wissens besteht die Möglichkeit, dass sich Landkreise in das Behördennetz einklinken, aber nicht einzelne, kleinere Kommunen, also Rathäuser in normalen Gemeinden. Wäre es sinnvoll, das zu erweitern, um gewisse Angriffsvektoren herauszunehmen? Welche Strategie fahren Sie bei dem Thema "kommunale IT-Sicherheit"?

Frau Schuller, das Thema Ausbildung wurde heute von mehreren angesprochen. Ich glaube, die IHK ist natürlich ganz relevant, wenn es darum geht, das Thema IT-Sicherheit sowohl in die Ausbildung von allen Fachinformatikerinnen und Fachinformatikern als auch in anderen Ausbildungsrichtungen einzubauen und nicht nur in die Ausbildung derjenigen, die sich darauf spezialisieren, weil heute einfach alle damit konfrontiert werden. Was macht die IHK, wenn es um die Lehrpläne in den Schulen, in den Berufsschulen geht?

Zu guter Letzt haben ich eine Frage an Frau Schulman zum Wissenstransfer aus der Wissenschaft. Sie haben sehr viele wissenschaftliche Erkenntnisse, und ich glaube, Ihre Forschungsstelle im ATHENE beschäftigt sich auch genau mit dem Transfer in die Unternehmen. Wie ließe sich das strukturell stärken, damit am Ende vor allem kleine Unternehmen in den Bereichen Prävention und Reaktion das,

was wir wissenschaftlich wissen – die Probleme, die Lösungsmöglichkeiten, die wir haben –, zielgerichtet am besten umsetzen können?

Abg. Tobias Beck (FREIE WÄHLER): Herzlichen Dank für Ihre Ausführungen. Meine erste Frage bezieht sich auf die staatlich unterstützten APT-Gruppen. Herr Schinabeck, wie sehen Sie das gerade im Hinblick auf unsere KMUs? Welche Verbesserungen könnte man herbeiführen, damit solche Bedrohungen vielleicht bereits in der Entstehung verhindert werden? Allerdings glaube ich auch, dass das ganz, ganz schwierig ist.

Herr Blumberg, Unternehmen haben oft verschiedenste Netze. Meistens ist das IT-Netz eines der sicheren Netze. Natürlich gibt es aber auch OT-Fernzugänge, Servicenetze oder Zuliefererzugänge. Wo gibt es hier Möglichkeiten, zum Beispiel Verbesserungen herzustellen?

Eine weitere Frage richtet sich an das LSI und das LKA. Der derzeit gefährlichste und ressourcenintensivste Angriffsvektor ist die Ransomware. Welche zusätzlichen Unterstützungsstrukturen – sei es technisch, organisatorisch oder rechtlich – braucht die bayerischen Wirtschaft, um hier im Ernstfall schneller agieren zu können?

Meine letzte Frage, die vielleicht ein wenig technischer ist, richtet sich an Frau Schulmann. Es geht um DNS-Routing und Manipulation, denn man hört immer wieder, dass das weltweit zunimmt. Ist eine verpflichtende DNSSEC oder eine DNS-based Authentication of Named Entities sinnvoll? Sollte Deutschland eine BGP-Härterichtlinie einführen – ich glaube, aus Bayern heraus würde das wenig Sinn machen –, oder wäre das sogar etwas, das man auf europäischer Ebene regulieren müsste?

Abg. Florian von Brunn (SPD): Ich danke den Expertinnen und Experten für die Statements. Zunächst habe ich Fragen zu den Angriffen auch mit Datenverlusten, die es bisher schon gab. Mir ist aufgefallen, dass das insbesondere häufig Krankenhäuser, aber auch Behörden betroffen hat. Bei den Behörden wird jetzt versucht, immer mehr kommunale Behörden in das Bayerische Behördennetz mit einer Absicherung hineinzunehmen. Herr Boele, Herr Geisler und Herr Radmacher: Was müsste man aus Ihrer Sicht im Bereich der Krankenhausinfrastruktur tun – das betrifft vielleicht auch Pflegeheime, wo private Daten und Gesundheitsdaten abfließen können –, um die Sicherheit zu erhöhen, und was kann man bei den Behörden noch tun?

Dann möchte ich den Kreis auf Frau Schuller und auf Frau Schulmann erweitern. Was kann im Hinblick auf die ausländischen Akteure – Stichwort: Industriespionage, Abfluss von Daten und möglicherweise auch Denial of Service – noch getan werden? Was bringt in diesem Zusammenhang digitale Souveränität, sich also eben von ausländischen Anbietern und insbesondere von den USA unabhängig zu machen?

Dann noch am Rande: Wie bekommen wir das angesprochene Problem in den Griff, dass das, was wir an Regulierungen haben, bei den kleinen und mittleren Unternehmen sehr viel Overhead erzeugt? Wie kommt man statt der reinen Berichte und der formalen Verfolgung von Prozessbeschreibungen mehr in den praktischen Schutz?

Zuletzt habe ich eine weitere Frage an Herrn Geisler. Wie ist die Zusammenarbeit zwischen BSI und LSI geregelt? Ich glaube, Vorfälle der kritischen Infrastruktur werden an das BSI gemeldet. Wie ist Ihre enge Abstimmung mit dem BSI? Gibt es hier Verbesserungsmöglichkeiten?

Abg. Kerstin Schreyer (CSU): Auch ich richte ein Dankeschön an alle für den wertvollen Input. Frau Schuller, Sie werden bei den IHK-Mitgliedern feststellen, wie sich die Unternehmen auf dieses Thema vorbereiten. Mein Gefühl ist: Die großen Unternehmen haben eine ganze Abteilung, sie wissen, wie es geht, und sie werden sich zumindest einigermaßen vorbereiten, sofern man das überhaupt kann. Demgegenüber hat ein Handwerker vor Ort mit einem kleinen Betrieb das Personal und die Manpower überhaupt nicht.

Haben Sie einen Überblick, was diese Unternehmen machen? Bitte verstehen Sie mich nicht falsch; ich erwarte keine Statistik. Sie bekommen aber bei den Terminen und Veranstaltungen natürlich ein Stück weit mit, was die kleinen Unternehmen machen. Machen sie die Augen zu und hoffen darauf, dass es sie nicht erwischt? Was sind da aktuell die Antworten? Ungeachtet der Frage, was wir tun müssen, wüsste ich also gerne: Wie ist aktuell die Situation in den Unternehmen, oder wie nehmen Sie sie wahr?

Vorsitzende Stephanie Schuhknecht (GRÜNE): Vielen Dank. – Ich werde versuchen, das jetzt ein wenig zu strukturieren. Herr Blumberg, bei Ihnen ging es unter anderem darum, wie die Förderprogramme ausgestaltet sein sollten und wie eine staatliche Unterstützung konkret aussehen sollte. Natürlich können Sie auch zu den Fragen, die an die anderen gerichtet waren, Stellung nehmen. Bitte, Herr Blumberg.

SV Holger Blumberg (KRONES AG): Zum Thema Förderung: Was stelle ich mir dabei vor? Ich hatte in meiner Ausführung angesprochen, dass ich große Unterschiede bei der Einkaufsmacht eines großen versus eines kleinen Unternehmens sehe, und ich weiß auch, dass wir uns in unserem Land in der Regel eigentlich heraushalten, Unternehmen bei, ich sage einmal, Preisen und diesen Dingen zu helfen. Allerdings glaube ich, dass wir hier einen Handlungsbedarf haben. Wir müssen Rahmenbedingungen schaffen, dass sich kleinere Unternehmen zusammentun – sei es über Verbände, sei es über andere Organisationen.

Mein Wunsch wäre, den politischen Rahmen dafür zu schaffen, damit das funktioniert. Wie gesagt: Jemand wie BMW kauft bei einem großen israelischen Sicherheitshersteller und erhält einen ganz anderen Rabatt, wenn er 40.000 Lizenzen kauft, als der kleine Handwerker – bleiben wir bei diesem Beispiel – oder das kleine Unternehmen, das ich vorhin angesprochen hatte, wenn fünf Lizenzen gekauft werden.

Bei den Dienstleistungen ist es genauso. Ich hatte ausgeführt, dass wir uns ein Sicherheitscenter leisten. Dort sitzen heute zehn Mitarbeiter, die unser komplettes Netz 24/7 überwachen. Das machen wir nicht in Deutschland. Das macht bei uns ein Team in Indien, an unserem indischen Standort, weil wir uns das in Deutschland gar nicht leisten könnten. Der kleine Unternehmer geht zu irgendeinem Dienstleister, der das anbietet und der natürlich eine Marge daran hat, und zahlt erheblich mehr. In der Regel ist das für das kleine Unternehmen auch fast wieder nicht bezahlbar.

Wie finden wir hier Möglichkeiten? Wie sind wir hier vielleicht in einem ganz anderen Rahmen kreativ? Denn auch das ist etwas, das ein kleines Unternehmen im Zweifelsfall nur dann macht – Sie hatten es angesprochen –, wenn der Einschlag stattgefunden hat.

Meine Wahrnehmung ist: Wenn ein Unternehmen einmal richtig hart erwischt wurde und einmal mehrere Wochen gebraucht hat, um die Daten zu rekonstruieren, dann nimmt es richtig Geld in die Hand. Gerade die kleineren tun das zunächst nicht. Damit komme ich wieder darauf zurück: Wie können wir einen poli-

tischen Rahmen schaffen, damit diese Dinge für kleine Unternehmen bezahlbarer werden?

Zur Frage zum Thema Netze: Ich möchte jetzt nicht zu technisch sein, aber ich glaube, es wurde schon angesprochen, dass Unternehmen mehrere Netze haben. Wir haben ein ganz normales Netz für die kaufmännischen Dinge – ein Officenetz, das Sie im Landtag auch haben werden –, und wir haben ein Netz, an dem bei uns zum Beispiel Produktionsmaschinen dranhängen. Das muss man konsequent trennen, aber das findet in vielen kleineren Unternehmen heute noch nicht statt.

Wir haben auch noch eine dritte Art von Netzwerktechnologie, weil in unseren Abfüllanlagen, die wir unseren Kunden verkaufen, ganz viel Netzwerktechnologie steckt. Sie wurde in der Vergangenheit in Hallen gestellt, und niemand hat daran gedacht, dass man von draußen eigentlich darauf zugreifen kann. Heute ist das ein ganz großes Thema.

Was tun wir im Unternehmen? Wir fördern den Austausch. In der Vergangenheit waren es komplett getrennte Organisationen. Maschinen werden von der Produktion eingekauft. Interne IT wird von der internen IT betrieben und eingekauft. Produkte werden eigentlich von den Konstrukteuren entwickelt. Wir machen das interdisziplinär und tauschen uns aus.

Sehr stark nach vorne treiben wir, die Erfahrung, die wir in der internen IT haben, in die anderen Bereiche hineinzubringen, weil wir in der Regel, was die Themen Struktur und Systematik angeht, in den zentralen EDV-Bereichen im Schnitt fünf bis zehn Jahre weiter als die Produktionsbereiche oder zum Teil auch die Produktentwicklungsbereiche sind. Tiefer möchte ich hier nicht hineingehen; das können wir gerne später offline machen.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Herzlichen Dank. – Herr Boele, bei Ihnen hatte der Kollege von Brunn bezüglich Krankenhäusern und Behörden nachgefragt. Bitte schön.

SV Thomas Boele (Check Point Software Technologies GmbH): Ich denke, wichtig in diesem Bereich ist: Die Digitalisierung ist gerade bei den Krankenhäusern und bei den Behörden in aller Munde, um den ganzen Betrieb einfach effizienter zu gestalten. Wir sehen allerdings insbesondere bei den Krankhäusern, dass ziemlich viel Legacy Technologie im Einsatz ist, die zwar gut funktioniert, aber die natürlich schon veraltet ist. Dazu kommt: Wir haben einige große Konzerne, die in dem Bereich Krankenhäuser fokussieren, und wir sehen, dass zum Beispiel im Bereich der Altenpflege die Budgets mit sehr spitzem Bleistift berechnet sind. Das heißt, man hat in vielen Bereichen reaktive Geschichten, und man hat natürlich nicht immer genügend Personal, um die Sachen abzusichern.

Was macht normalerweise ein Angreifer? Er sucht sich das schwächste Glied in der Kette, um dort hineinzugehen. Das ist zum einen in vielen Bereichen die Krankenhausinfrastruktur; dort kann man sehr effektiv und medienwirksam angreifen. Zum anderen sind das natürlich auch Behörden. Das heißt, wir haben dort eine Mischung aus den unterschiedlichsten Technologien, und wir haben die Notwendigkeit, zu digitalisieren, um das Ganze effizienter zu machen.

Für mich beginnt Security im Kopf. Man muss sich darüber bewusst sein: Was bedeutet das für mich? Ich arbeite gerne mit First Principles. Was möchte man verhindern? Im Prinzip sollte man sich zum Beispiel aufschreiben: Ich möchte einen messbaren Verlust mit einem Cyberevent über die nächsten drei Jahre verhindern und darauf die Maßnahmen ausrichten.

Bei einem Krankenhaus muss man natürlich überlegen: Was sind die Kronjuwelen? Das sind die Patientendaten. Sie müssen ausgetauscht werden – ich denke, es ist wichtig, dass Ärzte vernetzt sind –, und dafür muss man Plattformen liefern. Man sollte aber im Prinzip für sich festlegen, was für einen wichtig ist. Dabei sollte ein Prevention-first-Paradigma gelten, also Maßnahmen zu ergreifen, um Angriffe zu verhindern. Es geht natürlich auch darum, eine gewisse Standardisierung vorzunehmen – im Bereich von Konzernen kann man das relativ gut tun –, und Maßnahmen umzusetzen.

Das Gleiche gilt im Bereich der Behörden. Dort haben wir sicherlich sehr viele Dinge, die zum Beispiel in Kommunen von kleineren Gruppen gemanagt werden. Auch hier geht es darum, zu fragen: Wie kann ich Synergieeffekte erzielen? Wie kann ich ein vernünftiges Sicherheitskonzept aufsetzen, das weiter reicht?

Wir hatten vorhin über den Informationsaustausch gesprochen. Letztendlich geht es dabei auch darum, dass gemeldet wird, wenn etwas passiert, dass den Leuten bekannt ist, dass etwas passiert ist, dass man die Mechanismen versteht, was passiert ist, und dass man das Ganze entsprechend austauscht.

Ich bin zwar bei einem Hersteller, aber für mich kommt die Technologie am Schluss. Die Technologie ist das, was im Prinzip eine Taktik und eine Strategie umsetzt.

Long story short: Wir müssen im Bereich von Krankenhäusern und Behörden verstehen, was die Kronjuwelen sind und was gesichert werden muss. Sicherheit soll in diesen Bereichen enabler sein. Das heißt, die Sicherheit sollte so eingesetzt werden, dass man als normaler Mensch – als normaler Mitarbeiter oder als Bürger, der auf Ressourcen zugreift – gut arbeiten kann. Das Ganze basiert wiederum auf einer vernünftigen Sicherheitsstrategie mit offenen Standards, die entsprechend umgesetzt wird.

Wir hatten eben noch über das Thema Netzwerke gesprochen. Da geht es auch darum: Im Bereich OT hat man viel Legacy Technologie. Warum sollte man aber Roboter oder Werkzeugmaschinen wegwerfen, selbst wenn sie 15 oder 20 Jahre alt sind? Dort geht es wirklich darum, dass man, wie das Herr Blumberg angesprochen hat, die Sachen segmentiert, Sicherheitsbereiche definiert und sicherstellt, dass die Maschinen nicht einfach so nach außen kommunizieren können. Hier kann man mit Segmentierung viel erreichen.

Ich denke, man kann eine Maschine nicht wegwerfen, wenn sie noch Geld verdient. Man muss aber eine Hülle darum machen, um das Ganze abzusichern und entsprechend weiterentwickeln zu können. Dafür gibt es Möglichkeiten, und darüber muss man einfach offen sprechen.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Vielen Dank. – Herr Geisler, an Sie gab es die Frage nach den Kommunen und nach dem Bayerischen Behördennetz, die Frage zu den Krankenhäusern und Behörden und die Frage nach der Zusammenarbeit LSI/BSI und den Verfahren.

SV Bernd Geisler (LSI): Zu den Kommunen: Als Vorteil des Bayerischen Behördennetzes möchte ich betonen, dass das Bayerische Behördennetz unter sehr intensiver Beobachtung und Betreuung durch das LSI steht. Wir haben, ähnlich wie das Bayerische LKA, eine 24/7-Bereitschaft. Wir haben eine Echtzeitüberwachung aller Systeme. Wir haben zahlreiche proaktive Maßnahmen im Einsatz, die verhindern, dass Angreifer erfolgreich in das örtliche Behördennetz eindringen können. Das Bayerische kommunale Behördennetz ist letztlich ein Teil dieses staatlichen Behördennetzes, und wer an dem kommunalen Anteil des Behördennetzes teil-

nimmt – ich sage an der Stelle "ausschließlich teilnimmt" –, profitiert von allen diesen Maßnahmen.

Wir könnten jetzt eine ganze Stunde damit füllen, darzulegen, was das alles ist. Es sind aber wirklich sehr wirksame Maßnahmen, denn – auch das kann man durchaus einmal sagen – eine erfolgreiche Kompromittierung, Verschlüsselung einer staatlichen Einrichtung ist mir an dieser Stelle nicht bekannt. So etwas gab es nicht. Im Bereich der Kommunen gab es das durchaus, das ist klar. Wer sich also ausschließlich in dieses kommunale Behördennetz begibt, hat durchaus zahlreiche Vorteile kostenfrei im Bereich der IT-Sicherheit.

Wie funktioniert das? Das kommunale Behördennetz wird über die Landkreisämter ausgebreitet. Man braucht initial immer einen Knotenpunkt, einen Ansatzpunkt an einem Landratsamt. Kreisfreie Städte sind natürlich ausgenommen, aber ein Landratsamt muss letztlich Zugang zum kommunalen Behördennetz bieten. Das machen in Bayern nahezu alle Landkreise, wobei nicht alle Kommunen an diesem kommunalen Behördennetz teilnehmen; das muss man an dieser Stelle auch sagen. Mein aktueller Stand ist, dass einige wenige Landkreise diese Möglichkeit noch nicht bieten. Dann tritt genau das ein, was Sie, Herr Adjei, gesagt haben: Es gibt einzelne Kommunen, die tatsächlich nicht am kommunalen Behördennetz teilnehmen können.

Im Moment ist das einfach so im KomBN vorgesehen. Ich wüsste auch nicht, dass eine Änderung erfolgt, wonach einzelne kreisangehörige Kommunen unabhängig von ihrem Landratsamt am Behördennetz teilnehmen können.

Wie ist die Strategie? Unser Petitum ist natürlich, dass bitte alle Landkreise einen kommunalen Behördennetzzugang anbieten, weil das im Hinblick auf die IT-Sicherheit erhebliche Vorteile beinhaltet.

Im Bereich der Zukunftskommission wird dieses Thema zentral angegangen. Die Idee dabei ist, einen kommunalen IT-Dienstleister zu haben, der diesen Zugang letztlich auch zentral – davon gehe ich einmal aus – anbietet. Es steht noch nicht genau fest, wie das Ganze einmal ausgestaltet wird. Wenn man aber einen kommunalen zentralen IT-Dienstleister hat, dann hat man auch ganz andere Möglichkeiten.

Das ist eine ganz wichtige Sache, weil man hier sehr viel Positives im Sinne von Standardisierung, Zentralisierung und Konsolidierung bewirken kann. Denn wir sehen schon: Wir haben eine sehr inhomogene Landschaft im kommunalen Bereich. Hier mehr Standardisierung und Standards umzusetzen, wäre ein erheblicher Sicherheitsgewinn, den wir uns von dieser Maßnahme "Zukunftskommission, kommunaler IT-Dienstleister" versprechen würden.

Herr Beck, Sie hatten zum Thema Ransomware auch mich kurz angefragt, wer von Ransomware betroffen ist oder sich überhaupt einmal damit beschäftigt. Da muss man sich auch die Frage stellen: Was sind die Ursachen, um überhaupt erfolgreich verschlüsselt zu werden? Unsere Empfehlung wäre, sich an gängige Maßnahmen zur IT-Sicherheit, an den Stand der Technik zu halten. Dann ist man eigentlich sehr gut geschützt, weil die erfolgreichen Kompromittierungen im Bereich Ransomware letztlich überwiegend durch Kleinkriminelle geschehen, die finanzielle Motive haben; das sind keine high sophisticated APT-Dienstleister.

Die Angriffsvektoren wurden schon genannt. Phishing und Schwachstellen: Da kann man eigentlich sehr viel tun. Man kann mit Awareness arbeiten, und man kann ein vernünftiges Schwachstellenmanagement proaktiv vorschalten, damit man gar nicht in die Lage kommt, erfolgreich angegriffen zu werden. Das wären meine Ansatzpunkte. Wenn es jedoch passiert ist, muss die Reaktion sehr schnell

erfolgen. Mittlerweile gibt es Gruppierungen, die ein System, wenn sie einmal eingedrungen sind, sogar innerhalb weniger Minuten erfolgreich kompromittieren, übernehmen und verschlüsseln.

Man muss also sehr schnell reagieren, und eigentlich ist der beste Rat, den man geben kann, zu verhindern, dass überhaupt jemand unerkannt auf solche Systeme draufkommt. Dafür ist viel zu tun, und mit Sicherheit geht es dabei auch darum: Muss alles nach außen exponiert sein? Wie sichere ich die Zugänge ab? Auch die Multi-Faktor-Authentisierung zieht sich ein wenig durch. Nicht Multi-Faktor-abgesicherte Zugänge aus dem Internet in kritische Netze dürften eigentlich gar nicht existieren.

Zu den Krankenhäusern und Behörden: Im LSI kümmern wir uns insbesondere auch um die Krankenhäuser; wir haben ein KRITIS-Referat, das vor sieben Jahren zum Beispiel mit der Krankenhausberatung begonnen hat. Ich kann nur bestätigen, was von der "Bühne" bereits gekommen ist: Wir haben hier eine sehr inhomogene IT-Landschaft. Es gibt viele alte Systeme, die noch auf alten Betriebssystemen laufen. Sie funktionieren für die Technik, die dahintersteckt, sehr gut. Wenn das Ganze aber von außen erreichbar ist und nicht mehr durch den Hersteller mit Updates unterstützt wird, hat man das Problem, wenn Schwachstellen bekannt werden, dass es keine Schutzmaßnahmen gibt.

Natürlich ist eine Frage: Wo in meinem Netzwerk sind diese Einrichtungen oder diese Anwendungen erreichbar? Hier gilt, wie auch für Kommunen und andere staatliche Einrichtungen: Eine starke Absicherung ist unerlässlich für das, was von außen erreichbar ist. Dafür gibt es ISMS-Standards; konkret: Grundschutz oder ISO 27001. "Ich muss jetzt so einen Grundschutz oder eine DIN, eine ISO umsetzen" hört sich immer sehr dramatisch an. Letztlich dienen diese Standards aber dazu, standardisiert und strukturiert die IT-Sicherheit in einer Einrichtung zu verbessern.

Es werden ganz viele Fragen automatisch beantwortet, wenn man sich da durchhangelt, und eigentlich soll das eine Arbeitserleichterung sein. Ich habe allerdings manchmal den Eindruck, dass es als Arbeitserschwernis gesehen wird. Eigentlich ist es das aber nicht. Die Umsetzung eines Informationssicherheitsstandards soll die Arbeit erleichtern, weil sie strukturiert durch bestimmte Dinge hindurchführt und Dinge herauskommen, die man dann letztlich umsetzen kann. Es ist jedem nur zu empfehlen, solche Standards umzusetzen.

Für Krankenhäuser und Behörden gilt das Thema "von außen erreichbar, Multi-Faktor-abgesichert" ebenfalls. Das ist, denke ich, zwingend.

Darüber hinaus ist das Thema Identitätsdiebstahl ganz dringlich, das in der Regel auch hinter Phishing-Angriffen steckt. Es wird versucht, Identitäten abzuziehen, um sich dann als legaler, regulärer Mitarbeiter an irgendeinem System anzumelden. Der Schutz von Identitäten ist also ganz zentral.

Letztlich gewinnt auch für Behörden – egal ob staatlich oder kommunal – eine vernünftige Endpoint Security immer mehr an Bedeutung. Schauen wir uns das Thema Cloud an. Wenn wir bestimmte geschütztere Bereiche verlassen und Anwendungen im Cloudumfeld nutzen, ist es von zentraler Bedeutung, dass eine vernünftige Endpoint-Security auf den Clients funktioniert, die sich in diesem Cloudumfeld bewegen.

Zur Zusammenarbeit BSI und LSI: Sie haben vielleicht mitbekommen, dass wir vor knapp zwei Monaten auf der it-sa mit dem BSI eine Kooperation geschlossen haben. Wir arbeiten mit dem BSI aber schon sehr viel länger zusammen. Das BSI

hat im Übrigen auch beim Aufbau des LSI unterstützt. Da haben wir uns in der Aufbauphase 2017 tatsächlich das Know-how geholt.

Wir sind mit dem CERT des BSI in einem Echtzeitaustausch. Das ist unsere zentrale Kommunikationsverbindung. Wir kommunizieren täglich in Echtzeit im Chatformat mit dem BSI über relevante Vorkommnisse, die das BSI sieht und die wir sehen. In diesem VCV, dem VerwaltungsCERT-Verbund, sind allerdings nicht nur wir, sondern auch alle anderen CERTs der Bundesländer. Jetzt haben aber nicht alle anderen Bundesländer so ein LSI mit diesen Möglichkeiten und Fähigkeiten. Der Austausch erfolgt also oftmals zwischen LSI und BSI, und der Rest hört zu und profitiert davon, wobei uns das auch wichtig ist, weil wir unsere Informationen ja teilen wollen. Es gibt diesen Austausch aber schon.

Im Zuge der Kooperation haben wir jetzt auch fachspezifische Dinge vereinbart. Wir suchen uns bestimmte Themen heraus und wollen zum Beispiel im Bereich WebPentesting einen Austausch machen. Wir machen WebPentesting, das BSI macht WebPentesting. Warum tun wir uns also nicht zusammen und schauen, wer da vielleicht das bessere Know-how oder vernünftigere Dinge hat? Wir haben aber auch einen sehr regelmäßigen Austausch auf der Führungsebene, also letztlich mit der Präsidentin und mir vereinbart.

Daneben sind wir – das habe ich auch in der schriftlichen Stellungnahme dargelegt – die Kontaktstelle des Freistaats Bayern für Meldungen oder für Erkenntnisse des BSI betreffend Betreiber kritischer Infrastrukturen. Wenn Betreiber kritischer Infrastrukturen von einem schwerwiegenden Cybersicherheitsvorfall betroffen sind und dieser noch andauert, dann bekommen wir eine Meldung vom BSI für die zuständigen Aufsichtsbehörden. Das heißt, wir erhalten einen Überblick, was passiert. Das Ganze geben wir an die Aufsichtsbehörden in Bayern weiter, und das geht dann auch wieder in Richtung BSI zurück.

Das wird sich mit der Umsetzung der NIS-2 auf Bundesebene verändern. Wir sind auch da die für den Freistaat Bayern zuständige Behörde und gespannt, wie die endgültige Regelung auf Bundesebene aussieht; die zuständigen Behörden müssen sich dann ja auch mit der Kontaktstelle auf der Bundesebene austauschen.

Weil künftig also sehr viel mehr Behörden und vor allem Einrichtungen von NIS-2 betroffen sein werden, gehen wir davon aus, dass das Meldeaufkommen deutlich mehr wird, als es aktuell ist. Aktuell ist es sehr überschaubar. In dieser Schwere passiert in Bayern nicht allzu viel – das muss man an dieser Stelle auch sagen –, was wir vom BSI gemeldet bekommen.

Die Betroffenheit von Einrichtungen wird sich aber vervielfachen, denn die Schwelle, wann man über NIS-2 reguliert ist, geht deutlich nach unten. Dann wird sich auch ein neues Meldeverfahren mit dem BSI ergeben. Das wird aber mit Sicherheit – das erhoffe ich mir zumindest – mit den Bundesländern noch abgestimmt.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Danke schön. – Herr Radmacher, Sie wurden von Herrn von Brunn auch zu dem Thema "Krankenhäuser und Behörden" angesprochen.

SV Norbert Radmacher (LKA): Beim Thema "Krankenhäuser und Behörden" kann ich mich eigentlich den Ausführungen von Herrn Geisler anschließen. Das sind genau die Empfehlungen, die wir auch unserer Arbeit heraus geben würden. Letztlich müssen die Organisation, die Technik und der Mensch zusammenspielen, um hier erfolgreich zu sein.

Ein weiteres Thema waren die Ransomwareangriffe. Das ist in der Tat das Thema, das uns am meisten beschäftigt. Aus unserer Sicht ist die wichtigste Botschaft,

dass wir darum bitten, möglichst frühzeitig mit ins Boot geholt zu werden, wenn ein Unternehmen einem solchen Angriff ausgesetzt ist. Nur dann haben wir eine Chance auf entsprechende Ermittlungserfolge, die wir in der Vergangenheit auch hatten.

Wenn Sie erlauben, werde ich die Herausforderungen anhand von einem Fall darstellen. Dieses Jahr ist es uns gelungen, die Ransomgruppierung 8Base zu bekämpfen. Dabei haben wir sehr eng mit dem FBI, mit Schweizer Behörden und mit weiteren internationalen Strafverfolgungsbehörden zusammengearbeitet. Letztlich konnten wir über 130 Server sicherstellen und 25 aktive Server abschalten. Gleichzeitig erkennt man daran, wie Strafverfolgung dann sofort auch in Prävention umschaltet. Wir konnten über 240 Firmen in 30 Ländern warnen, von einer Verschlüsselung bedroht zu sein, und dadurch, wenn man das einmal hochrechnet, einen Schaden von rund einer Milliarde, wenn man konservativ rechnet, abwenden.

Das heißt, die Strafverfolgung bringt in diesem Bereich etwas, wenn wir frühzeitig mit dabei sind. Hier gebe ich auch noch einmal den Hinweis auf unsere 24/7-Bereitschaft, die man jederzeit alarmieren kann.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Herzlichen Dank. – Der Nächste ist Herr Schinabeck zur Frage nach den APT-Gruppen.

SV Josef Schinabeck (LFV): Vielen Dank für Ihre Frage, Herr Abgeordneter. Ich sage es einmal so: Dem Opfer kann es schon fast egal sein, von wem es angegriffen wird. Der Unterschied ist nur dahin gehend, dass die Ressourcen und die Manpower noch größer sind und die angewandte Technik vielleicht noch ausgefeilter ist, wenn ein ausländischer Akteur oder Dienst dahintersteckt.

Die Defizite bei den kleinen und mittelständischen Unternehmen sind natürlich dieselben wie bei einem Angriff durch einen Kriminellen. Das sind das fehlende Bewusstsein, die fehlenden Ressourcen, eine veraltete Technik und der Umstand, dass kleine und mittelständische Unternehmen nicht die Ressourcen zur Verfügung haben, um sich entsprechend aufzustellen. Meine Mitarbeiter haben mir aufgeschrieben, dass es bereits professionelle Unternehmen gibt, bei denen man solche Dienste einkaufen kann. Sie sind aber eben auch sehr teuer.

Insofern: Es hakt einfach am Bewusstsein, an den Möglichkeiten, an den Ressourcen und natürlich auch an den finanziellen Mitteln, die diese Unternehmen zur Verfügung haben, um sich gegen Angriffe zu wappnen bzw. zu wehren. Im Ergebnis kann es, wie gesagt, dem Opfer egal sein, von wem es angegriffen wird. Die Intensität eines ausländischen Dienstes ist aber eine andere, denn er hat noch mehr Power zur Verfügung und wird noch hartnäckiger versuchen, in die Systeme einzudringen.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Danke schön. – Es gab einige Fragen an Frau Schuller, zum Beispiel zum Thema der Ausbildung der Fachinformatiker. Bitte schön.

SVe Prof. Dagmar Schuller (IHK): Zum Thema Fachinformatiker ist vorneweg zu sagen, dass sich die Ausbildung im Bereich Informatik generell gerade stark reformiert. Wir haben mit einem Trend insbesondere im Bereich der generativen KI zu kämpfen. Was heißt kämpfen? Im Grunde genommen ist eine Anpassungsfähigkeit notwendig, die wirklich darstellt, dass man deutlich stärker in interdisziplinären Projekten arbeiten muss.

Wir haben beim Fachinformatiker unterschiedliche Fachbereiche, zum Beispiel Systems Engineering, Entwicklung und Data Processing. Sowohl in der IHK als auch in der universitären Landschaft – insbesondere an den Hochschulen – zeigt sich sehr stark, dass wir bei der Ausbildung der Informatiker deutlich projektorientierter und schneller arbeiten und mehr methodische Kompetenzen darstellen müssen. Dazu zählt unter anderem verstärkt der IT-Security-Bereich. Das Wesentliche an dieser Stelle ist, zu erkennen, wie schnell Entwicklungen im informatischen Bereich heutzutage passieren.

Wenn Sie sich zum Beispiel den Trend zum Vibe Coding anschauen – das heißt, man verwendet KI oder Plattformen, die sich darauf spezialisiert haben, Codes Snippets unmittelbar durch den Einsatz von generativer künstlicher Intelligenz zu generieren –, dann sehen Sie, wie stark das angenommen wird. Eine der größten Plattformen als europäisches Aushängeschild ist hier Lovable.

Diese schwedische Plattform hat es geschafft, erst kürzlich – ich glaube, es war letzte Woche – Bescheid zu geben, dass sie in ungefähr vier Monaten 200 Millionen Doller Annual Recurring Revenue aufgebaut haben. Das ist ein unglaublicher Umsatz, denn Annual Recurring Revenue bedeutet, immer wiederkehrende Umsätze zu haben. Wir konnten in diesem Bereich in Europa also ganz klar ein Unicorn durch einen europäischen Wagniskapitalgeber aufbauen, das in Summe die ganze informatische Entwicklung sehr stark mit beeinflusst.

Genau diese Art der Entwicklung und dieser Kompetenzen ist es, die in Unternehmen sehr stark gerade für kleinere Tasks eingesetzt wird, zum Beispiel wenn es einmal darum geht, ein Dashboard oder andere Dinge zu erstellen. Natürlich sind das dann auch Tools, die im Grunde genommen dazu führen, dass wir eine andere Art von methodischer Kompetenz in der Ausbildung brauchen.

Zum einen muss man verstehen, wie diese Tools funktionieren. Zum anderen muss man die komplexen Zusammenhänge besser erkennen können. Das heißt: Weg von dem singulären Auswendiglernen und davon, stur bestimmte Tasks zu entwickeln, und hin zu einem Verständnis, wie man ein Problem von mehreren Aspekten her sehen kann.

Wir beobachten das in der Ausbildung, wenn wir uns Schulen wie die 42 Coding School anschauen, die gerade auf diese interdisziplinäre Kompetenz deutlich stärker setzt. Dahin gehend muss die Ausbildung deutlich stärker fokussieren. Eine Herausforderung dabei ist natürlich, Lehrpersonal zu finden – also diejenigen Lehrkräfte und Personen, die bereits didaktisch über diese methodische Kompetenz verfügen –, um das korrekt beibringen zu können.

Darüber hinaus fehlt die Praxis in der Anwendung. Wenn wir ausbilden, um entsprechende Fachkräfte vor allem im Bereich IT-Security oder künstliche Intelligenz für die Wirtschaft zur Verfügung zu stellen, dann müssen wir ein deutlich stärkeres Verständnis für die Zusammenhänge in Summe schaffen. Das bedeutet auch hier eine klare Tendenz zu stärkerem Holismus und zu interdisziplinärem Verständnis statt singulärer Kompetenz, weil eben bestimmte repetitive singuläre Kompetenzen durch den Einsatz der Technologie – insbesondere künstliche Intelligenz – durchaus ersetzt werden.

Das soll aber nicht bedeuten, dass es in Zukunft keine Informatiker mehr geben muss. Ganz im Gegenteil: ein guter Informatiker mit einer soliden Ausbildung ist kaum durch die KI zu ersetzen, weil wir hier gerade auch über kreative Kompetenzen verfügen, die im Grunde genommen die statistische Wahrscheinlichkeit klassischer Algorithmen im Normalfall nicht unbedingt hervorbringen würde.

Wir haben hier einen Umschwung, und diesen Umschwung müssen wir von der wirtschaftlichen Seite, aber gerne auch von der Verwaltungsseite her in der Ausbildung noch einmal stärker unterstützen. Sie wissen es vielleicht noch aus Ihren Studienzeiten: Die eine oder andere Studienprüfungsordnung ist gar nicht so schnell zu reformieren, wie man sich das eigentlich denken würde.

Deswegen: Ja, Fachkräfte sind ein ganz wesentlicher Punkt. Da bedarf es eben auch eines Feedbacks, Möglichkeiten, Unterstützung und einer Zusammenarbeit mit der Wirtschaft, damit wir diese Fachkräfte auf den Stand bringen, den sie tatsächlich brauchen, um effizient umsetzen zu können. – Ich hoffe, das hat Ihre Frage beantwortet.

Stv. Vorsitzende Kerstin Schreyer (CSU): Ich möchte, auch wenn ich jetzt die Sitzungsleitung habe, an die Beantwortung meiner Frage erinnern, wie sich die kleinen und großen Unternehmen aufgestellt haben. Darauf hätte ich gerne noch eine Antwort.

SVe Prof. Dagmar Schuller (IHK): Insofern kann ich berichten: Wie kleinere und größere Unternehmen die sicherheitsrelevanten Faktoren angehen, ist sehr unterschiedlich. Wir haben es bereits gehört. Ein großes Unternehmen verfügt nicht nur über die zeitlichen und finanziellen Ressourcen, sondern auch über die Möglichkeiten, hier umfangreichere Maßnahmen im Alltagsgeschäft abzuwickeln, wobei ich damit aber nicht sage, dass es dort nicht herausfordernd ist.

Die Standardmaßnahmen sind bei kleineren und mittelständischen Unternehmen durchaus normal. Die Durchführung von Backups und Updates ist etwas, das sich im täglichen Betrieb oder im Daily Business sehr gut etabliert hat.

Was fehlt, sind aber zum Beispiel die Notfallexperimente. Es fehlen Anlaufstellen, wo man sich mit Experten auseinandersetzt, die man eben nicht von der finanziellen Komponente her teuer einkauft, und wo man konkrete Probleme, die man im Unternehmen hat, vielleicht durch Externe getestet bekommt oder sich hier versuchen kann. Es gibt zwar mehrere behördliche Anlaufstellen, aber eine zentrale Stelle wäre sehr sinnvoll, um ein sehr niederschwelliges Angebot gerade für die kleinen und mittelständischen Unternehmen bereitstellen zu können.

Deutlich seltener haben wir Notfallpläne oder Abschätzungen, was in kleinen und mittelständischen Unternehmen passiert, wenn es tatsächlich zu einem Angriff oder zum Ausfall eines bestimmten Systems kommt.

Zudem ist bei kleinen und mittelständischen Unternehmen die Abhängigkeit von externen Systemen deutlich höher als bei großen Unternehmen. Sie werden kaum einen Kleinbetrieb kennen, der sich ein eigenes Rechenzentrum leisten kann. Hier wird sehr oft auf Cloudstrukturen oder auf Infrastrukturen von Drittanbietern zurückgegriffen, und man hat nicht die notwendige Transparenz und manchmal auch nicht die notwendige Sicherheit, um verstehen zu können, was die Implikationen des jeweiligen Ausfalls bedeuten würden und ob so etwas an dieser Stelle tatsächlich vorkommen kann.

Bei kleinen Unternehmen sehen wir auch, dass gerade für das Thema Cybersecurity keine ausreichenden Ressourcen zur Verfügung stehen. Oft arbeiten Personen hier multifunktional. Es gibt einen oder zwei IT-Verantwortliche, die plötzlich alles können sollen. Derjenige soll von einem Tag auf den anderen in den Bereichen Systems Engineering, KI, Security der Experte sein. Das ist schlichtweg nicht abbildbar. Man muss dafür sorgen, eine entsprechende Ressource zur Verfügung zu stellen, auf die kleine und mittelständische Unternehmen unter der Implikation Zeit-

und Kostenaufwand effizient zugreifen und bei der wir Umsetzungsstärke zeigen können.

Das heißt, wir haben in bestimmten Bereichen wirklich ein Know-how-Defizit. Man weiß noch gar nicht so richtig, was hier passieren kann. Wir schlagen an dieser Stelle vor, deutlich mehr in die Präventionsarbeit zu gehen.

Es gibt, wie gesagt, eine sehr gute Infrastruktur. Besonders hervorzuheben ist auch die Arbeit des Bayerischen Landesamts für Datenschutzaufsicht, das sehr gute Checklisten zur Verfügung stellt, konkrete Hilfestellungen gibt und den Dialog mit den kleinen und mittelständischen Unternehmen sucht, um zu verstehen, wo die Problematiken liegen. Hier müsste man aber doch noch einmal deutlich stärker in den Austausch gehen, um vor allem die Priorisierung der Problematik zu begreifen.

Dann muss man tatsächlich niederschwelliger klarmachen, an wen man sich im Falle eines Falles wenden kann und was dann passiert. Kleine Unternehmen haben sehr oft Angst, wenn sie den einen oder anderen behördlichen Namen sehen, und oft wird zurückgespiegelt: Oh mein Gott, was kommt denn jetzt alles auf mich zu? Was muss ich liefern? Wie viele Leute muss ich zur Verfügung stellen, um die Informationen tatsächlich bereitstellen zu können? Das sind Dinge, die für den Austausch bzw. für die Offenheit der Kommunikation eher schädlich sind.

Das läuft an dieser Stelle eben nicht so koordiniert und strukturiert wie bei ressourcenstarken größeren Unternehmen ab, die einfach über geschulte Abteilungen und entsprechendes Fachpersonal verfügen. Deswegen sagen wir im Grunde genommen immer wieder: Niederschwellige Angebote, Veranstaltungen und Webinare sehr stark kommunizieren, um das leistungstechnisch an die kleinen und mittelständischen Unternehmen zu bringen, und gerade für diese Zielgruppe – damit zurück zu den zielgruppenspezifischen Angeboten – vielleicht auch innerhalb der Behörden bestimmte Stellen schaffen, die sich konkret damit auseinandersetzen und zu einem kooperativen Austauschpartner für die KMUs werden.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Vielen Dank. – Fragen an Frau Schulmann gab es unter anderem zu dem Thema, wie der Transfer aus der Wissenschaft in die Unternehmen gelingen kann. Von Tobi Beck kam die Frage zur DNS-Routing-Manipulation, welche Ebene am besten regulieren sollte. Vom Kollegen von Brunn gab es auch noch eine Nachfrage. Ich bin mir nicht mehr ganz sicher, in welche Richtung die ging, aber ich glaube, Sie haben es gehört.

SVe Prof. Dr. Haya Schulmann (Goethe Universität Frankfurt): Das mit dem Transfer ist eine gute Frage. Ich sehe folgende Hauptprobleme:

Erstens. Wie nutzt man eine Technologie? Wie nutzt man IT? Das ist das, was Frau Prof. Schuller gerade angesprochen hat. Wie konfiguriert man einen Router? In unseren Studien, in unserer Forschung messen wir und sehen, dass ganz viele Sicherheitsmechanismen in der Praxis gar nicht verwendet oder fehlerhaft genutzt werden. Ein ganz einfaches Beispiel: Wie der Rufstatus von Zertifikaten ist, die widerrufen werden, abgelaufen sind oder invalide sind, checken die Browser gar nicht und werden diesen Status ignorieren. Das heißt, die Benutzer, die Klienten besuchen Webseiten mit invaliden Zertifikaten und werden das gar nicht erkennen. Aber das gilt für viele Aspekte der IT in einem Unternehmen oder in einer Organisation. Viele Sachen werden nicht verwendet oder falsch verwendet, und dann bekommt man keine Sicherheit oder im schlimmsten Fall noch mehr Probleme.

Zweiter Aspekt ist, man hat keine Übersicht in einer Organisation. Was hat man alles in seiner IT? Welche IT ist veraltet? Welche Legacy? Wie sieht meine IT aus?

Wo wächst sie? Werden ganz viele Domänen registriert oder ganz viele Dienste aufgesetzt? Das unterscheidet sich zwischen verschiedenen Sektoren. Nicht überall ist das so. Zum Beispiel Landesverwaltungen sind viel struktureller. Das sieht man. Bei Unternehmen ist das weniger der Fall. Unternehmen haben ganz viele Interfaces nach außen, weil sie sichtbar sein wollen. Dann braucht man natürlich diese Übersicht. Jede Organisation weiß, dass sie Schwachstellen hat. Es gibt keine einzige Organisation in Deutschland und weltweit – wir vergleichen Deutschland auch mit anderen Ländern –, die keine Probleme hat. Jeder weiß, dass er Probleme hat. Deshalb hilft eine Liste, die besagt: "Du hast viele Schwachstellen" sehr wenig. Die Organisationen wissen schon, dass sie Probleme haben.

Was sie eigentlich brauchen, ist Priorisierung: Was bedeutet das für meine Organisation? Was stellt das größte Risiko dar? Wo soll ich anfangen? Welche kurz- und langfristigen Strategien soll ich entwickeln?

Ich muss verstehen, wie meine IT aussieht, wie sie wächst, wo es Bedarf gibt und dementsprechend Strategien planen. Das kann man natürlich aus der Forschung bekommen, wie Sie gesagt haben. Wir brauchen dafür Strukturen. Viele Sachen haben Sie schon angesprochen. Man braucht dauerhafte Transferplattformen. Man braucht standardisierte Mindestprofile. Man braucht zentrale Plattformen, die die Unternehmen verwenden können, und man braucht ein landesweites Attack-Surface-Monitoring, eine Übersicht, ein Lagebild, das nicht nur sagt: "Diese Organisation hat tausend Schwachstellen", sondern auch: Was führt zu diesen Schwachstellen? Was bedeutet das aus Sicht des IT-Managements? Wo sind die Probleme? Hat man nicht ausreichend Management oder Governance oder Verständnis oder Expertise usw.?

Wenn man so etwas macht, dann würde das erlauben, diese Erkenntnisse und Methoden aus der Wissenschaft in die Praxis einzubringen.

Zweite Frage zu der Internetinfrastruktur. Sie haben DNS und BGP, Routing und Naming angesprochen. Das sind Mechanismen, die die Organisationen ganz oft nicht direkt sehen. Das sind Sachen, die irgendwo laufen. Das ist kein Webserver, den man sehen und konfigurieren kann. Die haben ganz oft Probleme und viele Ausfälle. Man hört von Cloudflare. Solche Probleme gab es oft. Die passieren auf Internetinfrastruktur.

Ja, aus meiner Sicht ist das nicht nur sinnvoll, sondern sogar überfällig, dass wir hier verbindliche Anforderungen einführen, zum Beispiel für DNSSEC und RPKI. Übrigens haben die USA das in beiden Administrationen gemacht. Sie hatten Roadmaps zu verschiedenen solchen Sachen. Viele von denen haben unsere Forschung direkt zitiert, weil das etwas ist, was wir stark machen.

Aber die Sache ist, das Internet hat keine Landesgrenzen. Das heißt, wenn man das selbst macht, hilft das ein bisschen, aber nicht signifikant. Wenn es Angreifer gibt, die Angriffe durchführen wollen, werden sie es schaffen, weil das ganze Internet gebraucht wird, das es gemeinsam macht. Dafür braucht man Zusammenarbeit nicht nur auf europäischer Ebene, sondern viel mehr.

Man kann damit anfangen, zum Beispiel in der europäischen Region. Man kann anfangen mit verbindlichen DNSSEC für Betreiber und RPKI und anderen Sicherheitsmechanismen für Netze und für Routing. Natürlich ist auch eine Frage: Wer würde das machen? – Wie schon angesprochen wurde, sind das sehr komplexe Sachen. Wenn man einfach so etwas aufsetzt, kann man ganz oft neue Lücken und neue Angriffsvektoren schaffen. Man braucht Expertise und automatisierte Werkzeuge.

Zurzeit wird diese Software hauptsächlich von Open-Source-Projekten betrieben. Ich stimme zu, Open Source ist wichtig. Aber man muss unterscheiden. Open Source ist nicht gleich Open Source. Es gibt Open Source, zu denen jeder beitragen kann. Vor kurzem gab es einen Angriff. Jemand hat einen Code mit einer Hintertür eingebaut. Wenn jeder beitragen kann und man nicht weiß, wer einen Code schreibt, ist das natürlich gefährlich. Aber nicht alles an Open Source ist so. Es gibt professionelles Open Source. Nur der Code wird dann öffentlich. Man muss einfach die Produkte für diese Protokolle und Systeme professionalisieren. Zurzeit ist das nicht so, und viele haben Probleme.

Wenn Organisationen diese Sicherheitsmechanismen einführen, können sie über diese Mechanismen auch angegriffen werden. Das haben wir untersucht und viele Probleme gefunden. Organisationen wissen nicht, was das bedeutet. Sie denken, sie stellen etwas ins Netz, aber tatsächlich eröffnet das neue Angriffsvektoren. Also ja, das ist wichtig. Wichtig ist aber auch, zu verstehen, was das bedeutet und da zu investieren.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Danke schön.– Wir kommen jetzt zur zweiten Fragerunde. Auf der Liste stehen Herr Köhler, Kollegin Schack, ich selbst und Herr Meier in dieser Runde. Erfahrungsgemäß werden die Antworten kürzer, je länger der Vormittag wird. – Herr Köhler, bitte.

Abg. Florian Köhler (AfD): Herr Schinabeck, Sie haben betont, dass der Austausch zwischen nationalen und internationalen Diensten vital für die Sicherheit sei. Wie bewerten Sie die Forderung des US-Senators Tom Cotton vom Mai 2025, diesen Austausch einseitig zu unterbinden, solange deutsche Behörden die AfD als Oppositionspartei beobachten? Wer ist Tom Cotton? Tom Cotton ist der Vorsitzende des parlamentarischen Kontrollgremiums, also quasi des Pendants zum US-Senat. Wie bewerten Sie die Forderung des US-Senators? Stimmen Sie mir zu, dass das den Schutz Bayerns vor realen Bedrohungen wie Wirtschaftsspionage gefährdet?

Ich habe noch eine Frage an Sie. Das Bayerische Landesamt für Verfassungsschutz ist aufgeteilt in fünf Abteilungen. Abteilung 3 ist ausschließlich mit Rechtsextremismus und Terrorismus befasst, während Linksextremismus in Abteilung 5 mit organisierter Kriminalität, dem Cyber-Allianz-Zentrum, Wirtschaftsschutz, Spionageabwehr und Geheimschutz gebündelt ist. Deutet diese Aufteilung auf eine ungleiche Priorisierung hin, die den Fokus auf rechtsextreme Phänomene einschließlich der AfD-Beobachtung stärkt, und dies auf Kosten einer eigenständigen Bearbeitung von linken Extremisten und staatlichen Akteuren, die Angriffe auf unsere Wirtschaft fahren?

An Herrn Radmacher habe ich auch zwei Fragen. Der Cybersicherheitsbericht 2024 warnt vor einer anhaltenden hohen Bedrohungslage mit 48.000 Angriffen. Welche Sektoren der bayerischen Wirtschaft wie die Automobilwirtschaft oder der Mittelstand sind am stärksten betroffen? Wie hoch schätzen Sie die unmittelbaren wirtschaftlichen Schäden für 2025 ein? Welche Maßnahmen plant das LKA, um diese nicht nur zu bekämpfen, sondern präventiv zu mindern?

Zu guter Letzt: Fehlt es Ihrer Meinung nach in Bayern an einem einheitlichen Cybersicherheitsgesetz? Sieht das LKA gesetzliche Lücken in der IT-Sicherheit, oder reichen die bestehenden Gesetze bis jetzt aus?

Abg. Jenny Schack (CSU): Ich möchte wieder zurückführen auf das eigentliche Thema der IT-Sicherheit in der bayerischen Wirtschaft. Deswegen habe ich ganz konkret eine Frage dazu. Sie geht vornehmlich an Frau Schuller, weil sie es schon angesprochen hat. Wir haben kleine und mittlere Unternehmen, die unter Umständen, das haben wir immer wieder gehört, aus unterschiedlichsten Gründen nicht so

gut vorbereitet sind – und nicht vorbereitet sein können, muss man dazu sagen. Sie haben schon alle ausgeführt, dass es diverse Gründe dafür gibt und was man verbessern könnte. Das wäre auch – Sie hatten es schon angedeutet – eine Frage an Herrn Blumberg. Bei Ihnen habe ich herausgehört, dass Sie auch für das Handwerk sprechen, was man konkret in Bezug auf TTZ in der Ansprache machen könnte.

Frau Schuller, der Bereich Cybersecurity wird mehr und mehr, auch was KI anbelangt, unterstützt werden können. Nun muss man eine KI aber auch trainieren. Wir werfen immer mit diesen Begrifflichkeiten um uns. Eine KI braucht Daten, eine KI muss trainiert werden, sonst ist sie einfach sinnlos oder funktioniert nicht. Ich stelle mir die Frage, wie wir gerade in diesem Bereich eine KI trainieren können, wenn wir die Daten gerade aus den mittelständischen Unternehmen nicht haben, weil wir gleichzeitig Datenschutz gewährleisten wollen. Die Unternehmen fragen aber auch natürlich und nachvollziehbarerweise: Warum soll ich meine Daten hergeben? Wie vulnerabel bin ich da? – Da sehe ich ein Spannungsfeld. Vielleicht gibt es Ideen oder Wege, wie man damit umgehen kann. Deswegen ganz konkret: Wie können wir eine KI trainieren? – Um uns am Ende sicherer zu machen, müssen vielleicht gerade mittelständische Unternehmen erst einmal ihre Daten hergeben.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Vielen Dank. – Ich habe mich selbst auf die Redeliste gesetzt. Ich habe noch eine Nachfrage zu dieser Aufteilung, dass die Kleinen sich schwerer tun, weil sie oft nur eine Person haben, die sich kümmern kann. Ich habe in meinem engeren Umfeld in letzter Zeit einen Fall gehabt, in dem die ganze IT sogar ausgelagert war und sich trotzdem im Nachgang herausgestellt hat, es gab große Lücken. Auch bei Handwerkskammern in Bayern haben ja vor Kurzem Angriffe stattgefunden. Die IT war an einen Dienstleister ausgelagert, und trotzdem hat sich im Nachgang herausgestellt, es war unzureichend.

Gibt es irgendeine Möglichkeit, Unternehmen zu beraten, wer wirklich auf dem Stand der Technik ist, wer sozusagen das liefern kann, was es heute braucht, um abgesichert zu sein? – Natürlich kann immer etwas passieren. Wir wissen, die absolute Sicherheit wird nicht erreichbar sein. Aber wenn man schon den Schritt gegangen ist, Geld für einen externen Dienstleister auszugeben und dann immer noch unsicher ist, stellt sich die Frage: Wie kommt man dahin, dass man weiß, was ein guter Dienstleister ist? – Das wäre die eine Teilfrage. Frau Schuller, Frau Schulmann, Sie beide können vielleicht etwas dazu sagen.

Ich komme zu einem zweiten Komplex, den wir heute noch nicht angesprochen haben. Die Staatsregierung hat vor einigen Jahren einen Cyberschutzschirm für den bayerischen Mittelstand ausgerufen. Der war angedacht als Informationsbund. War jemand von Ihnen daran beteiligt? Gab es da eine Vernetzung? Wie hat die Zusammenarbeit bezüglich dieses Cyberschutzschirms stattgefunden? Was wäre vielleicht noch mehr wünschenswert? Ist ausreichend, was dort bisher gemacht worden ist, oder wäre der Staat an der Stelle noch etwas mehr gefordert? – Das waren meine Fragen. Herr Meier ist der Vierte in der Runde.

Abg. Johannes Meier (AfD): Vielen Dank, Frau Vorsitzende. – Auch von mir erst einmal ein herzliches Dankeschön an die Expertinnen und Experten, dass sie sich die Zeit genommen haben, hier heute anwesend zu sein und sich den Fragen kompetent zu stellen.

Ich habe zu Beginn zwei Fragen an Herrn Luczak. Welche unmittelbaren Maßnahmen sollte der Freistaat jetzt Ihrer Meinung nach ergreifen, um die Resilienz und auch die sicherheitsrelevante Leistungsfähigkeit seiner Industriepartner nachhaltig

zu stärken und zu schützen? Welche strategischen Risiken sehen Sie – Sie haben es eingangs schon angesprochen – für die langfristige digitale Souveränität insbesondere im Hinblick auf globale Anbieterstrukturen?

Ich bin ein absoluter IT-Laie. Wir hatten es ganz am Anfang. Deswegen geht die Frage an Herrn Blumberg, Herrn Boele, Herrn Geisler oder auch Herrn Luczak. Die Lizenzen würden mich interessieren. Von welchen Summen sprechen wir bei diesen Lizenzen, wenn ich sie in kleinen Mengen einkaufe, wenn ich sie in großen Mengen einkaufe, und inwiefern werden solche Lizenzen, wenn es möglich ist, im Rahmen des Digitalbonus schon gefördert, wenn es denn diese Möglichkeit gibt?

Herr Geisler, wie bewerten Sie die aktuelle Gefahrensituation oder das Potenzial von Cyberangriffen auf die Energieinfrastruktur bei uns, also in Deutschland, insbesondere in Bezug auf kritische Komponenten wie Smartmeter oder Heimspeicherbatterien? Welche Schutzmaßnahmen erachten Sie als vorrangig, und wie beurteilen Sie mögliche Risiken durch ausländische Betreiber, speziell China?

Die zweite Frage an Herrn Geisler lautet: Wie schätzen Sie die gleichen Sicherheitsrisiken beim Zugriff auf moderne PKW ein, Stichwort autonomes Fahren, also dass quasi ausländische Angriffe hier stattfinden können, oder auf amerikanische Hersteller? Welche Präventionsstrategien würden Sie empfehlen, um Fremdzugriffen im Falle geopolitischer Konflikte wirksam vorzubeugen?

Vorsitzende Stephanie Schuhknecht (GRÜNE): Wunderbar. Wir fangen am besten wieder von vorne an. Ich glaube, Herr Blumberg war wieder angesprochen, und dann gehen wir dieses Mal die ganze Runde durch. Bitte schön.

SV Holger Blumberg (KRONES AG): Okay, danke. – Frau Schack, ich komme auf Ihre Frage zum Thema Handwerker zurück. Prävention und Information sind sehr wichtig. Das wurde schon angesprochen. Ich glaube, da gibt es gute Ansätze von den Verbänden, sei es die IHK, seien es aber auch die anderen Verbände. Ich glaube, wichtig ist, und das haben wir im Unternehmen gelernt, egal, ob das Unternehmen groß oder klein ist, das muss von oben nach unten vorgelebt werden. Das Topmanagement muss den Mitarbeitern vermitteln: Jeder, aber auch jeder hat sich darum zu kümmern.

Ein Thema, was mir noch am Herzen liegt, ist ein anderes. Was mache ich, wenn ich angegriffen wurde? – Wir leisten uns einen Vertrag mit einem entsprechenden Forensik-Dienstleister, der quasi eigene Hackerkompetenz betreibt und sofort einsatzbereit ist. Ich nenne das einmal schnelle Eingreiftruppe. Auch hier wiederum gilt: Das kleine Unternehmen kann sich wahrscheinlich diesen Service nicht leisten. – Das wäre für mich auch ein Thema, bei dem man, sei es auf verbandlicher oder auf behördlicher Seite, unter Umständen schauen kann: Wie können wir da besser eingreifen?

Wenn ich angegriffen werde, dann ist Zeit das entscheidende Kriterium, um den Schaden einzugrenzen. Wenn ich dann zuerst den Hörer ergreifen und telefonieren muss, wo ich den Forensiker habe oder wen ich finde, der mir helfen kann, dann ist schon unwahrscheinlich viel in den Brunnen gefallen. Auch da wieder gilt: Die Großen können sich das leisten, genauso wie die Versicherungen. Die Großen erreichen die Standards, die Versicherungen heute haben wollen. Die kleinen Unternehmen können die Standards, die Versicherer haben wollen, gar nicht mehr abdecken. Insofern ist für mich das Thema klein/groß ein großes Thema.

Zum Thema Kosten für Lizenzen. Im Schnitt sind es, wenn man auf Standard-Office-Produkte oder so etwas schaut, meiner Einschätzung nach bei einem kleinen Unternehmen 10 bis 15 % mehr als bei einem großen Unternehmen. Ich habe auch schon höhere Preisunterschiede gesehen. Je nachdem. Das hängt einfach

von dem Volumen ab und davon, wie groß gebündelt wird. Das sind signifikante Unterschiede. – Ich hoffe, ich habe Ihre beiden Fragen ausreichend beantwortet.

SV Thomas Boele (Check Point Software Technologies GmbH): Zuerst zur Lizenzfrage. Die klare Antwort lautet: Es kommt darauf an. – Letztendlich beantworte ich das politisch korrekt. Wir vertreiben zu 100 % über Partner. Das heißt, die Preisgestaltung liegt bei den Partnern. Sternchen: Ich denke, man kann natürlich Skaleneffekte erreichen.

Ich habe ja eingänglich über MSSPs gesprochen. Ich denke, damit kann man eigentlich auch ziemlich viele Sachen abbilden.

Wie können sich KMU besser behandelt fühlen bzw. besser vorbereiten? Ich denke, da geht es wirklich darum, diese Dienstleistungen zu koppeln. Da gibt es Unternehmen, die wirklich einen 24/7-Dienst anbieten und dann im Prinzip alles machen können. Wenn ich mir heute irgendwelche anderen Dienste hole – E-Mails usw. –, das ist as a Service. Im Prinzip kann man Security auch as a Service machen. Das heißt, auch ein kleines Unternehmen kann von besseren Preisen profitieren, indem es sich über diese Sachen anschließt. Ich denke, das ist sicherlich ein wichtiger Bereich, um das Ganze sehr gut leistbar zu machen.

Bei uns geht es in der Regel darum: Man hat ein Produkt, und dort gibt es natürlich eine Funktionalität, die drauf ist. Je nachdem, welche Ausprägung man haben will, ist das mit unterschiedlichen Lizenzen verbunden. Wir sind eine Softwarefirma, so funktioniert das. Es ist auch Hardware dabei, aber das ist sicherlich der wichtigste Bereich. Wie gesagt, wenn man es alleine nicht schaffen kann, sucht man sich grundsätzlich einen vertrauensvollen Partner. Zwischendurch kam die Frage: Wie kann man damit umgehen? Wie kann ich feststellen, dass ich einen guten Partner habe? – Natürlich muss man gucken: Welche Kunden hat er? Hat er Referenzen? Kann ich mit denen sprechen? Kann ich als Kunde ein Referenzgespräch mit einem anderen führen und wirklich die Haube hochheben und feststellen, was in diesen Bereichen passiert? – Ich denke, das kann man sicherlich noch länger diskutieren, aber, wie gesagt, man kann an den Skaleneffekten teilhaben, wenn man einfach einen Partner nimmt, der einen großen Vertrag mit verschiedenen Herstellern hat.

Dazu gibt es die Theorie: Mache ich alles aus einer Hand, dann hat man wieder Abhängigkeiten. – Heute spricht jeder gerne von Plattformen und Cloud. Wichtig ist eigentlich, dass man eine offene Plattform hat, dass man unterschiedliche Sachen miteinander koppeln kann und letztendlich mit nicht zu vielen Anbietern arbeitet – ansonsten wird es unübersichtlich – und ein vernünftiges Security-Konzept aufstellen kann.

Frau Schack erbat noch einen Kommentar bezüglich KI und kleineren Unternehmen. In vielen Bereichen kann ich Foundation-Modelle nehmen, gerade wenn es um Transformer-Modelle geht. Die kann ich erwerben, die kann ich von verschiedenen Herstellern benutzen. Ich kann sie natürlich auch aus einer Public Domain kriegen.

Ich hatte neulich ein Interview zum Thema Jupiter, also zu dem High-End-Rechner, dem Exascale-Rechner, den man jetzt in Jülich aktiviert hat. Dort kann man natürlich auch Foundation-Modelle erstellen. Das Ganze ist mit europäischen und natürlich auch deutschen Forschungsmitteln finanziert. Dort kann man Foundation-Modelle holen und die spezifisch trainieren. In vielen Bereichen, gerade wenn es um Cybersecurity geht, sind die Muster ähnlich. Das heißt, ich brauche kein spezielles LLM, was Muster hat, die auf KMU abgestimmt sind. Dort kann man an dem, was draußen vorhanden ist, partizipieren.

Im Bereich GKV usw. wird man sicherlich demnächst KI-gestützte Bots zur Verfügung stellen, um eine saubere Deflection und einen sauberen Service für die Bürger zu haben. Da sollte man langsam darüber nachdenken: Okay, ich habe eine neue Box der Pandora geöffnet, weil dort natürlich auch Sicherheitsmaßnahmen ergriffen werden müssen. – Das Gute ist, man denkt darüber nach; es gibt Lösungen, die man in diesem Bereich verwenden kann, um einfach die Leitplanken der Kommunikation festzusetzen.

SV Bernd Geisler (LSI): Zum Thema "Lizenzen und Förderung". Mir sind keine Fördermaßnahmen bekannt, die das Thema Lizenzen betreffen. Das weiß ich nicht. Ansonsten kann ich mich den Einschätzungen zu den Kosten- bzw. Skaleneffekten, was das Ganze ausmachen könnte, wenn man sich zusammenschließt, den Vorrednern anschließen. Das ist auch das, was wir selbst als Lizenznehmer wahrnehmen. Ansonsten machen wir im Bereich Lizenzen nichts zentral für den Freistaat. Das läuft nicht über uns, aber wir beobachten das Ganze aus der Ferne, weil wir eben auch Lizenznehmer sind.

Zum Thema "Gefahrenpotenzial bei Energieversorgern". Ja, es gibt mit Sicherheit ein Gefahrenpotenzial. Für den Bereich Energieversorgung ist die zuständige regulierende Fachbehörde die Bundesnetzagentur. Das muss man an der Stelle ganz klar sagen. Die wird einen guten Überblick haben. Diesen Überblick haben wir als LSI nicht. Die Energieversorgung ist unser jüngster KRITIS-Bereich. Das haben Sie vielleicht aus einer Pressemitteilung mitbekommen. Dem haben wir uns sehr jüngst angenommen. Wir haben uns hier auf Wasserkraftenergieanlagen konzentriert. Davon gibt es in Bayern sehr, sehr viele, sehr kleine, die aber insgesamt doch 19, 20 % der Energieversorgung ausmachen und zu einem relativ großen Teil nicht die Regulierungsschwelle der Bundesnetzagentur überschreiten.

Für diese Einrichtungen haben wir letztlich Beratungsangebote erstellt. Die brauchen die auch. Das haben wir uns mit den zuständigen Branchenverbänden angeguckt. Das sind teilweise familiengeführte kleine Anlagen, die, ähnlich wie andere, mit sehr alten Steuerungstechniken ausgestattet sind, vielleicht sogar für eine Fernwartung von außen erreichbar sind. Dann haben wir wieder die Problematik: Ich kann das System von außen erreichen. Es ist unklar oder ungenügend abgesichert und möglicherweise störbar.

Wir haben auch schon Vorfälle im europäischen und internationalen Ausland gesehen, wo Angriffe auf solche Einrichtungen stattgefunden haben. In der Auswirkung muss man allerdings sagen, das ist im Moment marginal. Das ist mein Kenntnisstand. Also: Gefahrenpotenzial mit Sicherheit vorhanden, in der Realisierung bisher aber nicht aufgetreten. Wir unterstützen an der Stelle die kleinen bayerischen Energieversorger im Bereich von Wasserkraftanlagen. Das sind so 3.500, glaube ich, insgesamt.

Zum Thema PKW müsste ich jetzt nach links gucken, weil wir zur Absicherung von Kraftfahrzeugen allgemein und zur Vernetzung keine Informationen haben.

SV Marc Luczak (BMW Financial Services): Ich greife den Punkt gleich auf, auch wenn die Frage nicht an mich gerichtet war. Wir müssen uns in unserer heutigen Zeit vorstellen, ein Auto ist im Endeffekt ein fahrender Computer. Unheimlich viele Daten werden generiert, es werden unheimlich viele Daten aus dem Auto abgegriffen. Ja, und das Auto kommuniziert auch mit etlichen Endpunkten. Das heißt, das Auto ist tatsächlich ein Schadobjekt gegenüber Angriffen. Völlig klar. Wenn Sie neue Modelle fahren, willigen Sie in die Datenschutzbestimmungen ein. Auch da muss man genauer lesen, in was Sie da einwilligen, was mit Ihren Daten geschieht und wo die verwendet werden oder wer auf die Daten zugreifen kann. Das ist ein ganz kritisches Thema. Aber ja, das Auto ist wie auch andere internetbasierte Techniken – ich rede da von den weißen Haushaltsgeräten, dem Thermomix, dem

Kühlschrank usw. – mit dem Internet verbunden. Das sind Dinge, die uns im Alltag unterstützen, die aber auch Risiken bergen. Völlig klar. War das an der Stelle zufriedenstellend? – Ja.

Dann würde ich auf die beiden Fragen angehen, Herr Meier, die Sie gestellt haben. Was kann der Freistaat Bayern tun? Wir sind kurz vor Weihnachten, da kann man sich vieles wünschen. Wir haben das hier, glaube ich, relativ ausgiebig besprochen. Ich mag behaupten, dass große Unternehmen in Bayern – viele DAX-Unternehmen sind ja in Bayern ansässig – im Bereich IT-Sicherheit recht gut aufgestellt sind. Die Bedingungen haben wir heute schon mehrfach skizziert: Wir haben ausreichend Personal, wir haben das Budget dafür. – Natürlich gibt es den einen oder anderen Angriff, aber wir haben präventive Maßnahmen auf hohem Schutzniveau, die im Endeffekt den eintretenden Schaden relativ gering halten.

Ich will das an einem Beispiel deutlich machen, am Thema BCM/TCM, also Kontinuitätsmanagement. Ja, wir haben Transparenz über unsere kritischen Prozesse, und zwar kritische Prozesse in dem Sinne, die uns das Fortbestehen der Produktion gewährleisten. Die haben wir, und wir haben die auch häufig redundant abgesichert. Ich habe in meiner Eingangsrede von einem Rechenzentrum gesprochen, das teilweise auf Hot oder Cold Standby steht. Wir können da relativ schnell in einem Schadfall andere Systeme anschalten und haben eine Art Redundanz. Das alles ist dokumentiert in Notfallvorsorgekonzepten etc., etc. Da sind große deutsche Unternehmen recht gut abgesichert. Ich bin dazu auch häufiger im Austausch mit anderen in München ansässigen DAX-Unternehmen. Das passt.

Wo haben wir aber Nachholbedarf? Das sind die kleinen und mittelständischen Unternehmen. Ein Punkt ist hier noch nicht besprochen worden. Wenn ein Schadfall eintritt, dann ist der in kleinen Unternehmen häufig viel signifikanter als bei großen Unternehmen, und zwar so signifikant, dass wir über geschäftsschädigenden Ausfall sprechen. Teilweise kann das geschäftsbedrohlich sein. Wenn Sie eine Internetplattform für ein kleines oder mittelständiges Produktionsunternehmen haben und die drei, vier Tage nicht läuft, kann das durchaus kritisch für den gesamten Geschäftsbetrieb sein.

Ich habe den Wunsch, und das haben wir schon besprochen, dass wir eine Zusammenarbeit mit den Behörden haben. Ich stelle mir auch vor: Warum gibt es nicht wenigstens bayernweit so etwas wie ein zentrales CISOC, also ein Zentrum, was Sicherheitsvorfälle koordiniert, auch bekämpft – wir hatten das Thema Forensik –, und die Angriffe rechtlich dokumentiert, um das den Behörden zu übergeben? Das entlastet Kommunen, und das würde wahrscheinlich auch dem einen oder anderen kleinen und mittelständischen Unternehmen unter die Arme greifen.

Digitale Souveränität ist auch ein sehr spannendes Thema. Dabei geht es nur um den Sektor Cloud, den ich eingangs erwähnt habe, sondern auch um das Recht an meinen digitalen persönlichen Daten. Jeder von uns hat Social Media, jeder wird in Datenschutzbestimmungen einwilligen. Wir haben häufig gar keine Transparenz, und gehen sehr leichtfertig damit um. Heute wurde schon angesprochen, dass wir eine Awareness schaffen müssen. Digitalisierung ist immer Fluch und Segen. Wir geben eine Vielzahl von Informationen, von persönlichen Daten oder Unternehmensdaten an Akteure im Markt, wobei wir nicht wissen, was mit diesen Daten ganz genau passiert. Der Fall Cambridge Analytica dürfte jedem noch von vor einigen Jahren bekannt sein. Wir haben das Thema Palantir, etc., etc. Ich weiß nicht, was mit meinen Daten passiert.

Jetzt übertrage ich das einmal. Wir sind in einem fortschreitenden Prozess, das habe ich gesagt, On-Prem-Lösungen in die Cloud zu überführen. Ja, die Cloud

birgt natürlich enormes Potenzial. Wir haben hier eine skalierbare Infrastruktur, wir sind flexibel, wir haben natürlich auch im Business Case immer positive Effekte. Völlig klar.

Die negativen Effekte sind: Wir nutzen die beiden Cloud-Anbieter, die in Amerika sitzen. Das mag gutgehen, solange wir in der jetzigen Zeit leben. Geopolitisch weiß ich nicht, ob das zukunftsgerecht ist.

Digitale Souveränität ist ein großes Thema. Wir müssen das nehmen, was wir am Markt zur Verfügung haben. Ich weiß, es gibt eine Cloud der Telekom. Die ist aber, jedenfalls für deutsche Unternehmen, fast nicht relevant. Wir können nur das nehmen, was am Markt ist, und ja, das birgt Gefahren. – Hat das die Frage ausreichend beantwortet?

SV Norbert Radmacher (LKA): Ich möchte auf die Frage eingehen: Welche Unternehmen sind aus unserer Sicht besonders betroffen? – Das sind in der Regel kleine und mittelständische Unternehmen aus der Industrie und dem verarbeitenden Gewerbe, in Einzelfällen auch aus dem Finanzsektor.

Zur Frage der ausgewiesenen Schadenshöhe. In unserem Cybersicherheitsbericht 2024 sind 20,07 Millionen Euro ausgewiesen. Uns ist bewusst, das ist nicht der wirtschaftliche Gesamtschaden, der hier zu Buche schlägt. Das sind polizeiliche Daten, die für uns relevant sind. Wir erfassen hier ausschließlich den Beuteschaden. Das ist für uns relevant, wenn es um das Thema Vermögensabschöpfung bei den Tätern geht.

Nicht drin ist der wirtschaftliche Gesamtschaden für ein Unternehmen. Stichwort Wiederherstellung der Systeme. Aber auch der Ausfall der Lieferketten ist da natürlich nicht beinhaltet. Insofern bildet diese Zahl die Realität nicht vollständig ab. Ich denke, Sie kennen aber die Zahlen, die insbesondere Bitkom veröffentlicht. Das ist, denke ich, sehr valide.

Eine weitere Frage betraf die Regulatorik. Wir sind in Sachen Polizeirecht, Strafrecht, denke ich, sehr gut aufgestellt. Ein Fortschritt wäre, aber das gilt nicht nur für das Thema Cybercrime, sondern insgesamt für die Kriminalitätsbekämpfung, ist die verpflichtende Speicherung der IP-Adressen. Das ist eine Forderung, die in diesem Haus schon oft gehört worden ist, denke ich.

SV Josef Schinabeck (LFV): Zu den Fragen des Abgeordneten Köhler. Die Forderung des US-Senators von Cotton kenne ich leider nicht, und ich würde mich dazu auch nicht positionieren wollen. Aber ich kann Ihnen versichern, dass der Austausch mit den befreundeten Diensten bisher nach wie vor sehr gut funktioniert. Die Welt ist unsicherer geworden; da haben Sie Recht, und wir können uns vielleicht nicht mehr über die nächsten Jahrzehnte darauf verlassen, dass das alles sehr gut funktioniert. Aber für den Augenblick kann ich Ihnen versichern, dass es nach wie vor auf dem Niveau fortgeführt wird, wie wir es die letzten Jahre über erfahren haben. Das passt alles wirklich sehr gut. Wie gesagt, diese Forderung des US-Senators kenne ich nicht, und ich möchte mich dazu auch nicht positionieren. Wie sich das im Laufe der nächsten Jahre und Jahrzehnte weiterentwickelt, können wir nicht abschätzen. Aber sowohl auf Bundesebene als auch auf Landesebene funktionieren die Kontakte nach wie vor, und der Info-Austausch ist auf gewohntem Niveau.

Zu der Frage, wie die Organisation des LfV aussieht. Behörden müssen sich immer den Gegebenheiten und den Notwendigkeiten anpassen, auch was die vorhandenen Ressourcen betrifft. Sie wissen vielleicht, dass die reine Abteilung Rechtsextremismus im Bayerischen Landesamt für Verfassungsschutz nach den Geschehnissen um den NSU-Komplex entstanden ist. Damals war es eine politi-

sche Forderung, dass man sich hier mit einer reinen Abteilung für diesen Phänomenbereich anders organisiert. Das haben wir damals auch gemacht.

Wir haben dankenswerterweise im vergangenen Jahr 10 neue Stellen und in diesen Jahren 30 neue Stellen bekommen. Diese in der Gesamtschau 40 Stellen sind angesichts der politischen Notwendigkeiten fast alle in den Bereich der Spionageabwehr und der Cyberabwehr geflossen. Insofern sehe ich hier keine Schieflage, was die Organisationsform des LfV betrifft.

SVe Prof. Dagmar Schuller (IHK): Ich bedanke mich ganz herzlich für die Frage zum Thema KI-Daten und die Ansprache zu Unternehmen. Wir haben gerade schon gehört, es gibt Basismodelle, mit denen man an der Stelle schon arbeiten kann. Wesentlich ist aber, glaube ich, zu verstehen, dass wir hier nicht von Systemen sprechen, die ein bestimmtes Plateau erreicht haben und dann ist es gut, sondern wir haben hier ständig lernende Systeme. Das sieht man auch, was die Angriffe anbelangt, sehr klar. In verwandten Gebieten wie beispielsweise Fraud Detection muss man wirklich ständig am Puls der Zeit und der Forschung bleiben und daran arbeiten, bestimmte Gefahren zu erkennen, um effizient dagegen einwirken zu können. Da sind Daten und vor allem personenbezogene Daten ein sehr kritisches Thema, wo man in bestimmten Bereichen abwägen muss.

Aus unternehmerischer Erfahrung kann ich Ihnen sagen, Daten mit Personenbezug, wenn Sie beispielsweise in Richtung Medizin oder in andere Bereiche gehen, sind in Europa sehr, sehr schwierig in guter Qualität und ausreichendem Maße zu bekommen. Das hat natürlich auf der einen Seite den Schutzhintergrund der Regulatorik, auf der anderen Seite stehen entsprechende Maßnahmen oder Sanktionen gegenüber, wenn man bestimmte Datenschutzmaßnahmen oder Datenschutzvorkehrungen verletzt.

In der aktuellen algorithmischen Struktur der momentan hauptsächlich verwendeten Transformermodelle in der Technologie ist es nun einmal so, dass eine Menge nicht unbedingt homogener Daten, sondern idealerweise heterogener Datenstrukturen in ausreichend guter Qualität und in möglichst großer breiter Masse zu diesen Generalisierbarkeiten dieser Modelle geführt haben. Das ist einer der Gründe, warum wir hierzulande neben dem fehlenden finanziellen Hintergrund und den entsprechenden Tickets, die von der Venture-Seite nicht gelöst werden, nicht über eigene große Basismodelle verfügen. Ich spreche da ganz konkret Foundation-Modelle an, die wiederum zum Trainieren von anderen Foundation-Modellen verwendet werden. Das ist wirklich ein Punkt. Gerade, wenn man sich den verwandten Bereich mit Betrugsmanagement, Fraud System und Fraud Detection anschaut, muss man noch einmal sehr stark auf die behavioristische Komponente abzielen. Wenn ich vollautomatisiert betrugs- oder entsprechende sicherheitsrelevante Aspekte erkennen möchte, dann muss ich auf der anderen Seite das System dementsprechend lernen lassen, in welcher Art und Weise diese Ausprägungen passieren. Da sind wir noch einmal auf der architektonischen Seite von sicherheitsrelevanten Konzepten, die sehr stark menschenzentriert erfolgen. Ich kann nur dann tatsächlich sehr sinnvolle Abwehrmechanismen schaffen, wenn ich verstehe, wie diese Angriffe zustande kommen. Zu dem Thema gibt es sehr gute Forschung beispielsweise in der Ben-Gurion-Universität in Israel – Fraud Detection wäre hier noch einmal verwandt –, wo man versucht, ganz gezielt zu denken, wie beispielsweise dieser Angreifer denken würde und wie er sich diese Schwachstelle aussucht, um effizient seinen Angriff voll- oder teilautomatisiert durchführen zu können.

Diese Gebiete verschmelzen deutlich stärker. Wir denken beispielsweise an den Themenbereich der Sprachsynthese. Man bekommt vollautomatisiert den einen oder anderen Anruf, der klingt wie jemand, den man kennt, vielleicht sogar wie ein

Verwandter, und der behauptet, in einer Notsituation zu sein. Die kognitive Last überwiegt, man ist in einer Stresssituation und tut Dinge, die man normalerweise gar nicht tun würde, würde man rational an dieses Problem herangehen.

Gerade diese teilweise Nichtrationalität ist schwierig abzubilden. Was passiert im Nachgang, wenn es einem tatsächlich passiert ist? Man hat irgendwie Schuldgefühle, man möchte diesen Fehler auf keinen Fall breitgetreten wissen. Im Idealfall spricht man über ihn, aber sehr oft kommt auch vor, dass man ihn verschweigt. Daher kommt diese Dunkelziffer.

Um auf Ihre Frage zurückzukommen: Die Erhebung und das Training personenbezogener Daten sind für eine sehr konkrete, aber koordinierte und sichere Nutzung dieser Daten unerlässlich, um die Systeme weiter lernen zu lassen und deutlich zu verbessern. Hierfür braucht es eine entsprechende Struktur – auch regulatorisch. Wir können Datenschutz nicht gewährleisten oder beispielsweise Persönlichkeitsrechte nicht schützen, wenn wir an dieser Stelle nicht eine entsprechend koordinierte Nutzung ermöglichen.

Das ist natürlich immer eine emotionale Grauzone, aber es ist wichtig, sie zu diskutieren, offen anzusprechen und auch Reallabore zu schaffen, wo man diese Vorfälle ganz konkret trainieren kann, um diese Systeme weiterzuentwickeln.

Dazu ein kleiner Schwenkerle zu § 202 StGB, dem "Hackerparagrafen". An der Stelle ein ganz kleines Plädoyer für diejenigen, die tatsächlich proaktiv in dieses Schwachstellenmanagement gehen oder versuchen, diese Schwachstellen zu verorten und auch zu melden. Es kann nicht sein, dass man diese Personengruppen oder diese Unternehmensgruppen in eine strafbare Handlung zwingt. Das senkt die Motivation, etwas preiszugeben, wenn man etwas gefunden hat, natürlich deutlich. Das ist, glaube ich, nicht im Sinne dessen, wozu es eingesetzt werden sollte.

Was kann man machen, um noch stärker besser zu verorten, in welche Tendenzen es geht? Zusammenarbeiten, austauschen, Erfahrungswerte bewerten können und auch an der Stelle wirklich positiv, incentive-orientiert an diese Themen herangehen.

Zu Ihrer Frage, Frau Vorsitzende. Wie kommen wir dazu? Wie kann man liefern, dass man, wenn man zum Beispiel teilweise an Externe auslagert, einen höheren Schutz bekommt? Das ist an der Stelle einerseits eine Kennzeichnungsgeschichte. Deutlicher zu machen, dass tatsächlich bestimmte Kennzeichen oder Benchmarks eingehalten werden, ist für jeden in der Auswahl schon ein sehr positives Kriterium.

Dieses Benchmarking bringt mich noch einmal zurück zu Ihnen, Frau Schack. Was kann ich tun, um da weiterzuentwickeln? Benchmarking bedeutet, ich lege offen, inwieweit oder wie gut ich in bestimmten Bereichen tatsächlich eine Accuracy, eine Performance bei einem bestimmten Modell, bei einer bestimmten IT-Leistung oder einer Sicherheitsmaßnahme erreichen kann. Wenn wir beispielsweise diese öffentlichen Benchmarkdaten zur Verfügung stellen, damit man sich in der Forschung besser vergleichen kann, hat man aus dem Bereich wieder deutlich mehr gewonnen.

Ich habe deshalb die ganz große Bitte, wirklich noch deutlich stärker und intensiver im Austausch zusammenzuarbeiten und proaktiv auf ein positives Fehlermanagement hinzuwirke. Nur durch positive Fehlermanagement- und Lernerfahrungen kann man tatsächlich einen höheren Standard erreichen.

SVe Prof. Dr. Haya Schulmann (Goethe Universität Frankfurt): Ich fange damit an, welche Unternehmen besonders betroffen sind. Das hängt natürlich davon ab, welche Angriffe das sind. Unternehmen oder Organisationen sind unterschiedlich

betroffen. Die Frage ist, um welche Angriffe es geht. Wenn es um Diebstahl geht, merkt man es zum Beispiel oft gar nicht. Wir reden nur von Ransom. Solche Angriffe merkt man: Die Daten werden verschlüsselt und nichts funktioniert. – Aber Datendiebstahl oder Angriffe, die Ressourcen oder Reputationen von Organisationen ausnutzen, um Malware und Schadsoftware zu verbreiten und andere Angriffe durchzuführen, merkt man nicht. Bei den meisten Angriffen merkt man gar nicht, dass sie passieren.

Wenn es Ransom-Angriffe gibt, bedeutet das, davor gab es ganz viele andere Angriffe oder Schritte, die dazu geführt haben, dass die Angreifer alle Daten verschlüsseln konnten. Zum Beispiel wurden Zugangsdaten gelegt, die MFA wurde angegriffen oder andere Sachen in Organisationen wurden angegriffen; denn es braucht viele Schritte, um so einen komplexen Angriff durchzuführen. Das heißt, man kann diese Angriffe erkennen und verhindern, bevor sie passieren. Hier spielt Geschwindigkeit eine zentrale Rolle.

Ransom oder Denial of Service ist sehr sichtbar, weil dann die Dienste nicht erreichbar sind, und die Reputation ist dann sehr geschädigt. Aber es gibt viele Angriffe, und viele Unternehmen sind betroffen.

Welche Organisation das am häufigsten sind, ist schon gesagt worden. Das sind Kommunen, aber auch Parteien. Das sind nicht die Parteien im Bundestag, sondern in Ländern und Landkreisen. Sie haben ähnliche Strukturen wie Kommunen. Wenn man die IT anschaut, sind da viele Ähnlichkeiten. Das bedeutet, die brauchen zentrale Angebote, die brauchen Mindeststandards, und sie brauchen auch Verantwortlichkeiten. Oft gibt es keinen Verantwortlichen für den Server oder die IT, die läuft.

Von dem Hauptproblem Dritter, das wir in Deutschland und auch in Bayern sehen, sind auch große Unternehmen und Konzerne betroffen. Wenn Sie eine Webseite nehmen, sagen wir von der Automobilindustrie, so haben die viele Ressourcen und investieren ganz viel, aber natürlich bauen sie nicht alles selbst. Auf einer Webseite hat man ganz viele Komponenten von Dritten, zum Beispiel Zahlungen, zum Beispiel Chatbots, zum Beispiel Analytics. Das alles nehmen auch die großen Konzerne von externen Dienstleistern. Interessanterweise haben diese externen Dienstleister oft viel weniger Ressourcen als die großen Konzerne. Dadurch sind diese Konzerne angreifbar. Wir sehen viele Angriffe, auch in verschiedenen Sektoren in Bayern. Die Angriffe kommen über Dritte, über Lieferanten, über Hosting Provider, über Dienstleister, weil die nicht genug Ressourcen haben. Ich will keine Firma konkret nennen, aber ein Großkonzern, der Ressourcen hat und eine Webseite braucht, lagert das oft an eine Agentur aus oder macht es im Prinzip zwar selbst, aber macht trotzdem nicht alles selbst. Er wird viele Komponenten einkaufen, und die sind verwundbar. Das heißt, man braucht Mindeststandards auch für Dienstleister. Man muss schauen, wen man in der eigenen Infrastruktur hat. Diese Übersicht hat man nicht.

KI ist ein wichtiges Thema. Das wurde viel angesprochen und es stimmt. Wir brauchen in Deutschland aber nicht nur das Feintuning, sondern die Basismodelle. Für diese Modelle braucht man auch Expertise, Ressourcen und Infrastruktur.

In Deutschland trainieren wir zurzeit. Deutschland hat zwischen 70 und 100 Milliarden Parameter. Nur zum Vergleich: In den USA ist das 1 Billion. – Je größer die Modelle sind, desto mehr Kontext verstehen sie natürlich, und umso besser können sie Entscheidungen treffen und umso effektiver können sie sein. Natürlich werden auch wir in Deutschland immer Sachen verwenden, die besser funktionieren.

Interessanterweise können solche Modelle unsere Entscheidungen bewusst oder unbewusst sehr beeinflussen. Sie repräsentieren fremde Wertevorstellungen und haben sogar Definitionen für Sachen.

Wenn wir Modelle aus dem Ausland verwenden, also Basismodelle im Ausland trainiert wurden und wir das Feintuning machen, dann bringen wir natürlich diesen Einfluss in alle Bereiche Deutschlands hinein, von der Verwaltung bis hin zu Organisationen und Unternehmen. Das heißt, es ist sehr wichtig, dass wir in Deutschland auch diese Kapazitäten entwickeln.

Das bringt mich zur digitalen Souveränität. Wir sagen, wir müssen alles in Deutschland selbst machen. Dem stimme ich zu. Ich wäre total begeistert, wenn wir in einem Bereich, in einer Software oder in einem Produkt weltweit führend wären. Das sind wir leider nicht. Gesagt wurde schon, dass Deutschland die Sachen verliert, die es hier gab.

Jedes Mal wird gesagt: "Wir brauchen dies und auch das", aber wir können nicht alles haben. Wir können keine souveräne eigene Cloud in Deutschland bauen und KI in Deutschland bauen und Plattformen wie Palantir in Deutschland bauen. Das ist unmöglich. Wir haben nicht genug Ressourcen in Deutschland, wir haben nicht genug Expertise, wir haben nicht genug Geld. Das heißt, wenn wir so etwas sagen, verlieren wir eigentlich langfristig, weil wir keine Technologie haben werden, in der wir wirklich führend sind.

Wie sollen wir entscheiden, in welcher Technologie wir investieren sollen? Die Entscheidung soll risikobasiert sein; wir sollen eine Risikoabwägung machen. Sie soll auch zukunftsorientiert sein. Welche Technologie wird zukunftsprägend sein?

Was bedeutet risikobasiert? Palantir wurde erwähnt. Aber Palantir sitzt auf einem abgeschotteten Bereich und verwendet zurzeit keine KI. Es hat die Möglichkeit, KI zu verwenden, aber man kann eigene KI für Palantir verwenden. Palantir hat keinen Zugriff auf Daten, die die Polizei vorher nicht hatte. Palantir ermöglicht der Polizei oder den Behörden nur, die Arbeit effizienter zu machen. Wenn morgen die USA sagen: "Wir liefern keine Patches mehr für Palantir", dann ist das Risiko eigentlich nicht so hoch, weil es sowieso vom Internet getrennt ist. Uns über Palantir anzugreifen, ist nicht so einfach.

Wenn ich mir auf der anderen Seite Betriebssysteme, Cloudsysteme oder KI anschaue, sind die überall, und es ist sehr leicht, uns über diese Systeme zu beeinflussen und anzugreifen. Das heißt, wir sollten wirklich abwägen: Wo sind die größten Risiken, und wo sind die größten Chancen? – Dort sollten wir alle unsere Ressourcen investieren. Vielleicht wird Deutschland dann in fünf oder zehn Jahren führend in diesen Bereichen. Wenn wir irgendwo führend sind, dann haben wir Gegenabhängigkeiten. Das heißt, die ganze Welt kauft unsere Technologie und ist von uns abhängig. Das ist eigentlich wichtig und nicht Autarkie, weil wir dafür nicht genügend Ressourcen haben. Deshalb ist das vielleicht nicht die richtige Strategie, sondern, dass wir Gegenabhängigkeiten haben.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Vielen Dank. – Ich glaube, wir kommen zu unserer letzten Fragerunde, wenn ich auf die Uhr schaue. Wir haben auf der Redeliste den Kollegen Adjei, den Kollegen von Brunn und den Kollegen Beck. Gibt es weitere, die sich gerne noch einmal in diese Runde reinschmeißen möchten? – Das ist erst einmal nicht der Fall. Bitte, Benni, du hast ist Wort.

Abg. Benjamin Adjei (GRÜNE): Vielen Dank für die Ausführungen. – Ich würde zum einen noch einmal auf das Thema Data Governance eingehen, das gerade auch in Bezug auf die Frage von Jenny Schack angesprochen wurde. Wir reden jetzt immer davon, Daten zum Training von Modellen zu benutzen. Dann ist genau

die Frage: Wie schafft man es, dass Unternehmen an die Daten kommen oder die Daten tauschen können? – Es gibt Möglichkeiten, dezentrale Datenpools wie beispielsweise Federated Learning oder andere Technologien einzusetzen, um auf große Modelle zu trainieren und gleichzeitig die eigenen Daten nicht hergeben zu müssen.

Für BMW ist das sicherlich etwas anderes als für einen Handwerksbetrieb. Welche Möglichkeiten sehen Sie besonders für die kleinen Unternehmen, Frau Schuller, als IHK oder Handwerkskammer oder Staat Strukturen aufzubauen, um solche dezentralen Datenaustauschpools bereitzustellen und das Ganze auch sicher zu gestalten? Wenn man das alle kleinen Unternehmen selbst machen lässt, dann haben wir natürlich wieder ganz viele verschiedene Angriffsvektoren, die damit aufgemacht werden.

Angriffe finden, das haben Sie auch gesagt, noch sehr stark personalisiert oder durch Menschen statt. Das verändert sich jetzt. Wir haben jetzt den ersten Angriff, der dokumentiert – ich habe es mir im Detail nicht angeschaut – vollautomatisiert stattgefunden hat, also wo die KI selbst die eigene Angriffsstrategie entwickelt, den Angriff durchgeführt und abgeschlossen hat und bei dem Menschen gar nicht mehr beteiligt waren. Bisher nutzen wir KI häufig eher so, dass man sich beraten lässt. Das verändert natürlich die Skalierbarkeit von solchen Angriffen.

Frau Schulmann, welche Probleme sehen Sie durch diese Veränderung der Skalierbarkeit, dass ich in Zukunft nicht mehr an der Ressource Mensch, sondern nur noch an der Rechenkapazität begrenzt bin? Inwieweit geht das jetzt schon die Wissenschaft mit ein, dass man sich auch da vielleicht neue Verteidigungs- und Abwehrstrategien überlegen muss? – Sie haben ja gesagt, dass KI jetzt schon Sprache generieren kann und selbstständig Fake-Anrufe produzieren könnte.

Die dritte Frage geht an Frau Schuller und Herr Boele, es ging jetzt mehrfach um das Thema Standardisierung. Wir diskutieren das immer aus zwei Richtungen. Auf der einen Seite gibt es die Bürokratie, wenn ich zum Beispiel die ISO 27001 nehme. Die ist Standard. Die einen lieben sie, die anderen hassen sie. Ich glaube, wir brauchen für eine gute IT-Sicherheit gute Standards. Die müssen aber irgendwie praktikabel und müssen umsetzbar sein. Am Ende müssen alle diese Standards einhalten können. Was sehen Sie für uns als Staat an Möglichkeiten, diese Standards aufzubauen? Was für ein Gremium, was für Organisationen sollten solche Standards aufbauen? Wir diskutieren jetzt in Bayern sehr stark darüber, die Standards sehr stark abzuschwächen und abzuschaffen, was sicherlich am Ende nicht zu mehr IT-Sicherheit führt.

Abg. Florian von Brunn (SPD): Ich bin etwas spät, aber es ging aufgrund der Reihenfolge nicht anders. Ich habe eine Nachfrage an den Herrn Geisler zum Behördennetzwerk. Mich würde interessieren – Sie müssen nicht die Namen nennen –, wie viele unserer Landkreise nicht im Behördennetz sind.

(Zuruf: Fünf!)

– Fünf okay.

Sagen Sie mir bitte auch, wie viele unserer bayerischen Kommunen nicht drin sind.

(Zuruf)

Dann würde mich interessieren, wie viel ein Beitritt einer Kommunen im Durchschnitt kostet und wie dieser Anschluss an das Landratsamt technisch funktioniert. Vielleicht können Sie das grob umreißen, ohne in schwierige Details zu gehen.

Abg. Tobias Beck (FREIE WÄHLER): Ich habe noch zwei Fragen. Die eine geht in Richtung Datenspeicherung. Wo sehen Sie die Chancen und Risiken von lokalen Datenspeichern und von Cloud-Datenspeichern?

Ich bin ein großer Fan von Bandspeicherungen, also Tagessicherungen auf Band, weil ich das früher gern gemacht habe. Hat das Ihrer Meinung nach Zukunft, oder kann das in Zukunft wegfallen?

Meine letzte Frage ist, glaube ich, für uns alle interessant. Sie betrifft biometrische Daten. Am iPhone oder anderswo kann man sich durch Gesichtserkennung authentifizieren. Ich bin da sehr skeptisch. Ich habe, wie die meisten, zehn Finger, zwei Augen und ein Gesicht. Wenn diese Daten einmal abgegriffen sind, habe ich keine Chance mehr, das einzufangen. Wie sehen Sie da die Chancen und Risiken? Kann man das so einfach an der Masse testen, oder sollte man da sehr vorsichtig agieren?

Vorsitzende Stephanie Schuhknecht (GRÜNE): Danke schön. – Ich möchte noch einmal an meine ursprüngliche Frage zum Cyberschutzschirm für den Mittelstand erinnern. Falls jemand dazu in dieser letzten Runde noch etwas sagen kann, wäre ich sehr dankbar.

Ich würde sagen, wir fangen einfach noch einmal ganz von vorne an und machen jetzt die letzte Runde. – Herr Blumberg, Sie dürfen wieder anfangen.

SV Holger Blumberg (KRONES AG): Ich glaube, ich gebe das Wort direkt weiter, weil keine der Fragen direkt an mich adressiert war.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Das ist auch sehr gut, wenn Sie das so machen. – Herr Boele.

SV Thomas Boele (Check Point Software Technologies GmbH): Die Frage bezog sich auf die Standardisierung. Ich denke, da müssen wir zwei Ebenen unterscheiden. Das ist sicherlich die administrative und die regulatorische Ebene. Es gibt natürlich auch die technische Ebene, die für mich aus Herstellersicht interessanter ist. Wenn Sie weiter zurückgehen, haben Sie sicherlich solche Geschichten wie Ethernet. Das ist auch mal vom IEEE standardisiert worden. Das Gleiche gilt für WLAN. Hier geht es wirklich darum, Plattformen zusammenzubringen. Heute macht man das meistens über RAPIs und einem bisschen Aufwand und Programmierung. Wir werden draußen nicht unbedingt immer den gleichen Hersteller finden, sondern es gibt die unterschiedlichsten. Jede Firma kommt von irgendwo, hat ihre Prinzipien und möchte Funktionen hinzugestalten. Das heißt, dort brauche ich Möglichkeiten, um auf legalem und sauberem Wege Daten auszutauschen. Wenn ich einen Breach habe, wenn ich im Prinzip einen Zero-Day-Angriff finde, muss der andere darüber Bescheid wissen. Im Prinzip gibt es unter den Herstellern einen Kodex, dass man sich, wenn man etwas Kritisches findet, darüber informiert und Bescheid gibt. Aber das Ganze kann man natürlich auch offiziell mit standardisierten Schnittstellen machen.

Im Bereich der Regulatorik bzw. Strategien könnte man gucken: Welchen Katalog habe ich, den ich anwenden kann? – Ich habe eben schon gesagt, Zero Trust ist von BSE gefolgt und ist auch ein NIS-Standard. Wir haben eine Lockheed Martin Intrusion Killchain Prevention und ähnliche Methodiken. Den Leuten muss klar sein: Welche Methodiken habe ich, die ich anwenden kann, um sie letztendlich auch umzusetzen?

Der Bereich KI sollte natürlich auch betrachtet werden. Wir haben jetzt sehr, sehr viel über Transformermodelle gesprochen. KI wird eingesetzt. Ich denke, BMW wird das auch in den meisten Prozessen einsetzen. Das sehen wir durch die Bank in allen Kundengesprächen, die wir haben. Dort sollte im Rahmen dieser Tätigkeit festgeschrieben werden: Wie kann ich Informationen gesetzlich konform austauschen, damit die Systeme wissen, was passiert? – Sicherlich muss man auch festlegen: Welche Grenzen muss man diesem System setzen, und wie kann man das umsetzen?

Gerade gab es noch die Frage bezüglich lokaler Speicher versus Cloud-Speicher. Das ist immer eine Frage des Geldes, was man hat. Cloud bringt Agility. Das heißt, man kann sehr, sehr schnell Prototypen umsetzen und Dinge ausprobieren; man kann sich relativ einfach ein sekundäres Rechenzentrum einsetzen.

Grundsätzlich ist einfach wichtig, wie man auch einem ursprünglichen Papier aus den 2000ern der Berkeley University entnehmen kann, man sollte sich nicht als Geisel von einem einzelnen Cloud-Anbieter nehmen lassen. Das heißt, man sollte die Sachen so designen, dass man sie portieren kann und weitertransportieren kann, falls jemand sich einmal überlegt, dass man den Datenzugriff abdreht. Siehe WikiLeaks. Plötzlich war das erste Mal der Amazon Cloud-Speicher nicht verfügbar.

Das Band gibt es nach wie vor. Wenn Sie den Cold-Memory von einigen Cloud-Providern nehmen, wird das irgendwann von Band geholt, weil das nach wie vor funktional ist. Ich kann sehr, sehr viele Daten ablegen. Das gilt natürlich für Daten, die länger einen Wert haben. Wenn ich eine Datenbank habe und ich ein aktives Speicherlock brauche und das von vor zehn Tagen hole, ist die Datenbank kaputt. Wenn Sie in Hochregallager haben und der Stand von vor zehn Tagen wiedergegeben wird, dann ist wahrscheinlich eine Katastrophe eingetreten.

Das heißt, man muss wirklich den Bereich der Datensprecher so betrachten, dass ich eine vernünftige Backup- und Recovery-Strategie habe. Jeder spricht von Backup, denkt aber nicht darüber nach, zwischendurch auszuprobieren, ob ich meine Daten zurückspielen kann und ob ich die richtigen Daten sichere.

Wir haben viel über Ransomware gewonnen. Da gibt es das Stichwort des Immutable Backups. Das heißt, dass ich Speicherabbilder ziehe, beziehungsweise Snapshots von einem System ziehe, die nicht verändert werden können. Viele Angreifer haben heute zum Ziel, diese Systeme zu finden und natürlich auch das Backup abzudrehen. Das ist sicherlich sehr wichtig. Wenn wir über Daten und KI sprechen, geht es auch darum, dass sich ein vollkommen neues Feld erschließt, wo ein Angriff stattfinden kann. Man merkt es oft nicht, wenn beispielsweise Daten vergiftet werden. Das heißt, man muss sicherlich auch überlegen: Welche Daten spiele ich ein? – Es gilt das Stichwort "Garbage In, Garbage Out". Das heißt, man soll die Daten sauber konditionieren. Man sollte auch prüfen, ob diese Daten nicht auf dem Weg verfremdet werden, sodass mein KI-Modell plötzlich Ergebnisse liefert, die einen Angreifer günstig stimmen.

Nach statistischen Untersuchungen kann man bei 1 % fehlerhafter Daten bis zu 30 % falsche Ergebnisse bekommen. Das geht relativ schnell. Das heißt, hier ergeben sich neue Felder. Stichwort Standardisierung, verstehen, um was es geht, das Problem definieren können, die Sachen zusammenbringen.

In einer sehr guten Studie von IBM werden die Kosten von Data Breaches bzw. Cybervorfällen weltweit untersucht. Die neueste Studie ist gerade herausgekommen. Der Durchschnittswert beträgt 4,4 Millionen US-Dollar. Man kann sich dann das aufs eigene Unternehmen herunterrechnen.

In einem anderen Paper der Uni Maryland wird auch Cybersecurity als Investment betrachtet. Wenn ich die gesamten Kosten reinvestiere, ist es nicht effizient, aber es gibt einen idealen Wert, den man in Cybersecurity investieren kann, um einen optimalen Yield zu bekommen. Ich denke, es ist sicherlich wichtig, dass man das betrachtet.

SV Bernd Geisler (LSI): Ich will ganz kurz noch einmal das Thema automatisierte Angriffe aufgreifen. Wir sehen diese automatisierten Angriffe sehr deutlich. Zwei Zahlen dazu: Wir hatten im vergangenen Jahr an das Bayerische Behördennetz gerichtet rund 390 Millionen schadhafte E-Mails. Stand September dieses Jahres sind wir schon bei 700 Millionen schadhaften E-Mails, die wir erkannt und nicht weitergeleitet haben. Da erkennt man ganz deutlich, dass hier eine hohe KI-unterstützte Automatisierung dahintersteckt. Das passiert tatsächlich.

Noch kurz zum Thema Standardisierung, Grundschutz oder ISO. Das BSI entwickelt derzeit den Grundschutz++. Wir sind in Arbeitsgruppen beteiligt und versuchen, hier bayerische Positionen einzubringen und das Ganze handhabbarer zu machen. Ich gebe Ihnen recht, das ist mitunter zum Teil sperrig. Trotzdem und in der Summe, glaube ich, muss man es machen. Das ist sehr hilfreich.

Zum kommunalen Behördennetz. Tagesformabhängig fünf, sage ich mal. Das war mein letzter Stand. Es mag sein, dass es jetzt weniger sind. Ich hoffe nicht, dass einer das Ganze wieder aufgegeben hat. Das ist natürlich auch möglich.

Dazu, wie viele Kommunen tatsächlich teilnehmen, habe ich keine verlässlichen Zahlen, weil die Anbindung der Kommunen letztlich über VPN-Anbindungen in die Landkreisämter erfolgt, die die Landkreise selbst einrichten, aufbauen und unterhalten müssen. Dazu haben wir keine Informationen.

Wichtig in dem Zusammenhang wäre zumindest uns als LSI: Wer an so einem kommunalen Behördennetz teilnimmt, soll bitte den eigenen Internet-Breakout abschaffen. Das ist letztlich das Gefahrenpotenzial: der Eintrag von Schadcode, der hier noch durchaus möglich ist und auch nicht unserer Überwachung unterliegt. Der lokale Breakout wäre praktisch ungeschützt, zumindest von uns. Darum muss man sich wieder selber kümmern. Wenn alles über das kommunale Behördennetz läuft, dann geht das über den zentralen Internetübergang, und wir haben hier die volle Schutzfunktionalität.

Gefragt wurde nach den Kosten. Es kommt darauf an. Es kommt auf die Güte, die Bandbreite und darauf an, was man gerne vereinbart hätte, also letztlich auf die Verfügbarkeit. Mit Bycom gab es 2024 eine sehr sinnvolle Weiterentwicklung. In dem alten Vertrag, das wissen Sie vielleicht, hat man noch einen Baukostenzuschuss berechnet. Wenn ab einer gewissen Bandbreite Glasfaser verlegt wird, hat man pro Meter oder Kilometer, ich weiß es nicht genau, einen Zuschuss zahlen müssen. Das war sehr teuer für alle Beteiligten. Dieser Zuschuss ist weggefallen. Jetzt sind wir wieder auf allgemeine Regelungen, also Bandbreite, Verfügbarkeit usw., gegangen.

Insgesamt ist es natürlich nicht mit den Kosten für einen Privatanschluss vergleichbar, also mit den 19,99 Euro oder den 39 Euro von der Telekom. Nein, bei Weitem nicht. Da reden wir schon von mehreren Hundert bis zu mehreren Tausend Euro, je nachdem, wie viel Bandbreite und welche Verfügbarkeit ich möchte. Das sind dann die KSS-Tüten, die im Bycom-Rahmenvertrag vereinbart sind. Das liegt beim IT-DLZ. Da kann man sich erkundigen. Ich habe jetzt nicht parat, was es wirklich kostet, aber wir fangen schon bei mehreren Hundert Euro an und dann steigen die Preise, je nachdem, wie bandbreitig und welche Verfügbarkeit gewünscht wird.

SV Marc Luczak (BMW Financial Services): Ich möchte noch auf zwei Punkte eingehen. Herr Beck, Sie haben gerade biometrische Daten angesprochen. Ich will das ein bisschen aufgliedern, weil wir ein ähnliches Thema auch in der Industrie haben. Die digitale Souveränität, die Frau Prof. Schulmann angesprochen hat, ist uns eine Herzensangelegenheit. Sie haben gesagt, Deutschland ist da abgehängt. Okay, wir sind vielleicht nicht Weltmarktführer in bestimmten Systemen, in bestimmten Bereichen, in gewissen Forschungsthematiken. Dennoch ist das elementar wichtig; denn das ist im Endeffekt die Enabling Function für viele Produktionsprozesse, die wir haben. Gerade Bayern ist immer noch ein Produktionsstandort Nummer eins in Deutschland. Da sehe ich schon, dass eine gewisse digitale Souveränität Unabhängigkeit schafft und sogar auch einen Wettbewerbsvorteil bringt.

Das verknüpfe ich jetzt noch einmal mit den biometrischen Daten. Genauso wie bei der digitalen Souveränität, die ich dann habe, wo ich in meinen Cloudräumen spielen kann, wo ich entscheide, welche KI ich einsetze, wo ich weiß, wie die Daten genutzt werden, wer sie liest und wer Zugriff hat, kann man das auf den privaten Sektor übertragen. Ich bin manchmal recht schockiert, in welcher Form Awareness nicht stattfindet. Das typische Beispiel der Schwachstelle sitzt meistens 60 cm vorm Bildschirm. Wir geben leichtfertig Daten preis und ab. Ich rede nicht nur von Social Media. Ich rede auch von alltäglichen Gebräuchen. Wir müssten uns wieder viel mehr ins Bewusstsein rücken, dass alle Daten, die ich habe, und Informationen über mich, ob das Gesundheitsdaten sind, ob das Daten sind, wo ich mich bewege, wann ich wo einkaufe, ein schützenswertes Gut sind. Ja, man kann viele, viele Handlungsfelder daraus ableiten, aber nicht nur in gutem Sinne. Beides sehe ich im Endeffekt auch in der Verantwortung der Politik, hier gewisse Rahmenbedingungen zu schaffen, die sowohl auf dem privaten Sektor als auch bei den Unternehmen unterstützen.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Vielen Dank. – Herr Radmacher, möchten Sie noch einmal?

SV Norbert Radmacher (LKA): Ja, vielen Dank. – Ich möchte auch noch einmal auf biometrische Daten zu sprechen kommen und Sie in Ihrer Besorgnis unterstützen. Auch aus unserer Sicht sind das natürlich absolut schützenswerte Daten, und wir sehen leider, dass unser kriminelles Gegenüber keinerlei Skrupel hat, solche Dinge zu nutzen. Die sind technisch auf der absoluten Höhe der Zeit. Das ist eine besondere Verpflichtung für all diejenigen, die mit solchen Datensätzen umgehen.

Wir beobachten mit großer Sorge, was auch KI-generiert möglich ist, wenn man entsprechende Daten hat. Unser Gegenüber muss sich an keinerlei Regularien halten. Die sind in der Regel auch durchaus technisch auf der Höhe der Zeit und haben gewisse finanzielle Möglichkeiten. Nur als Beispiel: Wir haben letztes Jahr – Gott sei Dank nicht in Bayern, nicht in Deutschland – international den ersten Fall erlebt, da ist eine CEO-Fraud aufgegangen, indem ein KI-generierter Avatar an einer Videoschalte im asiatischen Raum teilgenommen und mehrere Millionen Euro angewiesen hat, die dann auf ein inkriminiertes Konto gezahlt werden konnten. – Das ist Technik, die unser Gegenüber nutzt. Das müssen wir wissen, und da müssen wir dranbleiben.

SV Josef Schinabeck (LFV): Noch einmal ganz kurz zum Thema Prävention. Ich habe in meinem Eingangsstatement relativ ausführlich dargestellt, dass die bayerischen Behörden schon ziemlich viel machen, was Prävention betrifft und was Awareness bei den Firmen betrifft. Aber offenbar sind wir noch nicht in allen Ecken angekommen. Das hat auch die Kollegin von der IHK hier dargestellt. Insbesondere bei kleinen und mittelständischen Unternehmen werden die richtigen

Adressaten noch nicht angesprochen. Insofern kann ich nur für uns werben, dass die Politik uns weiterhin die notwendigen Mittel und Ressourcen bereitstellt, damit wir unseren Aufgaben hier besser und verstärkt nachkommen können.

SVe Prof. Dagmar Schuller (IHK): Dann mache ich mit diesem Bereich weiter. Ich kann das, was Herr Schinabeck gesagt hat, nur noch einmal unterstützen. Die entsprechende Ausstattung der Behörden ist natürlich auch schlussendlich für die Wirtschaft extrem wichtig, weil man hier als Allianz auftreten muss und wirklich für den Austausch kompetente Partner auf beiden Seiten braucht, um tatsächlich noch dazuzulernen.

Zum Cyber-Schutzschirm für den Mittelstand noch ganz kurz. Ich habe hier ganz konkret keine Zahlen seitens der IHK vorliegen. Wir machen aber mit dem Innenministerium und mit unterschiedlichen behördlichen Stellen einen Cybersecurity-Tag, zu dem wir insbesondere unseren Klein- und Mittelstand einladen, um aktiv diesen Austausch nicht nur zu fördern, sondern auch diese Zugänglichmachung noch einmal zu demonstrieren, damit wir die Personen und entsprechende Ansprechpartner vor Ort haben, sodass sich auch klein- und mittelständische Unternehmer trauen, von sich aus diesen Kontakt aufzunehmen. Ich glaube, diese Art von Veranstaltungen müssen wir noch deutlich stärker intensiviert durchführen.

Nun zu den anderen Themen. Datenaustausch und was könnte man an der Stelle machen? Ich beginne gesamtwirtschaftlich. Es gibt Bestrebungen in diesem Bereich, vor allem Wettbewerbsvorteile zu heben, die wir hierzulande in Europa, speziell aber auch in Deutschland vor allem im Bereich der mittelständischen Industrie haben. Das hat mit Cybersecurity nicht primär etwas zu tun, aber vielleicht sekundär in der zweiten Nachdenkwelle. Insbesondere geht es darum, dass wir beispielsweise wirtschaftlich sehen, dass die Fertigungen oder die Produktionen von High Volume eher in Low-Volume-High-Mix-Varianten gehen. Gerade da sehen wir besondere Potenziale, wenn sich mittelständische Unternehmen, die sich spezialisiert haben, in diesem Bereich durch entsprechende Datenforen oder Datenplattformen austauschen können.

Das birgt natürlich immer, und das muss man wirklich sagen, das Risiko: Gebe ich Geschäftsgeheimnisse raus? – Aber wenn wir wieder zurück zur Struktur der Generalisierung entsprechender Modelle kommen, die adaptiv für solche Herausforderungen zugeschnitten werden können, hat man natürlich auch die Möglichkeit, eventuell ein Potenzial zu heben und sich wirtschaftlich so zu positionieren, und da komme ich zu dem zurück, was Kollegin Schulmann gesagt hat, dass ich in der einen oder anderen Variante einen sehr spezifischen Wettbewerbsvorteil für die entsprechenden Länder oder in dem Fall die entsprechende Wirtschaftskraft schaffe. Das heißt, die Strukturen zu einem Datenaustausch sind an sich gegeben.

Warum haben wir dann diese Daten nicht, oder warum tauscht man sich an dieser Stelle nicht aus? Wenn es um maschinenbezogene Daten geht, hat man hier vielleicht einen leichteren Zugang; wenn es um personenbezogene Daten geht, wird man sich hier deutlich schwerer austauschen können. Beides ist aber notwendig, um diese Plattformen aufbauen zu können.

Warum macht die IHK das nicht? Könnte sie das nicht machen? Primäre Aufgabe der IHK ist an der Stelle nicht, diese Plattformen zur Verfügung zu stellen, sondern in diesen wirtschaftlichen Austausch zu gehen. Aber man könnte natürlich andenken, unterschiedliche Akteure, die in diesem Bereich zusammenarbeiten, zusammenzubringen, um für diese Arten von Plattformen und Datenaustausch zu werben.

Beim Datenaustausch muss man, und das haben Sie vollkommen richtig gesagt, nicht immer auf Rohdaten zurückgreifen. Oft helfen an dieser Stelle sogar die

Signifikanzen, die man in den entsprechenden Datenbereichen erkennen kann, um auf Basis dessen entsprechende Modelle zu trainieren.

Das heißt, hier ist wirklich sehr viel Potenzial. Hier sollten wir eine sehr positive Struktur schaffen, um weiter in den Austausch zu gehen und sehr konkret die Möglichkeiten – idealerweise auch gesetzlich – durch Incentive- und Förderstrukturen unterlegen. Was meine ich mit Incentive- und Förderstrukturen oder Incentive-orientierter Politik an dieser Stelle? Da muss es nicht unbedingt das eine oder andere Förderprogramm geben, wo man Fördergelder abruft oder sich für ein Forschungsförderprogramm bewirbt, wo es dann doch etwas länger dauert, bis es tatsächlich zur Zuteilung dieser Fördermittel kommt und auch in der Abwicklung kompliziert ist, sondern es braucht hier sehr niederschwelligen Zugang.

Niederschwellig bedeutet kurzfristige kleinere Aktionen, die im Grunde genommen von staatlicher oder behördlicher Seite eventuell auch komplett unterstützt werden: Austauschmöglichkeiten, Hackathons, Benchmarking, digitale Möglichkeiten, diese Daten tatsächlich zur Verfügung zu stellen und ein entsprechendes Feedback zu bekommen, was das tatsächlich gebracht hat. – Das ist auch noch sehr oft etwas, was in der Wirtschaft gerade bei kleinen und mittelständischen Unternehmen noch nicht so oft ankommt: "Was bringt es mir, wenn ich das oder jenes umsetze oder wenn ich in dieser Art und Weise partizipiere?", weil ich immer diese Zeit- und Aufwandskomponente an dieser anderen Stelle im Hintergrund habe und vielleicht nicht die eigene Forschung oder die eigene Abteilung, die sich mit diesen Themen auseinandersetzt.

Zum Thema Standardisierung. Dazu haben die Vorredner schon sehr viel gesagt. Zum Thema Standardisierung wäre mir noch etwas wichtig. Wenn wir über entsprechende Normen, Benchmarks und Standards sprechen, dann ist natürlich wichtig, dass diese in entsprechender Form auch eingehalten werden. Wenn wir in den Zertifizierungsprozess gehen, beispielsweise im Themenbereich KI-Verordnung oder bei anderen Themen oder Produkten, die in dem Bereich mit Zertifizierungsprozedere behaftet sind, dann müssen wir gerade auch bei kleinen und mittelständischen Unternehmen ein Umdenken anstoßen. Bei diesen Prozessen reden wir nicht von zwei Wochen und dann sind sie durch. Meistens sind es 18 bis 24 Monate mit einem erheblichen Aufwand, der sich nicht in einem vierstelligen oder fünfstelligen, sondern zumeist in einem sechsstelligen Bereich bewegt. So geben wir auch diesen Unternehmen die Möglichkeit, zu partizipieren und diese Sicherheitsleistungen einzustellen. An der Stelle bitte ich auch wieder um eine incentive-orientierte, förderwillige Politik, weil es sonst in der Breite an der Stelle nicht so gut umsetzbar sein wird. Standardisierung lebt eben auch davon, dass man dieses Standards einhält und in der Breite in den Transfer bringt.

Zum Thema Transformermodelle möchte ich noch ganz kurz einen kleinen Schwenk machen, weil ich glaube, es ist ganz wichtig, in der technologischen Entwicklung etwas zu verstehen. Wenn ich von künstlicher Intelligenz spreche, spreche ich nicht von etwas, was von heute auf morgen passiert ist. Das erste Neuron wurde bereits im Jahre 1943 deskriptiv dargestellt – das McCulloch-Pitts-Neuron – und hat sich nicht von heute auf morgen entwickelt, sondern hatte einen längeren Prozessschritt. Die Transformermodelle, die momentan kommerziell, aber auch in der Forschung hauptsächlich eingesetzt werden, sind insbesondere durch ein sehr wesentliches Zusammenspiel, und das ist wichtig zu wissen, überwiegend industriell erforscht worden und weniger universitär oder akademisch.

Bei den Grundlagen handelt es sich, wenn wir von KI reden, immer um drei Fragen, die ich beantwortet haben muss: "Welche Art von Algorithmus habe ich? Wie wurde der trainiert und auf Basis welcher Daten?", damit ich überhaupt einschät-

zen kann, was ich an dieser Stelle vor mir habe. Gerade im Bereich der Algorithmik tut sich unglaublich viel. Sehr viele Modelle oder sehr viele algorithmische Ansätze wie zum Beispiel das an der TU München sehr stark entwickelte Long-Short-Term-Memory-Modell sind ein Revival. Wir haben Diffusionsmodelle oder algorithmische Ansätze in diesem Bereich, die insbesondere in der Bildgenerierung extrem performant sind, so dass wir uns nicht auf singuläre algorithmische Bereiche fokussieren können, sondern ein offenes Denken in diesem Bereich brauchen.

Transformermodelle haben beispielsweise, und das wissen wir alle, den Nachteil einer sehr hohen Rechenleistung, je nachdem mit wie vielen Prompts oder Token ich agiere. Wenn wir von vollautomatisierten Angriffen oder anderen Dingen sprechen, haben wir im Hintergrund auch noch energetisch eine entsprechende Leistung, die von der Forschungsseite her immer deutlich performanter abgeglichen werden will. Das heißt, es wird sich auch in der Algorithmik noch einiges tun. Wir sind hier nicht auf einem Plateau, sondern das wird sich in den nächsten fünf bis zehn Jahren entwickeln.

Wenn wir jetzt zur Standardisierung zurückkommen, müssen wir diese Standardisierung zwingend aufgrund dieser Dynamik halbwegs anpassbar offenhalten. Das heißt, wir können nicht irgendwann sagen: "Jetzt haben wir diesen Standard, und der gilt für die nächsten 15 Jahre", weil er eventuell für die nächsten 15 Jahre gar nicht mehr so relevant ist. Das ist das Wesentliche im Umdenken mit dieser Dynamik in dieser Entwicklung. An der Stelle nehme ich noch einmal das Beispiel KI. Wir können uns nicht darauf verlassen, dass Dinge, wenn wir sie einmal verabschieden, die nächsten 10, 15, 20 Jahre einfach so sind wie sie sind, weil sich dieser forscherische Bereich sehr dynamisch entwickelt.

Die Herausforderung auch im Bereich der Regulatorik ist, zu versuchen, und das ist nicht immer leicht, diese dynamische Denkweise auf diese Gegebenheiten anzupassen, damit ich flexibel auch mit den technologischen Hintergründen reagieren kann, die sich im Zweifel schneller verändern als ich das legislativ umsetzen kann.

Wie gesagt, gerade, wenn ich mir das Thema Standardisierung oder Datenaustausch anschaue, ist das etwas, etwas wo wir einfach offener in diesem Austausch sein müssen. Deswegen braucht es diesen Austausch so dermaßen intensiv. Ich kann das nicht oft genug betonen; denn nur dadurch können wir uns weiter in dem Bereich besser aufstellen.

SVe Prof. Dr. Haya Schulmann (Goethe Universität Frankfurt): Die Themen hängen eigentlich ein bisschen zusammen. Der Einsatz von KI hängt vom Zugriff auf die entsprechenden Trainingsdaten ab. Diese fallen oft verteilt über verschiedene Unternehmen und auch bei den Kunden dieser Unternehmen an. Neben den Modellen und den KI-Technologien wie Algorithmen usw. stellen diese Daten den größten Wert in der Datenökonomie dar. Datensouveränität erfordert, dass die Datenproduzenten die Kontrolle über diese Daten behalten und fair kompensiert werden, wenn diese Daten genutzt werden. Das kann man mit entsprechenden Dateninfrastrukturen erreichen. Das sind Cloud-Speicher mit besonderen Sicherheitseigenschaften. Die Grundidee dafür waren die Industrial Data Spaces, die schließlich zu GAIA-X geführt haben.

Die Idee ist eine Plattform, in die alle ihre Daten geben können. Die Plattform stellt sicher, dass man die Kontrolle über die Daten behält und für die Nutzung durch andere kompensiert wird. Das funktioniert eigentlich gut und sollten wir anstreben. Federated Learning alleine hilft da wenig. Das ist ein Spezialfall des Problems. Es ist sehr ressourcenlastig und sehr aufwendig. Deshalb würde ich für diese andere Richtung mit Dateninfrastrukturen und Speicher plädieren.

Zur Skalierbarkeit von Angriffen. Natürlich gab es KI schon viele Jahre. KI wurde in der Forschung verwendet, aber auch in Produkten. Seit 2022 gibt es KI für die Massen. Jeder kann KI verwenden.

Was bedeutet das für die Angriffe? Erst einmal bedeutet das, jeder kann Angriffe durchführen. Man braucht heute keine Expertise. Man muss kein Experte in Cybersicherheit, in Netzen, in Systemen sein. Es gibt verschiedene Versionen zum Bespiel von ChatGPT. Die wurden auf Schadsoftware und Angriffsdaten trainiert. Man kann sie einfach verwenden, um Angriffe durchzuführen. Das heißt, es ist zu erwarten, und man sieht das auch, dass es viel mehr Cyberangriffe gibt, weil man sie eben ohne viel Aufwand starten kann.

Der zweite Aspekt ist, dass staatliche Akteure oder kriminelle Gruppen die Expertise haben. Die verwenden die KI-Werkzeuge, um ihre Angriffe komplexer zu machen. Automatisierung gehört zur Vergangenheit. Wir hatten automatisierte Methoden und Werkzeuge schon vor ChatGPT. Heutzutage können einfach viel komplexere Angriffe durchgeführt werden. Viele Teile davon können autonom durchgeführt werden. Das sieht man auch. Vor Kurzem gab es einen Bericht von Anthropic darüber, wie sie gesehen haben, dass die staatliche Angreifer KI verwendet haben, um viele Ziele anzugreifen.

Das ist natürlich eine Gefahr. Wir sehen eine zunehmende Digitalisierung. Alles wird digitalisiert. Unsere Studie zwischen 2020 und 2025 zeigt, es gibt viel mehr IT in jedem Bereich. Alle haben mehr IT, alles wird digitalisiert. Das heißt, es gibt viel mehr Möglichkeiten anzugreifen. Es gibt viel mehr Angreifer, die versuchen anzugreifen. Zu erwarten ist, dass es mehr erfolgreiche Angriffe geben wird. Für die Angreifer kostet es keine Ressourcen, viele Opfer anzugreifen. Sie können das alles auf ihren Plattformen verwalten, sie müssen gar nicht persönlich mit den Opfern kommunizieren. Dafür kann man KI einsetzen.

Schon heute sieht man, es gibt mehr Angriffe, einfachere Angriffe und auch komplexere Angriffe. Dieses Thema muss sehr ernst genommen werden. Natürlich gibt es auch Chancen. Man kann KI verwenden, um unsere Prozesse zu automatisieren, und das sollten wir auch tun.

Vorsitzende Stephanie Schuhknecht (GRÜNE): Vielen Dank für dieses Schlusswort. Ich sehe jetzt keine Wortmeldungen mehr.

Ich glaube, wir haben sehr, sehr viel mitgenommen. Mein Fazit ist, dass das Thema IT-Sicherheit ein Standortfaktor, ein Wettbewerbsfaktor und natürlich auch ein Sicherheitsfaktor ist und fehlende IT-Sicherheit eine der größten Gefahren ist. Wir haben heute sehr eindrücklich geschildert bekommen, wie hoch die Schadensummen sein können. Vor allem die kleinen und mittelständischen Betriebe brauchen da Unterstützung, und wir müssen für die Awareness mehr tun.

Meine Hoffnung war, dass wir mit der Anhörung heute dazu beitragen, dass es in der Öffentlichkeit noch ein bisschen bekannter wird. Wir werden sehen, ob Berichterstattung aus dieser Sitzung entstanden ist, aber wir können es auch alle noch einmal nach draußen tragen, nachdem wir hier drei Stunden sehr intensiv darüber gesprochen haben.

Wir nehmen mit, wenn wir über Standards diskutieren, müssen wir bei der aktuellen Dynamik auch immer Flexibilität ermöglichen und können keine Einheitslösungen bringen. Insgesamt brauchen wir mehr Austausch. Ich denke, das war jetzt ein Auftakt für mehr Austausch zu dem Thema.

Ich danke Ihnen ganz herzlich für Ihre Zeit und für Ihre Expertise und wünsche Ihnen eine gute Rückfahrt, wo auch immer Sie heute hinmüssen. Danke schön.

(Beifall – Schluss: 13:17 Uhr)

Thomas Boele (Check Point Software Technologies GmbH)
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

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 Branchen waren besonders betroffen?
    - Die Bedrohungslage bleibt anhaltend hoch, mit leichten jährlichen Schwankungen in den Fallzahlen. 2024 wurden in Bayern 14.830 polizeilich erfasste Cybercrime-Fälle registriert (−9,6 % gegenüber 2023), Aufklärungsquote 35,2 %; der größte Anteil entfällt auf Computerbetrug. Hinter dem scheinbaren Rückgang steht u. a. ein hoher Dunkelziffer-Anteil (Melde- und Anzeigelücke). Treiber sind weiter Ransomware, Betrugsvarianten (u. a. Investment-/„Pig-Butchering“-Scams), DDoS-Kampagnen vor allem hacktivistischer Akteure, sowie Spionage/Exfiltration im Kontext geopolitischer Spannungen. Besonders exponiert in Bayern: Gesundheitswesen/KRITIS, Fertigung/Automotive & Maschinenbau, öffentliche Hand/Kommunen und Mittelstand. Beispiele wie der Ameos-Vorfall (Juli 2025) zeigen die anhaltende Verwundbarkeit des Gesundheitssektors.
- Welche Cyberangriffsarten (z. B. Ransomware, Phishing, verteilter Denial-of-Service Angriff (DDoS), Advanced Persistent Threats-Angriffe (ATPs)) oder Social Engineering sind aktuell besonders relevant für Unternehmen in Bayern?
    - Ransomware 2.0/3.0 (Double/Triple Extortion, Data-Theft-First): Primärzugänge über Phishing/BEC, gestohlene/unsichere Anmeldedaten, ungepatchte VPN/Edge-Geräte; Erpressung über Datenleaks. Betroffen: v. a. KMU, Fertigung, Gesundheitswesen.
    - Phishing & Business-Email-Compromise (BEC): Finanzumleitungen, CEO-Fraud; zunehmend KI-unterstützt (hochwertigere Texte/Stimmen/Deepfakes).
    - DDoS/Hacktivismus: Politisch motivierte Kampagnen mit Bezug zu Ukraine/Nahost; teils Erpress-DDoS. Relevanz für KRITIS und E-Commerce.
    - Advanced Persistent Threats (APT)/Spionage: Fokus auf Technologie- und Know-how-Abfluss (Automotive, Maschinenbau, Elektronik). Living-off-the-Land-Taktiken, lange Verweildauer.
    - Betrug/Scams (u. a. „Trading-/Krypto-Scams“, „Pig-Butchering“): Hohes Schadensvolumen; systematische Täterökonomie, teils mit Call-Center-Strukturen.
- Wie können die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben die bayerischen Unternehmen bei der Abwehr und Bewältigung von Cyberangriffen unterstützen?
    - LSI Bayern (Landesamt für Sicherheit in der Informationstechnik) – IT-Sicherheitsbehörde des Freistaats:
        - Bayern-CERT-Lageinfos/Warnungen, Beratung (v. a. öffentliche Unternehmen/KRITIS/Kommunen), ISMS-Leitfäden, Awareness.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Für Unternehmen: Abos von Lage-/Warnmeldungen, Orientierung an LSI-Leitfäden, Teilnahme an Sensibilisierungs-/Praxisformaten.

- BLKA – Jahreslagebild Cybercrime / Bayerische Polizei (ZCB-Anknüpfung):
  - Aktuelle Phänomenlage, Kontaktpunkte für Anzeige/Erstmaßnahmen, Präventionstipps.
  - Für Unternehmen: Lagebild jährlich prüfen, Incident-Playbooks anpassen, frühzeitig Anzeige/Kontakt bei Verdacht.
- ZCB – Zentralstelle Cybercrime Bayern (bei der Generalstaatsanwaltschaft Bamberg):
  - Spezialisierte Strafverfolgung, internationale Kooperationen, umfangreiche Ermittlungsmaßnahmen (z. B. gegen Cyber-Trading-Banden).
  - Für Unternehmen: Beweise sichern, frühzeitige Einbindung der ZCB über Polizei/STA, Nutzung der Erfahrungswerte für Präventionsarbeit.
- BayLDA – Bayerisches Landesamt für Datenschutzaufsicht:
  - Guidance zu DSGVO-konformer Incident-Response/Benachrichtigung, Tätigkeitsberichte mit Praxisfällen.
  - Für Unternehmen: Meldeprozesse und Betroffenenkommunikation an BayLDA-Vorgaben ausrichten; Lessons Learned aus Berichten übernehmen.
- Bund (BKA/BSI) – Ergänzend:
  - Bundeslagebild/Empfehlungen, Allianz für Cyber-Sicherheit (BSI) als Info-/Vernetzungsdrehscheibe; BKA-Lagebilder & Operationen als Trendindikator.
  - Für Unternehmen in Bayern: Mitgliedschaft in der Allianz, Warnmeldungen/Best Practices operationalisieren.

2. Stand der IT-Sicherheitsmaßnahmen

- Inwieweit ist der aktuelle Stand der IT-Sicherheitsmaßnahmen in bayerischen Unternehmen, insbesondere bei kleinen und mittleren Unternehmen (KMU) und im Bereich der kritischen Infrastruktur transparent?
- Die Transparenz ist uneinheitlich und hängt stark vom Sektor und von regulatorischen Vorgaben ab:
  - KRITIS / stark regulierte Sektoren (Energie, Gesundheitswesen, Telekommunikation, Transport):

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Durch IT-Sicherheitsgesetz, BSI-KritisV, NIS2-Vorbereitung, sowie sektorale Vorgaben besteht hohe Transparenz gegenüber Aufsichtsbehörden.
- Betreiber müssen prüffähige Nachweise zu ISMS, Risikoanalysen, Incident-Management, Meldepflichten etc. erbringen.
- In Bayern sind insbesondere Energieversorger und kommunale Betreiber vergleichsweise gut strukturiert, wenngleich oft legacy-belastet (OT/ICS).

o Großunternehmen (Automotive, Maschinenbau, Chemie, Versicherungen):

- Mittlere Transparenz – Security wird zunehmend daten- und kennzahlengetrieben gesteuert (SOC-KPIs, Schwachstellen-Backlogs, Patch-SLAs).
- Viele Unternehmen orientieren sich an ISO 27001, BSI-Grundschutz, oder Frameworks wie NIST CSF (Cyber Security Framework).

o KMU:

- Geringe bis sehr geringe Transparenz.
- Es gibt keine verpflichtende Berichterstattung über Reifegrad, Schutzmaßnahmen oder Vorfälle (Ausnahme: Datenschutzvorfälle – BayLDA).
- Viele KMU betreiben nur reaktive statt präventive IT-Sicherheit und verfügen nicht über systematische Metriken (z. B. Mean Time to Detect, Patch-Level, EDR-Coverage, MFA-Quote).

o Zentrale Ursachen der Intransparenz bei KMU:

- Fehlende gesetzliche Mindeststandards (NIS2 wird das teilweise ändern).
- Personelle Unterbesetzung (IT-Allrounder statt dedizierter Security).
- Fehlende Dokumentation (keine Inventarisierung, keine KPIs, kein ISMS).
- Lieferkettenabhängigkeit von externen Dienstleistern, die selbst wenig Transparenz bieten.

- Welche typischen Schwachstellen und Defizite bestehen bei den Unternehmen? Wo werden die vordringlichen Handlungsbedarfe gesehen?

o Die wiederkehrenden Schwachstellen sind über alle Branchen hinweg ähnlich, aber bei KMU tendenziell ausgeprägter:

- 1) Identitäts- & Zugriffssicherheit (größte Einfallstore)

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Fehlende oder nur teilweise implementierte Multi-Faktor-Authentifizierung.
- Schwache Passwort- und Berechtigungskonzepte (shared accounts, fehlendes RBAC – Role Based Access Control).
- Kein zentralisiertes Identity Management.

▪ 2) Patch- und Schwachstellenmanagement

- Ungepatchte VPN-Gateways, Firewalls, Exchange-Server, OT-Komponenten.
- „Technical Debt“: veraltete Hardware/Software ohne Security-Support.
- Keine Priorisierung nach Exploitable Vulnerabilities (EPSS), nur CVSS (Common Vulnerability Scoring System).

▪ 3) E-Mail- und Social-Engineering-Resilienz

- Fehlendes oder unzureichendes E-Mail-Hardening (DMARC/DKIM/SPF).
- Hohe Erfolgsquote von Phishing/BEC, insbesondere bei Finanzfunktionen.

▪ 4) Fehlendes oder sehr rudimentäres Incident-Response-Management

- Keine Playbooks, kein Notfallhandbuch, kein Krisenteam.
- Mangelnde Log-Daten, fehlendes zentrales Monitoring/SIEM/EDR.
- Keine regelmäßigen Table-Top-Übungen.

▪ 5) Mangelhaftes Backup- und Recovery-Konzept

- Backups nicht offline/immutable, zu selten getestet.
- Unternehmen wissen oft nicht, wie schnell sie aus Backup wieder produktiv werden können (RTO/RPO unbekannt).

▪ 6) OT/ICS-Sicherheit (bei Industrie, Energie, Wasser, Verkehr)

- Historisch gewachsene Netze, keine Segmentierung.
- Ungepatchte Steuerungsgeräte, teilweise > 15 Jahre alt.
- Schnittstellen zwischen IT und OT oft unkontrolliert.

▪ 7) Lieferkette & Dienstleister

- Fehlende Mindestanforderungen an externe IT-Dienstleister.
- Software-Bill-of-Materials (SBOM) fehlt praktisch vollständig.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Drittrisiken werden selten bewertet oder gemessen.

3. Resilienz und Krisenmanagement

- Wie gut sind bayerische Unternehmen auf größere Cybervorfälle vorbereitet? Gibt es beispielsweise Notfallpläne, Quick-Response-Teams (QRTs) und regelmäßige Übungen?
    - Insgesamt uneinheitlich – KRITIS und große Unternehmen sind deutlich besser vorbereitet als viele KMU. Bundesweite Indikatoren zeigen: nur ein Teil der Firmen verfügt über ausgereifte Notfall- und Lieferketten-Pläne; Bitkom-/Reuters-Daten nennen z. B. lediglich ~37 % mit Notfallplänen für Lieferketten-Vorfälle. Kommunale Bereiche/SME verzeichnen teils wochen- bis monatelange Ausfälle nach Ransomware, was auf fehlende Playbooks, Übungsmangel und unzureichende Telemetrie hindeutet. Für Bayern existieren LSI-Leitfäden zum IT-Notfallmanagement; Best-Practice ist die Ausrichtung an BSI-Standard 200-4/100-4 und IT-Grundschutz-Baustein DER.4.
    - Was Behörden/Verbände bereitstellen (zum Einbauen in deine Empfehlungen):
        - LSI Bayern: konkrete Handreichungen/Downloads zu Notfallmanagement und Incident-Kommunikation.
        - BSI: Notfallhandbuch-Struktur (IT-Grundschutz) – geeignet als Mindeststandard für KMU.
- Wie bewerten Sie die Notfallversorgung im Stromausfall (z. B. auch via Dieselgeneratoren) speziell bei Rechenzentren in Bayern?
    - Professionelle RZ-Betreiber (auch in Bayern, z. B. Nürnberg/München) orientieren sich i. d. R. an EN 50600 (teilweise zusätzlich Uptime-Tier-Zertifizierung). Typisches Design: USV überbrückt Sekunden, Dieselaggregate/Generatoren übernehmen binnen ~10 s; die Verfügbarkeit hängt dann v. a. von Brennstoffbevorratung/Nachschub, Wartung und Tests ab. Uptime-Daten zeigen, dass die Ausfallhäufigkeit insgesamt nicht mehr steigt (teils leicht rückläufig), Generator-Probleme bleiben aber ein relevanter Ausfalltreiber – gute Wartung/Tests sind entscheidend.
    - Trend: BESS-Lösungen (Batteriespeicher) werden von Hyperscalern pilotiert, Diesel-Abhängigkeit soll perspektivisch sinken, EN 50600-Nachweispflichten wurden 2025 verschärft (mehr organisatorische Dokumentation).
- Welche Erfahrungen gibt es mit der Wiederherstellung nach erfolgreichen Angriffen (Recovery-Zeit, Datenverluste)?
    - Ransomware bleibt Haupttreiber für lange Wiederanlaufzeiten; bundesweite Beobachtung: Kommunen/Unternehmen fallen teilweise monatelang aus.
    - Datenverluste passieren trotz Zahlung/Hilfe häufig: Laut Hiscox 2025 berichtet rund ein Drittel der Befragten von Datenverlust (verschlüsselt oder

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

unverschlüsselt); ein aktueller Branchenvergleich betont zudem, dass ~40 % der Zahlenden trotzdem Daten verlieren.

- Praktische Lehre: Testbare RTO/RPO-Ziele, immutable/offline Backups, Wiederherstellungs-Drills und forensisch einwandfreie Beweissicherung sind entscheidender als der reine „Backup-ist-gelaufen“-Nachweis. (Diese Punkte finden sich konsistent in BSI-Leitfäden/Grundschutz.)

- Liegen Erkenntnisse vor, inwieweit der kurzfristige Wegfall grundlegender digitaler Dienste von Drittstaatsanbietern wie Cloud-Diensten in den Notfallplänen/Business Continuity -Plänen der bayerischen Unternehmen durch geeignete Vorkehrungen berücksichtigt wird?

  - Noch Lücken. Laut Bitkom/Reuters berücksichtigen viele Unternehmen Lieferketten- und Cloud-Abhängigkeiten nicht systematisch; nur ~37 % haben dedizierte Notfallpläne für solche Fälle. NIS2 zwingt (auch in Bayern) zu Business-Continuity-Maßnahmen inkl. Backup/Recovery und Lieferanten-Risikomanagement – das schließt Cloud-Exit/Failover-Szenarien (z. B. Multi-Region, Cloud-to-Cloud-Backup, Minimalbetrieb On-Prem) ein.
  - Die BaFin fordert (basierend auf DORA) von Unternehmen die Cloud-Dienste auslagern, geeignete Vorgaben und Maßnahmen zur Risikoreduktion. Z.B.: Einbindung von Cloud-spezifischen Komponenten in das eigene IT-Notfallmanagement; Festlegung von Verfügbarkeitsanforderungen (SLAs), geografischer Redundanz und Ausstiegsoptionen; Dokumentation und regelmäßige Überprüfung von Ausstiegsplänen, um bei unerwarteten Beendigungen der Dienstleistung schnell reagieren zu können.

4. Lieferketten, digitale Resilienz und digitale Souveränität

- Wie können einheitliche IT-Sicherheitsstandards entlang der gesamten Wertschöpfungskette etabliert und durchgesetzt werden?

  - Regulatorischer Rahmen als Mindeststandard verankern:

    - NIS2 verpflichtet „wesentliche“ und „wichtige“ Einrichtungen zu Lieferketten-Security (Art. 21), inkl. Anforderungen an Beschaffung, Entwicklung, Schwachstellen-Handling und Wirksamkeitskontrollen. Das eignet sich als Baseline für bayerische Branchen – auch jenseits formal NIS2-pflichtiger Unternehmen.

    - DORA (für Finanzwirtschaft & kritische IKT-Dienstleister) legt verbindliche Regeln fürs ICT-Third-Party-Risk-Management fest (Art. 28–44): Vertragsinhalte, Exit-Strategien, Testen, Melden. Gute Blaupause für „Bank-like“ Lieferantensteuerung auch in Nicht-Finanzbranchen.

    - ENISA-Leitfaden bündelt Best Practices für Supply-Chain-Security (z. B. Lieferanteninventar, Risikobewertung, Monitoring, Audits).

  - Technische/organisatorische Baselines und Nachweise:

    - CIS Controls / ISO 27001 / BSI-Grundschutz als Controls-Kern; ISO 27036 (Supplier), IEC 62443 (OT) branchenspezifisch ergänzen.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Cloud-Nachweis mit BSI-C5 (prüfbares Minimum für Cloud-Dienste); perspektivisch EUCS (EU-Cloud-Zertifizierung), sobald final.

  - Vertraglich durchsetzen („Security by Contract“):

    - Sicherheits-Anhänge mit: MFA-Quote, Patch-SLAs (z. B. internet-exponiert < 7 Tage), Logging-/Retention-Pflichten, SBOM + VEX, Schwachstellen-Meldung/Remediation-Fristen, Audit-/Test-Rechte, Exit-/Portabilitäts-Zusagen.

    - Kontinuierliche Assurance: jährliche C5/ISO-Berichte, Pen-Tests, KPI-Reporting, Lieferanten-Reviews (mind. quartalsweise).

    - Operativ verankern: zentrales TPRM (Third-Party Risk Management), Lieferantenklassifizierung, Risiko-Charta, und Notfall-/Exit-Proben (Failover/Restore mit echten Datenkopien).

- Inwieweit bestehen Abhängigkeiten für bayerische Unternehmen von internationalen Cloud- und IT-Infrastrukturanbietern und ggf. welche Risiken ergeben sich hierdurch?

  - Konzentrations- und Lock-in-Risiken: hoher Marktanteil weniger Hyperscaler → Single-Vendor-Abhängigkeit, Preissetzungsmacht, proprietäre Dienste erschweren Portabilität. Der EU-Data Act wirkt explizit gegen Vendor-Lock-in (Wechsel/Portabilität, ab 12. Sept 2025 voll anwendbar).

  - Rechtsrahmen & Zugriffsrisiken (Drittstaaten): Schrems II (CJEU) kippte Privacy Shield; Transfers benötigen angemessene Garantien und „essentially equivalent“ Schutz – für EU-Unternehmen ein Dauer-Compliance-Thema. Debatten rund um EUCS zeigen die Spannung zwischen Sicherheits-/Souveränitätsklauseln und Marktoffenheit (u. a. Diskussion um US CLOUD Act-Risiken).

  - Resilienzrisiken: große Cloud-Outages sind selten, aber systemisch relevant (Multi-Tenant, gemeinsame Abhängigkeiten). DORA/NIS2 verlangen Business-Continuity inkl. Exit-/Switching-Plänen und regelmäßigen Tests – das sollte auch außerhalb der regulierten Sektoren adaptiert werden.

  - Pragmatische Gegenmaßnahmen: Multi-Region/-AZ-Design, zweiter Provider für kritische Workloads (aktive/warme Reserve), Daten-Portabilität (offene Formate, Export-APIs), Krypto-Trennung (Kundenschlüssel, EU-HSM/Extern-KMS), Support-Scopes EU-only wo verfügbar. (Data-Act-Portabilität vertraglich einfordern, inkl. Fristen/Kosten-Caps.)

- Welche Maßnahmen könnten zur Stärkung der digitalen Souveränität und zur Förderung europäischer Alternativen beitragen?

  - Europäische Rahmen & Ökosysteme nutzen/ausbauen:

    - Gaia-X, Delos Cloud, STACKIT, Ionos - z. B. als “Leitplanke” für Daten-Souveränität in Verbundprojekten. Hilfsweise Deregulierung in Bereichen, in welchen eine schnelle Umsetzung von Digitalisierungsvorhaben angeraten ist.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Sovereign Cloud Stack (SCS) (OSB Alliance): Open-Source-Referenzstack für föderierte Cloud-/Container-Infrastrukturen; Ziel: austauschbare, kompatible Angebote mehrerer EU-Provider.
- BSI-C5-Typ2-Testat als Mindest-Label für Cloud-Bezug (auch Hyperscaler können C5 liefern; Vergleichbarkeit & Auditierbarkeit steigen). EUCS bei Verfügbarkeit als nächster Schritt.

o Portabilität institutionalisieren (anti-lock-in):

- Data-Act-Klauseln: vertraglich Wechsel-/Exit-Rechte, Migrations-SLOs, Daten-/Schema-Export, Workload-Portierung (Container/Kubernetes/Terraform), „Re-Hosting-Playbooks“; jährliche Exit-Tests (Probe-Migration).
- Beschaffungsleitlinien in Bayern/DE anpassen:
  - „Cloud-Neutralität“ mit Souveränitätskriterien: Datenlokation, Schlüssel-Kontrolle (EU-KMS/HSM), Support-Jurisdiktion, Offene Standards, Reversibilität, C5/EUCS-Level, Sicherheits-KPIs als verpflichtende Zuschlagskriterien. (Viele öffentliche Stellen referenzieren bereits C5.)
- Fördern & bündeln:
  - Cluster & Förderlinien für Gaia-X-Datenräume (Automotive, Health, Manufacturing) in Bayern; Public-Private-Piloten mit EU-Cloud-Anbietern (z. B. IONOS/Hetzner/OVHcloud) inkl. C5-Nachweisen.
  - Die Verwaltung hat es hier etwas „einfacher“. Man könnte für die Landesbehörden das IT-DLZ als zugelassenen Cloudanbieter etablieren. Bei den Kommunen könnte man Anreize schaffen, die es schwer machen dem Move ins RZ entweder des IT-DLZ (falls gewollt) oder z.B. der AKDB zu widerstehen (kommuale Selbstverwaltung) - anstatt öffentliche Cloudanbieter zu nutzen. Die Flexibilität und Schnelligkeit muß gegeben sein. Zur Info: derzeit finden Verhandlungen zwischen Bayern und Microsoft zur flächendeckenden Einführung von Microsoft365 statt. Der „Bayern-Server“ wird vom IT-DLZ betrieben und ist für datenhoheitliche und sicherheitskritische Anwendungen gedacht. Dabei greift das IT-DLZ auch auf andere Anbieter zurück z.B. DVC und DELOS. Für die Kommunen gibt es die BayernBox basierend auf ownCloud. Diese wird auch vom IT-DLZ/LDBV bereitgestellt.

5. Regulatorische Anforderungen und Umsetzung

- Welche gesetzlichen Vorgaben zur Einhaltung von IT-Sicherheit, insbesondere zu Standards und Zertifizierungen, bestehen für bayerische Unternehmen?

o EU-Eckpfeiler (querschnittlich):

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- NIS2-Richtlinie (EU 2022/2555): verschärfte Mindestmaßnahmen, Management-Haftung, Meldepflichten, Lieferketten-Security; DE-Umsetzung NIS2UmsuCG weitet den Kreis betroffener Unternehmen deutlich aus (≈ 29.000).
- DORA (Finanzsektor): seit 17. Jan 2025 anwendbar (u. a. ICT-Risiko-Mgmt, Vorfall-Reporting, TLPT, Third-Party-Register).
- Cyber Resilience Act (CRA): produktbezogene Cyber-Sicherheitspflichten für vernetzte/Software-Produkte (in Kraft seit 10. Dez 2024; Hauptpflichten ab 11. Dez 2027).
- CER-Richtlinie (physische Resilienz kritischer Einrichtungen): gilt seit 18. Okt 2024; ergänzt NIS2.
- eIDAS 2 / EUDI-Wallet (Vertrauensdienste/Identitäten): Rahmen seit Mai 2024 in Kraft; Umsetzungen/Regelungen 2024/2025.

o Deutschland (bundesrechtlich):

- IT-Sicherheitsgesetz 2.0 + BSI-KritisV (zuletzt 2024 geändert): Pflichten für KRITIS-Betreiber (z. B. Systeme zur Angriffserkennung, niedrigere Schwellen in manchen Sektoren).
- Im Herbst 2025 hat die Bundesregierung zudem ein KRITIS-Dachgesetz angekündigt/auf den Weg gebracht (physische + organisatorische Resilienz).
- Standards/Zertifizierungen (Best Practice / oft gefordert):
- SO/IEC 27001 (ISMS), BSI-Grundschutz (BSI-200-1/-2/-3) inkl. Zertifizierung, BSI-C5 für Cloud-Provider; branchenspezifisch TISAX (VDA-ISA) im Automotive-Umfeld, IEC 62443 (OT).

o Bayern (Unterstützung/Anlaufstellen):

- LSI Bayern/Bayern-CERT (Leitfäden, Notfallmanagement für Kommunen/Unternehmen); BayLDA für DSGVO-Meldepflichten (72-Stunden-Frist).

- Welche Herausforderungen bestehen für bayerische Unternehmen aus Expertinnen- und Expertensicht bei der Umsetzung? Wo bestehen ggf. Unterstützungsmöglichkeiten durch staatliche Stellen?

o Herausforderungen (häufig bei KMU, aber auch in der Fläche):

- Komplexität & Überschneidungen (NIS2 ↔ DORA ↔ CER ↔ CRA), Lieferketten-Nachweise, Management-Accountability.
- Kosten/Personal: EU-Studie nennt GDPR/NIS2 als kostenstärkste Digital-Regulierungen für SME; viele Firmen berichten über Know-how-Engpässe.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Cloud-Abhängigkeiten & Souveränität: offene EUCS-Debatte (Sicherheits- vs. Souveränitätsklauseln) schafft Planungsunsicherheit.

o Unterstützung (konkret nutzbar):

- LSI Bayern/Bayern-CERT: Leitfäden, Vorlagen, Schulungen, Notfallmanagement-Bausteine.
- BSI – Allianz für Cyber-Sicherheit: Netzwerke, Profile/Workshops zu IT-Grundschutz, Materialien. (Registrierung/Teilnahmehinweise online.)
- Förderung: Digitalbonus.Bayern (neu aufgelegt, bis 31.12.2027; IT-Sicherheit förderfähig).
- Aufsicht & Leitfäden: BayLDA (Incident-Meldung/Datenschutz), BaFin/EU-Aufseher zu DORA-RTS/Leitlinien.

- Welche möglichen Nachteile ergeben sich für die Wettbewerbsfähigkeit bayerischer Unternehmen im Bereich IT- und Cybersicherheit durch nationale oder europäische Regulierung (z. B. zusätzliche Bürokratie)?

o Compliance-Kosten & Audit-Last: EU-Parlamentsstudie sieht GDPR/NIS2 als kostenstarke Regulierungen für SME; im Finanzsektor berichten Institute spürbare DORA-Aufwände (Register, TLPT, Lieferantensteuerung).

- Unsicherheit bei Cloud-Beschaffung: offener EUCS-Kurs (Souveränitätsklauseln) → Risiko von Investitions-/Migrationsaufschub, möglicher Lock-in-Bias.
- Fragmentierung während der Übergangszeit: zeitversetzte NIS2/CER-Umsetzungen in der EU erschweren grenzüberschreitende Vereinheitlichung.

o Risikomindernde Gegenmaßnahmen (für Unternehmen & Politik):

- Harmonisierte Beschaffung: landes-/bundesweit C5/EUCS-(sobald final), ISO 27001/BSI-Grundschutz als vergleichbare Nachweise akzeptieren; Mapping-Tabellen bereitstellen.
- Proportionalität für KMU: Förderlinien (z. B. Digitalbonus.Bayern) gezielt für MFA, EDR, Backup/Immutable, Protokollierung öffnen; Vorlagen-Sets (Policies, RoI nach DORA, Incident-Playbooks).
- Cloud-Souveränität vertraglich: Portabilität, Exit-Szenarien, Datenlokation, Kundenschlüssel und Support-Jurisdiktion EU als Zuschlagskriterien; EU-Data-Act-Portabilität operationalisieren.

6. Wirtschaftliche Auswirkungen und Kosten

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Welche wirtschaftlichen Schäden entstehen durch Cyberangriffe auf Unternehmen in Bayern? Inwieweit kam es dadurch bisher zu spürbaren Einschränkungen der laufenden Produktion?
    - Konkrete Bayern-Schadenssummen werden polizeilich nicht repräsentativ ausgewiesen; das BLKA-Lagebild Cybercrime betont explizit, dass die in der Polizeilichen Kriminalstatistik erfassten Schäden nicht repräsentativ sind und verweist auf Wirtschaftsstudien (Bitkom/BfV) für die volkswirtschaftliche Gesamtsicht, laut ZCB im Durchschnitt $5Mio pro Vorfall.
    - Deutschlandweit liegt der jährliche Schaden durch Datendiebstahl, Spionage und Sabotage laut Bitkom/Wirtschaftsschutz 2025 bei ~289 Mrd. € (Vorjahr ~206–224 Mrd. € je nach Messfenster). Das unterlegt die systemische Relevanz auch für Bayern als stark industrialisiertes Bundesland.
    - Produktionsausfälle: Branchenberichte und Lagebilder bestätigen spürbare operative Einschränkungen – gerade in Fertigung/Automotive, KRITIS, Gesundheit (z. B. Ransomware-bedingte Stillstände, Umstieg auf Handbetrieb). Bundeslagebild und Fachpresse zeigen, dass Ransomware weiterhin primärer Treiber von Ausfällen ist.
    - Einordnung: Für Bayern ist – mangels belastbarer eigener Euro-Summen – die Hochrechnung über Branchen- und Bundeswerte üblich. Mit Bayerns hoher Industriequote ist von einem überproportionalen Impact bei Fertigungsunternehmen auszugehen.
- Welche Dunkelziffer ist bei gemeldeten Schäden realistisch anzunehmen?
    - Das BLKA weist darauf hin, dass PKS-Schadenssummen nicht repräsentativ sind; ein erheblicher Underreporting-Effekt ist anzunehmen (unterlassene Anzeige/Meldung, Versicherungs- oder Reputationsgründe). Bayern-Innovativ gibt an, dass 70%-80% der Vorfälle nicht gemeldet werden - aus Unkenntnis bis hin zu Scham.
    - Bitkom ermittelt Schäden über Unternehmensbefragungen und kommt zu den o. g. dreistelligen Milliardenbeträgen – deutlich über dem, was in Polizeistatistiken sichtbar wird. Plausibel ist somit eine hohe Dunkelziffer bei Fällen und Schäden, insbesondere im Mittelstand.
- Wie bewerten Sie die Kosten-Nutzen-Relation von Investitionen in IT-Sicherheit, insbesondere für KMU?
    - Relevante Schadenshöhen (Referenzwerte):
        - Der IBM Cost of a Data Breach Report 2025 beziffert die durchschnittliche wirtschaftliche Belastung eines Datenvorfalls in Deutschland auf rund 3,87 Mio. €. Dieser Wert dient als ökonomische Referenzgröße, um den finanziellen Nutzen präventiver Sicherheitsmaßnahmen realistisch einzuschätzen. Er zeigt deutlich, dass schon ein einzelner schwerwiegender Vorfall die typischen Jahresinvestitionen eines KMU in IT-Sicherheit um ein Vielfaches übersteigen kann.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Methodik zur Wirtschaftlichkeitsbewertung:
  - ENISA empfiehlt Ansätze wie Annual Loss Expectancy (ALE) und Return on Security Investment (RoSI). Dabei werden der erwartete jährliche Verlust pro Risiko (z. B. Ransomware, Phishing, Ausfallzeiten) den Investitions- und Betriebskosten von Sicherheitsmaßnahmen gegenübergestellt – etwa MFA, EDR/XDR, immutable Backups oder automatisiertes Patch-Management.
  - In der Praxis amortisieren sich grundlegende Sicherheitsmaßnahmen in KMU häufig innerhalb von 12–24 Monaten, insbesondere wenn man die Kosten externer Incident-Response-Dienstleister, Produktionsstillstände und Wiederherstellungsaufwendungen berücksichtigt.
- Trendentwicklung (2024/2025):
  - Studien zeigen, dass Unternehmen mit schnellerer Erkennung (MTTD) und effizienterer Eindämmung (MTTR) – etwa durch Automatisierung, KI-gestützte Analyse, internem SOC oder MSSP-Services – ihre Vorfallkosten signifikant reduzieren. Dadurch verbessert sich die Kosten-Nutzen-Relation zusätzlicher Sicherheitsmaßnahmen weiter.
- Wirtschaftlich priorisierte „Daumenregeln“ für KMU
  - Identity First – MFA überall:
    - Sehr hohe Risikoreduktion bei minimalem Betriebskostenaufwand.
  - EDR/XDR + zentrales Logging:
    - Verkürzen MTTD/MTTR deutlich und reduzieren die Zahl externer Dienstleistertage.
  - Immutable/Offline-Backups + regelmäßige Restore-Tests:
    - Erhöhen die Widerstandsfähigkeit gegen Ransomware und minimieren Stillstandszeiten.
  - Schnelles Patchen „exponierter Systeme“ (< 7 Tage):
    - Reduziert die Ausnutzbarkeit kritischer Schwachstellen erheblich (VPN, E-Mail-Gateways, Edge-Systeme).

- In welchen wirtschaftlichen Nischen im Bereich Cybersicherheit haben bayerische IT-Unternehmen besondere Stärken oder Chancen in der internationalen Arbeitsteilung?
  - Bayern verfügt über ein ausgeprägtes Cybersecurity-Ökosystem, das sich insbesondere in folgenden international relevanten Nischen auszeichnet:
  - 1) Trustworthy / Industrial Security & Compliance (München, Regensburg, Nürnberg)

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Die Region ist ein zentraler Standort für besondere High-Trust-Sicherheitskompetenz:
- Fraunhofer AISEC (Garching):
  - Führend in angewandter Forschung zu Hardware-/Embedded-Security, Secure Coding, Industrial Security und KI-Sicherheit. Bedeutende Rolle im Technologietransfer zu Industrieunternehmen.
- Rohde & Schwarz Cybersecurity (München):
  - Starke Position im Bereich zertifizierte Hochsicherheitsverschlüsselung, VS-NfD-fähige Netzwerkkomponenten, gehärtete Browser-/Endpoint-Lösungen.
- Infineon (München):
  - Europäische Spitzenposition bei Kristallin-basierter IT-Sicherheit: TPM, Secure Elements, Automotive Security-Chips – Schlüsseltechnologien für „Security by Design“ in IoT, Automotive und Industrie 4.0.
- TÜV SÜD (München):
  - International stark nachgefragte Expertise in IEC 62443 Audits, OT-Security-Zertifizierung, Konformitätsbewertung für industrielle Steuerungssysteme.

o 2) Check Point Software Technologies (Ismaning bei München)

- Check Point ist ein weltweit führender Anbieter im Bereich Netzwerksicherheit, Workspace-, AI-, Cloud-Security und Exposure Managent– mit einer strategisch bedeutenden Präsenz in Ismaning.
  - Besondere internationale Relevanz ergibt sich durch:
    - EAL4+ (BSI) zertifizierte Sicherheitsplattformen:
      - Hohe Vertrauenswürdigkeit und formale Evaluierung nach Common Criteria, vielfach in regulierten und behördlichen Umgebungen weltweit eingesetzt.
    - BSI C5-Typ2-Testat (Cloud Security):
      - Die Cloud-Plattformen von Check Point verfügen über ein C5-Typ2-Testat, das internationale Kunden–insbesondere im KRITIS- und Enterprise-Umfeld–bei der Einhaltung von Cloud-Sicherheits- und Compliance-Standards unterstützt.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Globale Kompetenzzentren für Netzwerk-, Cloud- und OT-Security:
    - Der Standort Ismaning ist ein europäisches Zentrum für Forschung, Produktentwicklung, Threat-Intelligence und technisches Enablement – insbesondere im Bereich
- Cloud Security,
- Netzwerksegmentierung / Zero Trust,
- Exposure Management, Threat Intelligence / Malware-Analyse, und KI-basierte Sicherheitsmechanismen.

- Damit nimmt Check Point in Bayern eine Brückenfunktion zwischen europäischer Regulierung, internationaler Produktinnovation und regionaler Wirtschaftsförderung wahr.

- 3) Hardware-basierte Sicherheit und Kryptografie
    - Bayern ist durch Infineon, Rohde & Schwarz sowie mehrere spezialisierte mittelständische Hersteller ein führender Standort für HSM, Secure ICs, Kryptochips, Automotive-Sicherheitsmodule und „Trusted Computing“-Technologien.
- 4) Zertifizierungs- und Testlandschaft (konform zu EU- & BSI-Standards)
    - TÜV SÜD, Fraunhofer, unabhängige Prüflabore sowie industrienahe Institute ermöglichen IT-Grundschutz, ISO 27001, IEC 62443, TISAX, C5 sowie branchenspezifische Zertifizierungen – ein Standortvorteil für europäische und internationale Kunden.
- 5) Cluster, Netzwerke und Digitalstandort Bayern
    - Sicherheitsnetzwerk München e.V.,
    - IT-Sicherheitscluster e.V. (Regensburg),
    - Bayern Innovativ und ZD.B verbinden Forschung, Start-ups, etablierte Unternehmen und Behörden.
    - Dies stärkt Ko-Innovation und beschleunigt Technologietransfer – ein wesentlicher internationaler Wettbewerbsvorteil.
- Bayern verfügt im internationalen Vergleich über überdurchschnittliche Stärken in
    - zertifizierbarer Hochsicherheit,
    - Industrial/OT Security,
    - Hardware-Trust-Technologien,

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Cloud-/Compliance-Security und Threat Prevention.

- Mit Unternehmen wie Check Point (Ismaning), Rohde & Schwarz, Infineon, Fraunhofer AISEC und TÜV SÜD besitzt Bayern ein unikales, exportfähiges Portfolio für globale Cybersecurity-Märkte.

7. Sensibilisierung, Ausbildung und Fachkräftemangel

- Wie ist der Stand der Sensibilisierung und Weiterbildung im Bereich IT-Sicherheit in Unternehmen?

  - Der Reifegrad ist sehr heterogen – gut in stark regulierten Branchen, schwach im KMU-Sektor.

  - Status in Bayern und Deutschland:

    - Großunternehmen / KRITIS / Automotive / Finanzwirtschaft:

      - Haben in der Regel strukturierte Awareness-Programme, verpflichtende Schulungen, Phishing-Simulationen und rollenbezogene Trainings.

      - Awareness ist oft Teil von ISO 27001/BSI-Grundschutz oder branchenspezifischen Standards (z. B. TISAX, MaRisk, DORA).

    - Kommunen & Mittelstand:

      - Viele KMU verfügen nicht über regelmäßige Security-Schulungen oder stark variierende Qualitätsniveaus.

      - Phishing-Simulationen und IT-Sicherheits-Schulungen werden häufig ad hoc oder gar nicht durchgeführt.

      - „Human Risk Management“ (kontinuierliche Verhaltensanalyse, Wiederholungstrainings, Rollenmodelle) ist selten.

      - Kommunen leiden oft darunter, dass es im Rathaus keine Kompetenz im Bereich Cybersicherheit gibt. Hier wird häufig ein affiner Mitarbeiter zum IT-Beauftragten ernannt und dann auch noch zum IT-Sicherheitsbeauftragten, Datenschutzbeauftragten, Gleichstellungsbeauftragten, Behindertenvertretung, etc. Mit diesem Bouquet an Titeln kann kein adäquater Schutz umgesetzt werden, zumal der Kollege auch noch seinen eigentlichen Job hat. In Kleinstkommunen wird dann die IT bei einem lokalen Dienstleister gesourced, der aber von dem Thema auch nur bedingt Expertise hat. Hier könnten das IT-DLZ oder die kommunalen Dienstleister wie z.B. AKDB entsprechende Anreize schaffen, dass die Bürgermeister weiterhin für das „ob“ in der Umsetzung der Cybersicherheit verantwortlich sind, aber die Verantwortlichkeit um das „wie“ und die sich daraus ergebenden Konsequenzen abgeben können.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Gesundheits- und Pflegeeinrichtungen:
  - Weiterhin Nachholbedarf, obwohl die Branche besonders stark angegriffen wird.

- Fazit:
  - Sensibilisierung wird oft als „nice to have“ gesehen – und nicht als integraler Bestandteil der Sicherheitsarchitektur. Besonders KMU unterschätzen weiterhin Social Engineering, obwohl > 70 % der erfolgreichen Angriffe mit der Kompromittierung einer Identität beginnen.

- Gibt es ausreichend qualifiziertes Personal, um die IT-Sicherheit in Unternehmen zu gewährleisten? Wo sehen Sie etwaige Engpässe und deren Ursachen?
  - Nein. Bayern – wie ganz Deutschland – leidet unter einem massiven und strukturellen Fachkräftemangel im Bereich Cybersecurity.
  - Engpasslage:
    - BSI, Bitkom und ENISA berichten kontinuierlich von einem Nachfragedefizit:
      - In Deutschland fehlen über 100.000 IT-Sicherheitskräfte, davon ein großer Teil im süddeutschen Raum.
      - Besonders schwer zu besetzen: SOC-Analysten, Security Engineers, Cloud-Security-Architekten, OT-Security-Spezialisten, Pentester.
    - Engpässe in Bayern besonders sichtbar, da hier viele
      - Industriekonzerne (Automotive, Maschinenbau),
      - KRITIS-Betreiber (Energie, Gesundheit),
      - große IT-/Security-Unternehmen
    - um dieselben Fachkräfte konkurrieren.
  - Ursachen:
    - Steigende Komplexität der IT-Landschaften (Cloud, OT/ICS, IoT, KI).
    - Regulatorischer Druck (NIS2, DORA, CRA) erzeugt zusätzliche Positionen, aber keine zusätzlichen Fachkräfte.
    - Lange Ausbildungszyklen in Hochschulen (Bachelor/Master), die nicht mit dem Tempo des Marktes mithalten.
    - Unzureichende praxisorientierte Inhalte in klassischen IT-Ausbildungen.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Abwanderung in höher bezahlte Branchen (Consulting, Big Tech, Defense).
- Fehlende Spezialisierung in vielen Berufsbildern – Security ist oft nur ein Modul, nicht Kernbestandteil.

o Besonders betroffene Rollen:

- SOC-/SIEM-Analysten
- OT/ICS-Security (Industrie 4.0, Maschinenbau)
- Cloud-Security (AWS/Azure/GCP)
- Incident-Response-Spezialisten
- Identity & Access Management Experts
- DevSecOps-Engineers

- Wie kann die Aus- und Weiterbildung von IT-Sicherheitsfachkräften an bayerischen Hoch- und Berufsschulen verbessert werden?

o Mehr praxisorientierte Inhalte (hands-on) statt rein theoretischer Module

- Pflichtmodule zu
  - Incident Response,
  - Pentesting,
  - Cloud Security (AWS/Azure/GCP),
  - Zero Trust,
  - Logging & Detection Engineering,
  - OT/ICS-Security.
- Realistische Cyber-Range-Umgebungen an Hochschulen (z. B. in Kooperation mit Fraunhofer AISEC oder privaten Anbietern), Cyber-Park-Events / CTF-Challenges

o Spezialisierte Ausbildungsgänge für kritische Rollen

- „Cloud Security Specialist (IHK/Hochschule)“
- „OT-/ICS-Security Engineer“
- „Threat Intelligence Analyst“
- „DevSecOps Spezialist“

o Derzeit sind viele Studiengänge breit, aber nicht rollenorientiert.

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Duale Studiengänge & Industry-Sandwich-Modelle ausbauen
  - Kooperationen mit
  - Automotive-Unternehmen,
  - Energiewirtschaft,
  - kommunalen Trägern,
  - Sicherheitsfirmen (u. a. Check Point, Rohde & Schwarz, Infineon).
  - Wechsel zwischen Theorie und echten Security-Projekten.
- Stärkere Einbindung von Forschungseinrichtungen
  - Fraunhofer AISEC,
  - LMU/TUM Security Labs,
  - OTH Regensburg,
  - Hochschule Augsburg (IT-Sicherheit) bieten bereits gute Module – sollten aber stärker mit staatlichen Einrichtungen (LSI, BayLDA) und der Wirtschaft verzahnt werden.
- 5) Modernisierung der Berufsschulen in Bayern
  - Integration von Security-Themen in
  - Fachinformatiker-Ausbildungen,
  - Elektrotechnik/Automatisierungstechnik (für OT-Security),
  - Mechatronik (Industrial IoT).
  - Nutzung von Schulungsplattformen, Phishing-Simulatoren und virtuellen Laboren.
- Förderprogramme für Weiterqualifizierung
  - Landesprogramme zur
  - Umschulung,
  - berufsbegleitenden Weiterbildung,
  - Zertifizierung von Security-Basiskompetenzen (z. B. CompTIA Security+, CCNA Security, ISMS/ISO 27001 Practitioner, CISSP, CCSA, CCSE etc).
- Verpflichtende IT-Security-Module für alle digitalen Studiengänge

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Analog zur „Digital Literacy“ sollten Security-Grundlagen verpflichtender Bestandteil jedes technischen oder wirtschaftlich-technischen Studiums sein.

8. Zukunftsperspektiven und Innovation

- Welche technologischen Trends (z. B. Künstliche Intelligenz, Cloud-Lösungen) beeinflussen die IT-Sicherheitslage aktuell und künftig?
    - Die IT-Sicherheitslage bayerischer Unternehmen wird aktuell und künftig deutlich durch mehrere technologische Trends geprägt, allen voran durch den zunehmenden Einsatz von Künstlicher Intelligenz sowie den Übergang zu Cloud-, Container- und Edge-basierten IT-Infrastrukturen. Künstliche Intelligenz wirkt dabei zweischneidig: Auf der einen Seite ermöglicht sie leistungsfähigere Erkennungsverfahren für Anomalien, automatisierte Analysen großer Log- und Telemetriedatenmengen sowie schnellere Reaktionszeiten in Security Operations Centern. Auf der anderen Seite nutzen Angreifer dieselben Technologien, um z. B. täuschend echte Phishing-Nachrichten oder Deepfakes zu erzeugen, Angriffspfade zu automatisieren oder Schwachstellen effizienter auszunutzen. Die zunehmende Verbreitung generativer KI führt damit sowohl zu einer Beschleunigung der Verteidigung, aber auch zu professionelleren und skalierbareren Angriffsmethoden.
    - Darüber hinaus verändert die umfassende Nutzung von Cloud-Architekturen, Software-as-a-Service, Container-Orchestrierung und kontinuierlichen Deployment-Pipelines die Sicherheitsanforderungen der Unternehmen tiefgreifend. Fehlkonfigurationen, unzureichendes Identitätsmanagement, mangelnde Kontrolle über APIs sowie die wachsende Abhängigkeit von Drittanbieterplattformen sind bereits heute zentrale Risikofaktoren. Für industrielle Branchen kommt die zunehmende Vernetzung von Produktionsanlagen, sensorbasierten Systemen und Steuerungstechnik hinzu. Diese Entwicklungen verschieben die IT-Sicherheit vom klassischen Perimeterschutz hin zu Zero-Trust-Ansätzen, identitätszentrierter Sicherheit, Cloud-nativen Kontrollmechanismen und automatisierten Abwehrstrategien, die sowohl in großen Unternehmen als auch im Mittelstand zunehmend unverzichtbar sind.
    - Quantencomputer werden aktuell in rasanter Geschwindigkeit weiterentwickelt und zur Markereife gebracht, Post-Quantum-Verschlüsselung ist ein Thema, welches man auf dem Radar haben muss.
- Wie kann Bayern als Wirtschaftsstandort die digitale Souveränität stärken und Abhängigkeiten von internationalen IT-Anbietern verringern?
    - Um die digitale Souveränität Bayerns langfristig zu stärken und Abhängigkeiten von internationalen IT-Anbietern zu reduzieren, sind mehrere strategische Maßnahmen notwendig. Ein wichtiger Ansatzpunkt ist die konsequente Förderung europäischer Cloud- und Datenrauminitiativen sowie branchenspezifischer Datenökosysteme in Industrie, Gesundheit und Mobilität. Diese Initiativen ermöglichen interoperable, europäisch kontrollierte

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

Datenräume und reduzieren langfristig Abhängigkeiten von außereuropäischen Hyperscalern.

- Ebenso bedeutsam sind modernisierte Beschaffungsrichtlinien in Verwaltung und Wirtschaft, die Kriterien wie Datenlokation innerhalb der EU, Kontrolle über kryptografische Schlüssel, Supportleistungen innerhalb europäischer Rechtsräume sowie den Einsatz offener Standards und zertifizierbarer Sicherheitsmechanismen stärker gewichten. Zertifizierungen wie BSI C5 oder der kommende europäische Cloud-Sicherheitsstandard EUCS können dabei als Orientierungsrahmen dienen.

- Darüber hinaus verfügt Bayern bereits heute über mehrere international bedeutende Kompetenzträger, darunter Infineon, Rohde & Schwarz, Check Point Software in Ismaning, Fraunhofer AISEC sowie zahlreiche spezialisierte Mittelständler und Start-ups. Diese Unternehmen bilden eine starke Basis, um Schlüsselbereiche wie Hardware-basierte Sicherheit, Automotive- und OT-Security, Trusted Computing, Post-Quantum-Kryptografie und KI-Sicherheit weiter auszubauen. Flankierend dazu sollten Ausbildung, Forschung, Cyber-Ranges und gezielte Förderprogramme für Start-ups im Sicherheitsbereich gestärkt werden, um eine nachhaltige Wertschöpfungskette heimischer Sicherheitslösungen zu erzeugen.

- Insgesamt besitzt Bayern damit sowohl die technologische Expertise als auch die industriellen Strukturen, um im Bereich der Cybersecurity international wettbewerbsfähig zu bleiben und zugleich die Abhängigkeit von Anbietern außerhalb des vertrauenswürdigen Datenraumes zu minimieren.

9. Empfehlungen für die Politik

- Inwieweit kann die Politik bayerische Unternehmen dabei unterstützen, ihre IT-Sicherheit weiter zu stärken?

  - Die Politik kann bayerische Unternehmen auf drei Ebenen spürbar stärken: erstens durch verlässliche Mindeststandards und entlastende Umsetzungshilfen, zweitens durch gezielte Förderung von Kompetenzen und Infrastruktur, drittens durch bessere Verzahnung von Staat, Wirtschaft und Forschung. Kurzfristig wirksam sind Maßnahmen, die KMU den Einstieg in „Security-Basics“ erleichtern (MFA, EDR/XDR, E-Mail-Hardening, Patch-Prozesse, Backups mit regelmäßigen Restore-Tests) und gleichzeitig die Fähigkeit zur schnellen Erkennung und Reaktion erhöhen (Monitoring, Incident-Playbooks, Kontaktketten zu Polizei/Justiz/Aufsicht). Eine bessere Verzahnung zwischen Polizei, LKA und LSI ist wünschenswert. Da klemmt es derzeit teilweise noch sehr, was die Weitergabe von Ermittlungsergebnissen angeht.

  - Die aktuell verfolgten Maßnahmen auf Bundes- und Landesebene werden in der Tendenz positiv bewertet, weil sie mit NIS2/DORA/CRA klare Leitplanken, Haftungs- und Meldepflichten sowie Lieferkettenanforderungen setzen (bitte beachten: KRITIS, Verwaltung und Plankrankenhäuser sind gegenüber dem LSI nicht meldepflichtig). In der Praxis zeigt sich jedoch, dass insbesondere KMU an Komplexität, Dokumentationslast und Fachkräftemangel scheitern. Förderinstrumente wie der Digitalbonus, Angebote von LSI/Bayern-CERT und

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

die BSI-Allianz für Cyber-Sicherheit sind sinnvoll, sollten aber stärker auf Standardisierung, einfache Nachweise und wiederverwendbare Vorlagen abzielen. Verbesserungspotenzial besteht vor allem bei der flächendeckenden Operationalisierung (Templates, Werkzeuge, „One-Stop“-Anlaufstellen), bei der Beschaffung (einheitliche, praxisnahe Sicherheitskriterien) und bei der Skalierung staatlich unterstützter Ersthilfe im Incident-Fall.

- Wie werden aktuell verfolgte Maßnahmen auf Bundes- und Landesebene dahingehend bewertet?

    - Um die Resilienz weiter zu erhöhen, bietet sich ein Bündel konkreter Maßnahmen an: (1) „Security-Baseline Bayern“ als pragmatische Baseline für alle Branchen, abgeleitet aus ISO 27001/BSI-Grundschutz/CIS-Controls, mit wenigen messbaren Kennzahlen (z. B. MFA-Quote, EDR-Abdeckung, Patch-SLA für internetexponierte Systeme < 7 Tage, Backup-Erfolg/Restore-Zeit). Dazu passende, rechtssichere Musterpolicies, Vertragsanhänge für Lieferanten (SBOM/VEX, Patch-Fristen, Logging, Audit- und Exit-Rechte) sowie Checklisten für NIS2-relevante Unternehmen. (2) Finanzielle Anschubhilfe für KMU über Security-Gutscheine oder standardisierte Förderpakete („MFA+EDR+Backup“) inklusive Einführungs- und Schulungsbudget; optional steuerliche Begünstigung zertifizierter Sicherheitsinvestitionen. (3) Aufbau bzw. Ausbau eines landesweiten „Bayern-SOC-Netzes“ mit modularen Managed-Services (Threat-Monitoring, Notfall-Hotline, forensische Ersthilfe, DDoS-Vorsorge) – besonders für Kommunen und Mittelstand – sowie klare Eskalationspfade zu LSI, Polizei und ZCB. (4) Beschaffungsleitlinien für öffentliche Stellen und Landesbeteiligungen mit europäischen Souveränitätskriterien (Datenlokation EU, Kundenschlüssel/Key-Ownership, offene Standards/Portabilität, C5/EUCS-Nachweise), die gleichzeitig als Marktstandard für private Beschaffung dienen können. (5) Stärkung der Fachkräftebasis durch rollenorientierte, praxisnahe Ausbildungs- und Weiterbildungsprogramme (SOC-Analyst, Cloud-Security-Architekt, OT-Security-Engineer, DevSecOps), duale Studiengänge und gemeinsame “Cyber-Ranges” (Laborumgebungen) von Hochschulen, LSI und Industrie; flankiert durch beschleunigte Anerkennung internationaler Qualifikationen und zielgerichtete Zuwanderungswege für Security-Profile. (6) Fokussierte Innovationsförderung für bayerische Stärkefelder – OT/Industrial-Security, Automotive-Security, Hardware-basierte Sicherheit (TPM/HSM/Secure Elements), Trusted/AI-Security und Post-Quantum-Kryptografie – inklusive Transferprogrammen zwischen Fraunhofer/Universitäten und Mittelstand sowie Pilotvorhaben in Reallaboren. (7) Stärkung der digitalen Souveränität durch gezielte Förderung interoperabler Alternativen (vertrauenswürdige Datenräume, Sovereign Cloud Stack) und durch regelmäßige „Exit-/Portabilitäts-Proben“ als förderfähige Maßnahme, um Abhängigkeiten von einzelnen Cloud-Anbietern messbar zu verringern.

- Wo werden Potenziale gesehen, die Zusammenarbeit von Staat, Wirtschaft und Forschung zur Erhöhung der Resilienz gegen Cyberbedrohungen weiter zu verbessern?

Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 09.10.025

- Die Zusammenarbeit von Staat, Wirtschaft und Forschung lässt sich durch wenige strukturelle Hebel weiter verbessern: ein landesweites, kuratiertes ISAC-Netzwerk (branchenspezifischer Austausch mit klaren Vertraulichkeitsregeln), standardisierte Melde- und Informationskanäle mit „Safe-Harbor“-Charakter für frühe Vorfallmeldungen, gemeinsame Jahresübungen mit realistischen Szenarien (IT/OT, Cloud-Ausfall, Lieferkettenstörung), ein zentrales Repository wiederverwendbarer Artefakte (Playbooks, Vertragsklauseln, technische Härtungsprofile) sowie ein schlankes Monitoring relevanter Resilienz-KPIs auf aggregierter Ebene. Durch diese Kombination aus Mindeststandards, operativer Unterstützung, qualifizierter Ausbildung und koordiniertem Wissensaustausch können die Kosten und Auswirkungen von Cyberangriffen nachhaltig gesenkt, die Umsetzungslast für Unternehmen reduziert und gleichzeitig die Wettbewerbs- und Innovationsfähigkeit des Wirtschaftsstandorts Bayern gestärkt werden. Erwähnenswert ist zudem die 2012 gegründete Allianz für Cyber Security. Diese steht Unternehmen, Verbänden, Behörden und Organisationen eine kooperative Plattform zur Verfügung, über die Informationen zu aktuellen Bedrohungslagen und Cybersecurity-Maßnahmen bereichsübergreifend ausgetauscht werden können.

Landesamt für Sicherheit in der Informationstechnik

Anhörung des Ausschusses für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung zum Thema „IT-Sicherheit in der bayerischen Wirtschaft“

am 27.11.2025

Herr Bernd Geisler
Präsident des Landesamtes für Sicherheit in der Informationstechnik

Eingangsstatement

Das Landesamt für Sicherheit in der Informationstechnik ist die IT-Sicherheitsbehörde des Freistaats Bayern. Der Freistaat war damit das erste Bundesland, das eine eigenständige IT-Sicherheitsbehörde eingerichtet hat. Das LSI kümmert sich seit 2017 um den aktiven Schutz der staatlichen IT-Systeme und unterstützt Kommunen und öffentliche Betreiber kritischer Infrastrukturen bei der Absicherung ihrer Systeme durch Beratung sowie weiteren Angeboten.

Konkret sind im BayDiG Art. 42 die Aufgaben des LSI dargelegt.

Das LSI trägt insbesondere dafür Sorge, dass die Sicherheit an den Schnittstellen des Behördennetzes und zu anderen Netzen sichergestellt ist. Außerdem unterstützt das LSI sämtliche Stellen, die an das Behördennetz angeschlossen sind bei der Erkennung und Abwehr von Angriffen. Es werden sicherheitstechnische Mindeststandards für alle an das Behördennetz angeschlossenen Stellen entwickelt und die Einhaltung dieser Standards überprüft.

Aufgabe des LSI ist es auch Informationen zu aktuellen Sicherheitsrisiken zu sammeln und relevante Stellen regelmäßig über die aktuelle Sicherheitslage zu informieren. Als Kontaktstelle zum BSI gehört es zu den Aufgaben des LSI, die zuständigen Aufsichtsbehörden bayerischer Betreiber kritischer Infrastrukturen über relevante Sicherheitsvorkommnisse zu informieren.

Das LSI kann staatliche und kommunale Stellen, Betreiber kritischer Infrastrukturen und weitere Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen in Fragen der IT-Sicherheit beraten und unterstützen.

Die Polizei, die Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz können bei der Wahrnehmung ihrer gesetzlichen Aufgaben technisch unterstützt werden, insbesondere bei der Durchführung von technischen Untersuchungen oder der Datenverarbeitung.

Landesamt für Sicherheit in der Informationstechnik

Das LSI hat keine Aufsichts- oder Kontrollbefugnisse für bayerische Unternehmen, sondern bietet kostenfreie Unterstützung auf Anfrage für Betreiber kritischer Infrastrukturen und Unternehmen mit mehrheitlich staatlicher Beteiligung an.

Da Betreiber kritischer Infrastrukturen unter den jeweiligen im BSI-Gesetz definierten Schwellenwerten keine Melde- oder Berichtspflicht von IT-Sicherheitsvorfällen an das BSI haben, liegt dem LSI kein vollständiger Überblick über die aktuelle Sicherheitslandschaft bayerischer Unternehmen vor. Das LSI erhält allerdings Kenntnis von Strukturen und Vorfällen in Unternehmen, welche sich aktiv an das LSI wenden bzw. die Leistungen des LSI in Anspruch nehmen. Das LSI erhält zudem Kenntnis von akuten, noch anhaltenden, Vorfällen mit möglichem Ausfall der kritischen Dienstleistung bei bayerischen Betreibern kritischer Infrastrukturen die über den jeweiligen Schwellenwerten des BSI liegen.

Landesamt für Sicherheit in der Informationstechnik

1. Aktuelle Bedrohungslage und Angriffsarten

a) Wie hat sich die Bedrohungslage für bayerische Unternehmen in den letzten Jahren entwickelt, insbesondere vor dem Hintergrund zunehmender globaler Cyberattacken und geopolitischer Spannungen? Welche Branchen waren besonders betroffen?

- In den vergangenen Jahren hat sich die allgemeine Bedrohungslage durch Cyberangriffe nach Wahrnehmung des LSI deutlich verschärft. Diese erhöhte Bedrohungslage betrifft auch Betreiber kritischer Infrastrukturen in Bayern. Diese Entwicklung wird insbesondere bei vermehrten Vorfällen im Bereich Kliniken deutlich.
- Insgesamt ist eine zunehmende Professionalisierung von Cyberkriminellen, darunter auch staatlich motivierte Akteure und verstärkte Nutzung von KI zur Vorbereitung und Durchführung von Cyberangriffen zu beobachten.

b) Welche Cyberangriffsarten (z. B. Ransomware, Phishing, verteilter Denial-of-Service Angriff (DDoS), Advanced Persistent Threats-Angriffe (ATPs)) oder Social Engineering sind aktuell besonders relevant für Unternehmen in Bayern?

- Aus Sicht des LSI zeigt sich die Bedeutung von initialen Angriffsvektoren wie folgt:
- Der bedeutendste initiale Angriffsvektor für Cyberangriffe in allen Bereichen ist Phishing. Über die vergangenen drei Jahre verzeichnet das LSI eine enorme Zunahme an Phishing-Mails.
- An zweiter Stelle stehen aktiv ausgenutzte Soft- und Hardwareschwachstellen, die nicht rechtzeitig gepatcht wurden.
- Diese beiden initialen Angriffsvektoren bieten in der Folge ein Einfallstor für Ransomware-Angriffe, die auch in Bayern vom LSI beobachtet werden.
- DDoS-Angriffe auf Webseiten von Unternehmen sind aktuell gängiges Mittel politisch motivierter oder staatlich unterstützter Gruppierungen. Im Zuständigkeitsbereich des LSI konnten vorrangig Angriffe auf Webseiten im Bereich Kliniken und Dienstleister im Gesundheitssektor, Öffentlichen Verkehrsunternehmen und Messebetreibern festgestellt werden.
- Dem LSI sind zudem Vorfälle im Bereich Social Engineering wie beispielsweise Invoice-Fraud (die Fälschung von Rechnungen) und das Abgreifen von Kontodaten bekannt.

c) Wie können die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben die bayerischen Unternehmen bei der Abwehr und Bewältigung von Cyberangriffen unterstützen?

- Als IT-Sicherheitsbehörde des Freistaats Bayern betreibt das LSI zusammen mit dem Bayern-Server die zentralen Sicherheitsinstanzen im bayerischen Behördennetz und sorgt damit für den sicheren Betrieb staatlicher IT. Die bayerischen Kommunen können über das kommunale

Landesamt für Sicherheit in der Informationstechnik

Behördennetz partizipieren. Die in diesem Zusammenhang erlangten Erkenntnisse im Bereich Angriffserkennung und -abwehr werden im Rahmen der Unterstützung und Beratung von Kommunen und Betreibern kritischer Infrastrukturen durch das LSI geteilt.

- Das LSI stellt darüber hinaus den eigenen Zielgruppen zahlreiche Dienste und Unterstützungsangebote wie z.B.: die Bereitstellung eines Warn- und Informationsdienstes, die IP-basierten Alarmierung sowie Individualberatung, konkrete Beratungsunterlagen wie Handlungsempfehlungen, Orientierungshilfen, Leitfäden und Beispieldokumente, Informationsveranstaltungen und Awareness-Angebote zur Verfügung. Im Bereich der Bewältigung von Cyberangriffen kann das LSI auf Anfrage unterstützende, koordinierende Hilfe leisten.
- Im Falle von Cyberangriffen auf Kommunen und Betreiber kritischer Infrastrukturen stimmt sich das LSI eng mit den Partnerbehörden der Cyberabwehr Bayern ab.

2. Stand der IT-Sicherheitsmaßnahmen

a) Inwieweit ist der aktuelle Stand der IT-Sicherheitsmaßnahmen in bayerischen Unternehmen, insbesondere bei kleinen und mittleren Unternehmen (KMU) und im Bereich der kritischen Infrastruktur transparent?

- Dem LSI liegt keine abschließende Übersicht über den Stand der IT-Sicherheitsmaßnahmen bayerischer KMU und Betreiber kritischer Infrastrukturen vor, siehe Eingangsstatement.
- Betreiber kritischer Infrastrukturen, die den Schwellenwert nach BSI-Gesetz bzw. der BSI-Kritisverordnung überschreiten, müssen dem BSI regelmäßig nachweisen, dass sie IT-Sicherheit nach Stand der Technik umsetzen. Größere Firmen setzen dies oft durch IT-Sicherheitszertifizierungen um, z.B. ISO 27001, BSI Grundschutz oder Branchenspezifischen Sicherheitsstandards.

b) Welche typischen Schwachstellen und Defizite bestehen bei den Unternehmen? Wo werden die vordringlichen Handlungsbedarfe gesehen?

- Nach Kenntnis des LSI stehen bayerische Betreiber kritischer Infrastrukturen, unterhalb der Schwellenwerte nach BSI-Kritisverordnung, vor folgenden typischen Hemmnissen. Hierzu zählen hohe Kosten für die Umsetzung von Sicherheitsmaßnahmen, der Fachkräftemangel im Bereich IT-Sicherheit sowie ein oft mangelndes Bewusstsein für die Bedeutung von IT-Sicherheit im Unternehmen, gerade auf Leitungsebene.
- Das LSI beobachtet das daher stellenweise gängige Maßnahmen der IT-Sicherheit, z.B. Patchmanagement oder Multi-Faktor-Authentifizierung nicht vollständig umgesetzt werden.

Landesamt für Sicherheit in der Informationstechnik

- Aus Sicht des LSI wäre vordringlich folgendes umzusetzen: Einführung eines Information Security Management System (ISMS), die Basisabsicherung der IT-Systeme, die Einführung von Multi-Faktor-Authentifizierung (MFA), regelmäßige Sensibilisierungsmaßnahmen und Mitarbeiterschulungen, sowie die Implementierung eines Notfallmanagements.

3. Resilienz und Krisenmanagement

a) Wie gut sind bayerische Unternehmen auf größere Cybervorfälle vorbereitet? Gibt es beispielsweise Notfallpläne, Quick-Response-Teams (QRTs) und regelmäßige Übungen?
   - Dem LSI liegt keine abschließende Übersicht zu vorbereitenden Maßnahmen bayerischer Unternehmen vor.
   - Betreiber kritischer Infrastrukturen unterstützt das LSI hier zum Beispiel mit der Bereitstellung von Table-Top-Übungen, einer Handreichung zum Notfallmanagement, einem Ransomware-Leitfaden, einer IT-Sicherheitskampagne und einer Anleitung zur Durchführung von Phishing-Simulationen.

b) Wie bewerten Sie die Notfallversorgung im Stromausfall (z. B. auch via Dieselgeneratoren) speziell bei Rechenzentren in Bayern?
   - Die bayerischen staatlichen Rechenzentren sind nach Kenntnis des LSI ausreichend gegen Stromausfall abgesichert. Zu anderen Rechenzentren in Bayern liegen dem LSI keine Erkenntnisse vor.

c) Welche Erfahrungen gibt es mit der Wiederherstellung nach erfolgreichen Angriffen (Recovery-Zeit, Datenverluste)?
   - Die Recovery-Zeit und das Eintreten von Datenverlusten sind hochgradig von Art und Schwere des Vorfalls und der Vorbereitung des Unternehmens für derartige Notfälle abhängig. Bei Kliniken die in jüngerer Vergangenheit einen Ransomwareangriff zu bewältigen hatten dauerte die vollständige Wiederherstellung der Kernprozesse beispielsweise mehrere Monate. Analoge Erfahrungen können auch bei Kommunalverwaltungen beobachtet werden.
   - Von Lösegeldzahlungen bei Ransomwareangriffen zur Wiedererlangung der Daten rät das LSI grundsätzlich ab um Nachahmer zu vermeiden. Durch Zahlungen ist auch nicht sichergestellt, dass tatsächlich wieder ein Zugriff auf die Daten ermöglicht wird, oder kein Schadcode auf den Systemen unerkannt verbleibt.

Landesamt für Sicherheit in der Informationstechnik

d) Liegen Erkenntnisse vor, inwieweit der kurzfristige Wegfall grundlegender digitaler Dienste von Drittstaatsanbietern wie Cloud-Diensten in den Notfallplänen/Business Continuity -Plänen der bayerischen Unternehmen durch geeignete Vorkehrungen berücksichtigt wird?
- Dem LSI liegen keine Kenntnisse über Notfallpläne/BCM bayerischer Unternehmen bezüglich des kurzfristigen Ausfalls digitaler Dienste vor.
- Das LSI empfiehlt im Rahmen seiner Beratungstätigkeit die Erstellung von Notfallplänen bzw. die Einführung eines BCM.
- Das LSI geht davon aus, dass mit der Umsetzung der NIS-2-Richtlinie auf Bundesebene betroffene Unternehmen zur Aufstellung von Notfallplänen verpflichtet werden. Soweit Unternehmen sich an Standards wie ISO 27001 und IT-Grundschutz halten, sind entsprechende Maßnahmen vorzusehen.

4. Lieferketten, digitale Resilienz und digitale Souveränität

a) Wie können einheitliche IT-Sicherheitsstandards entlang der gesamten Wertschöpfungskette etabliert und durchgesetzt werden?
- Durch die Umsetzung gesetzlicher Vorgaben wie beispielsweise der NIS-2-Richtlinie könnte bei Unternehmen im Anwendungsbereich ein einheitliches Mindestniveau bezüglich IT-Sicherheit erreicht werden. Durch dabei gestellte Anforderungen an Unternehmen in der Lieferkette würde auch bei diesen, nicht unmittelbar betroffenen Unternehmen, das IT-Sicherheitsniveau ebenfalls steigen.
- Aus Sicht des LSI sollten Unternehmen verstärkt auf IT-Sicherheit bei ihren Zulieferern achten. Hierbei können beispielsweise Zertifizierungen (wie ISO 27001), oder die Einhaltung branchenspezifischer Sicherheitsstandards verlangt werden. Die Einhaltung solcher Standards und Normen ist in der Gesamtschau ein Wettbewerbsvorteil.
- In einigen Sektoren der kritischen Infrastrukturen gibt es branchenspezifische Sicherheitsstandards – B3S. Beispielsweise der branchenspezifische Sicherheitsstandard „Medizinische Versorgung“ in dem auch Anforderungen an Lieferanten und Dienstleister gestellt werden. Eine Einführung in andere Branchen wäre empfehlenswert.

b) Inwieweit bestehen Abhängigkeiten für bayerische Unternehmen von internationalen Cloud- und IT-Infrastrukturanbietern und ggf. welche Risiken ergeben sich hierdurch?
- Generell führt IT-Outsourcing immer zu einer gewissen Abhängigkeit, gerade bei Technologien wie Cloud-Dienstleistungen ist das der Fall. Der Markt in diesen Bereichen ist im Allgemeinen sehr durch internationale Anbieter geprägt.

Landesamt für Sicherheit in der Informationstechnik

- In manchen KRITIS-Bereichen ist aufgrund einer geringen Anzahl potenzieller Anbieter von einer höheren Abhängigkeit auszugehen. Diese Abhängigkeiten bestehen sowohl national als auch international.
- Möglichen Risiken sind der Verlust der Kontrolle über die eigenen Daten. Gerade bei Anbietern außerhalb der EU bestehen gegebenenfalls gesetzliche Regelungen die europäischen Regelungen entgegenstehen. So können zum Beispiel die Zugriffsberechtigungen auf Daten durch ausländische Ermittlungsbehörden und Nachrichtendienste unterschiedlich geregelt sein.
- Des Weiteren können politische Konflikte Auswirkungen auf die Verfügbarkeit von Cloud-Diensten oder Infrastrukturkomponenten haben.
- Grundsätzlich ist bei der Auswahl von Cloud-Dienstleistern darauf zu achten, dass diese für eine ausreichende Absicherung der Dienste und Daten sorgen, dies kann beispielsweise durch vertragliche Regelungen (Service Level Agreement und Zertifizierungen) sichergestellt werden.
- Der zu starken Bindung an einen Anbieter (Vendor Lock-in) sollte präventiv durch eine Exit-Strategie entgegengewirkt werden.

c) Welche Maßnahmen könnten zur Stärkung der digitalen Souveränität und zur Förderung europäischer Alternativen beitragen?
   - Aus Sicht des LSI zielt die Frage auf grundlegende Weichenstellungen im Rahmen der Europäischen Wirtschaftspolitik ab.
   - Unternehmen agieren vor allem auf Basis wirtschaftlicher Entscheidungen. Eine breite Palette möglicher Anbieter kann insgesamt für eine geeignete wettbewerbliche Umgebung sorgen.
   - Gerade im KI und Cloud Umfeld bestehen auch für Europäische Lösungen aktuell neue Möglichkeiten.

5. Regulatorische Anforderungen und Umsetzung

a) Welche gesetzlichen Vorgaben zur Einhaltung von IT-Sicherheit, insbesondere zu Standards und Zertifizierungen, bestehen für bayerische Unternehmen?
   - Bayerische Betreiber kritischer Infrastrukturen unterliegen den Vorgaben des BSI-Gesetzes, wenn sie in einen der bezeichneten KRITIS-Sektoren fallen und dabei die in der BSI-Kritisverordnung festgelegten sektorspezifischen Schwellenwerte überschreiten. Im Bereich der Trinkwasserversorgung liegt dieser beispielsweise bei 22 Mio. m³ pro Jahr, dies entspricht einer Trinkwasserversorgung von rund 500.000 Einwohnern.
   - Im BSI-Gesetz werden für diese Einrichtungen Anforderungen an die IT-Sicherheit gestellt, unter anderem das Treffen angemessener organisatorischer und technischer Vorkehrungen, sowie Nachweispflicht

Landesamt für Sicherheit in der Informationstechnik

und Meldepflichten gegenüber dem BSI. Nachweise können beispielsweise durch eine Zertifizierung, Audits oder Prüfungen erfolgen.

- Darüber hinaus gibt es für einige KRITIS-Sektoren noch weitere sektorspezifische Regelungen, wie beispielsweise im Sozialgesetzbuch V (Krankenhäuser), Energiewirtschaftsgesetz (EnWG, Strom-/Gasnetze), Telekommunikationsgesetz (TKG), Digital Operational Resilience Act (DORA, Banken, Versicherungen).
- Zukünftig werden mehr bayerische Unternehmen durch die Umsetzung der europäischen NIS-2-Richtlinie durch den Bund reguliert und müssen Cybersicherheitsvorgaben umsetzen.
- Hierbei sind nicht nur kritische Infrastrukturen, sondern auch Unternehmen betroffen, die in eine bestimmte Branche fallen und bestimmte Dienstleistungen anbieten (vergleiche Anlage 1 und 2 der NIS-2-Richtlinie).
- Hier wird zwischen wichtigen und besonders wichtigen Einrichtungen und Betreiber kritischer Anlagen unterschieden. Unterscheidungskriterien sind die Mitarbeiterzahl (50 bzw. 250 Mitarbeiter) und der Umsatz des Unternehmens (10 bzw. 50 Mio. €). Die bisherigen Betreiber kritischer Infrastrukturen fallen in die Kategorie kritische Anlagen. Je nach Zuordnung zu diesen drei Gruppen erhöht sich Art und Umfang der umzusetzenden Maßnahmen zur Cybersicherheit.
- Der Cyber Resilience Act (CRA) gibt für Produkthersteller einheitliche Sicherheitsstandards für vernetzte Soft- und Hardwareprodukte vor.
- Im Bereich des Datenschutzes machen die Datenschutz-Grundverordnung (DSGVO) und das deutsche Bundesdatenschutzgesetz Unternehmen Vorgaben zum Schutz personenbezogener Daten, die auch IT-Sicherheit betreffen.

b) Welche Herausforderungen bestehen für bayerische Unternehmen aus Expertinnen- und Expertensicht bei der Umsetzung? Wo bestehen ggf. Unterstützungsmöglichkeiten durch staatliche Stellen?

- Unternehmen benötigen einen Überblick über die sie betreffenden Regulierungen und deren Umfang, um erfolgreich Maßnahmen ergreifen zu können. Für die Umsetzung der Vorgaben sind entsprechendes Know-how sowie ausreichende finanzielle Mittel erforderlich. So zeigen Studien (TÜV Cybersecurity Studie 2025) und Gespräche des LSI, dass beispielsweise die NIS-2-Richtlinie nicht bei allen Unternehmen bekannt ist.
- Grundvoraussetzung für die erfolgreiche Umsetzung von IT-Sicherheitsmaßnahmen ist die Unterstützung durch die Führungsebene. Hier sind Kenntnisse zur eigenen Verantwortung und in Bezug auf die aktuelle Gefährdungslage unerlässlich.
- Des Weiteren kann sich speziell im KRITIS-Bereich die Erbringung der geforderten Nachweise schwierig gestalten, da ein begrenztes Anbieterumfeld für Audits und Zertifizierungen besteht.

Landesamt für Sicherheit in der Informationstechnik

- Das LSI unterstützt vor allem öffentliche Betreiber kritischer Infrastrukturen in Bayern durch Handlungsempfehlungen und Leitfäden, Sensibilisierungsangebote sowie branchenspezifische Veranstaltungen. Ergänzt wird das Angebot des LSI durch die IP-basierte Alarmierung und den kostenfreien Warn- und Informationsdienst, der Betreibern tagesaktuelle Informationen beispielsweise zu Schwachstellen liefert. Das LSI baut seine Angebote entsprechend der aktuellen Gefährdungslage und technischen Entwicklungen kontinuierlich aus.

c) Welche möglichen Nachteile ergeben sich für die Wettbewerbsfähigkeit bayerischer Unternehmen im Bereich IT- und Cybersicherheit durch nationale oder europäische Regulierung (z. B. zusätzliche Bürokratie)?
   - Mögliche Nachteile, die sich aus einer Regulierung ergeben, sind unter anderem höhere Kosten (z. B. durch komplexere Prozesse, höheren Personalbedarf, Audits) und höhere Ressourcenbindung (z. B. Arbeitszeit und Personalauslastung). Unternehmen im nicht-europäischen Ausland unterliegen diesen Vorgaben ggf. nicht.
   - Aufgrund des teilweise existenzbedrohenden und des insgesamt hohen Schadenspotenzials von Cyberangriffen stellen diese Aufwendungen aus Sicht des LSI in einer Gesamtschau keinen Wettbewerbsnachteil, eher einen Vorteil dar, da die Resilienz der Unternehmen gegen täglich stattfindende Cyberangriffe deutlich verbessert wird.

6. Wirtschaftliche Auswirkungen und Kosten

a) Welche wirtschaftlichen Schäden entstehen durch Cyberangriffe auf Unternehmen in Bayern? Inwieweit kam es dadurch bisher zu spürbaren Einschränkungen der laufenden Produktion?
   - Dem LSI liegen hierzu keine eigenen Erkenntnisse vor.
   - Der aktuelle Wirtschaftsschutzbericht des Branchenverbands bitkom (2025) beziffert den Gesamtschaden durch Cyberattacken in Deutschland im vergangenen Jahr auf rund 200 Milliarden Euro.
   - Erfahrungen des LSI zeigen, dass Vorfälle bei Betreibern kritischer Infrastrukturen regelmäßig hohe finanzielle Schäden nach sich ziehen. Bei einem dem LSI bekannt gewordenen Ausfall einer größeren Klinik in Bayern mussten im Nachgang für Wiederaufbau und Modernisierung der digitalen Infrastruktur 6,8 Millionen Euro aufgewendet werden. Die Einrichtung musste sich zeitweise von der Notfallversorgung abmelden.

b) Welche Dunkelziffer ist bei gemeldeten Schäden realistisch anzunehmen?
   - Dem LSI liegen hierzu keine Erkenntnisse vor.

Landesamt für Sicherheit in der Informationstechnik

c) Wie bewerten Sie die Kosten-Nutzen-Relation von Investitionen in IT-Sicherheit, insbesondere für KMU?
- Das hohe Schadenspotenzial von Cyberrangriffen rechtfertigt aus Sicht des LSI angemessene Investitionen in IT-Sicherheit. Als Richtwert kann von ca. 20 % des IT-Budgets für Cybersicherheit ausgegangen werden. Die Investitionen sollten zur Umsetzung angemessener, zielgerichteter und effektiver Maßnahmen getätigt werden.
- Der Branchenverband bitkom geht in seinem Wirtschaftsschutzbericht 2025 davon aus, dass 87 % der befragten Unternehmen von „Diebstahl, Industriespionage und Sabotage“ konkret betroffen und 10 % vermutlich betroffen waren.

d) In welchen wirtschaftlichen Nischen im Bereich Cybersicherheit haben bayerische IT-Unternehmen besondere Stärken oder Chancen in der internationalen Arbeitsteilung?
- Zu dieser Frage liegen dem LSI keine Informationen vor.

7. Sensibilisierung, Ausbildung und Fachkräftemangel

a) Wie ist der Stand der Sensibilisierung und Weiterbildung im Bereich IT-Sicherheit in Unternehmen?
- Dem LSI liegt keine Gesamtübersicht zum Stand der Sensibilisierung zum Thema IT-Sicherheit in bayerischen Unternehmen vor.
- Nach Einschätzung des LSI ist der Stellenwert von Sensibilisierungsmaßnahmen bei Betreibern kritischer Infrastrukturen sehr heterogen.
- Zukünftig werden Unternehmen, die von der NIS-2-Richtlinie betroffen sind, dazu verpflichtet, ihre Mitarbeiter sowie die Geschäftsleitung angemessen bezüglich IT-Sicherheit regelmäßig zu schulen.
- Das LSI unterstützt mit Sensibilisierungsangeboten für Betreiber kritischer Infrastrukturen zum Beispiel durch Bereitstellung von Table-Top-Übungen, Informationsmaterialien und Mustervorlagen zu den Themen Notfallmanagement, Ransomware, Awareness und NIS-2-Richtlinie. Das Angebot wird entsprechend der Sicherheitslage und der technischen Entwicklungen fortwährend überarbeitet und ausgeweitet.

b) Gibt es ausreichend qualifiziertes Personal, um die IT-Sicherheit in Unternehmen zu gewährleisten? Wo sehen Sie etwaige Engpässe und deren Ursachen?
- Betreiber kritischer Infrastrukturen berichten gegenüber dem LSI, dass die Gewinnung von qualifizierten Mitarbeitern problematisch sei.

Landesamt für Sicherheit in der Informationstechnik

c) Wie kann die Aus- und Weiterbildung von IT-Sicherheitsfachkräften an bayerischen Hoch- und Berufsschulen verbessert werden?
   - Neben spezifischen Studiengängen für IT-Sicherheit sollte auch für Ausbildungen und Studiengänge mit IT-Bezug ein höherer Anteil für IT-Sicherheit vorgesehen werden. Beispielsweise in Form von spezifischen Vorlesungen und praktischen Übungen oder auch verzahnt im gesamten Lehrplan.

8. Zukunftsperspektiven und Innovation

a) Welche technologischen Trends (z. B. Künstliche Intelligenz, Cloud-Lösungen) beeinflussen die IT-Sicherheitslage aktuell und künftig?
   - Sowohl der Einsatz von Cloud-Lösungen als auch KI beeinflusst aus Sicht des LSI die IT-Sicherheitslage aktuell und künftig.
   - Beide Technologien können einerseits dazu verwendet werden, um die IT-Sicherheit zu verbessern. Andererseits können durch deren Nutzung aber auch neue Schwachstellen entstehen.
   - Vor allem KI-Anwendungen können in der Hand von Kriminellen gefährliche Werkzeuge darstellen. Bei Angriffen mit KI ist zukünftig verstärkt mit Deepfakes (durch KI erzeugte oder manipulierte Bild-, Ton- oder Videoinhalte, die täuschend echt wirken), Vishing (ein Betrugsversuch, bei dem Betrüger Telefonanrufe nutzen, um sensible persönliche Informationen zu erlangen) und Spear Phishing (senden von stark personalisierten E-Mails oder Nachrichten an eine bestimmte Person oder Organisation, um sensible Daten zu erlangen oder Malware einzuschleusen) zu rechnen.
   - KI kann aber auch für Maßnahmen zur Verteidigung eingesetzt werden, um zum Beispiel große Datenmengen in Echtzeit zu analysieren. Hierdurch lassen sich Anomalien entdecken, die auf eine Kompromittierung hinweisen.
   - Cloud-Lösungen führen ebenfalls zu neuen Herausforderungen und Anforderungen in der IT-Sicherheit. Beispiele hierfür sind die Absicherung von Cloud-Zugängen und die Vergabe von Berechtigungen. Dies sind Aufgaben, die auch im Rahmen einer Migration in die Cloud bei den einzelnen Firmen verbleiben und bei Fehlkonfiguration Einfallsvektoren für Angreifer darstellen können.
   - Die Weiterentwicklung von Quantencomputern bringt neben Chancen auch erhebliche Risiken im Bereich IT-Sicherheit mit sich. Besonders die Möglichkeit, dass künftig leistungsfähigere Quantencomputer etablierte kryptografische Verfahren überwinden könnten, macht die frühzeitige Vorbereitung auf quantensichere Sicherheitstechnologien zu einer dringlichen strategischen Aufgabe. Davon unabhängig ist die Verbreiterung der algorithmischen Basis allgemein wichtig, um die Resilienz in der Kryptographie zu erhöhen. Vor diesem Hintergrund betrachtet das LSI die

Post-Quanten-Kryptografie als wesentliche Schlüsseltechnologie, um die langfristige Vertraulichkeit und Integrität von Daten sicherzustellen.

b) Wie kann Bayern als Wirtschaftsstandort die digitale Souveränität stärken und Abhängigkeiten von internationalen IT-Anbietern verringern?
- Investitionen in europäische IT-Anbieter und Lösungen sowie in Forschung können Abhängigkeiten insgesamt verringern.
- Durch Nutzung von Open-Source-Lösungen und offenen Standards kann ein Vendor Lock-in verhindert werden.

9. Empfehlungen für die Politik

a) Inwieweit kann die Politik bayerische Unternehmen dabei unterstützen, ihre IT-Sicherheit weiter zu stärken?
- Aufgrund des gesetzlichen Auftrags des LSI wird diese Frage im Hinblick auf Betreiber kritischer Infrastrukturen beantwortet.
- Förderprogramme stellen eine Möglichkeit dar, Betreiber kritischer Infrastrukturen bei der Umsetzung von IT-Sicherheitsmaßnahmen zu unterstützen, wie beispielsweise der Einführung eines Information Security Management System (ISMS).
- Eine adäquate Ausstattung der bayerischen Bildungseinrichtungen mit genügend finanziellen Mitteln sichert die Ausbildung zukünftiger IT-Experten und Innovationen. Der Blick darf hierbei nicht nur auf Hochschulen gerichtet werden – bereits in den Schulen müssen hierfür die Grundlagen geschaffen werden und Interesse an IT im Allgemeinen und IT-Sicherheit im Speziellen geweckt werden.
- Die Unterstützungsangebote des LSI für Betreiber kritischer Infrastrukturen in Bayern werden gut angenommen. Diese kostenfreien Angebote sollten aufrechterhalten, weiterentwickelt und ausgeweitet werden.

b) Wie werden aktuell verfolgte Maßnahmen auf Bundes- und Landesebene dahingehend bewertet?
- Der aktuelle Entwurf des BSI-Gesetzes zur Umsetzung der NIS-2-Richtlinie sieht vor, dass Betreiber kritischer Infrastrukturen Maßnahmen zur IT-Sicherheit umsetzen. Aus Sicht des LSI ist dies ein geeignetes Mittel um die IT-Sicherheit in bayerischen Unternehmen zu verbessern.
- Eine geeignete Maßnahme wäre zudem eine finanzielle Förderung. Neben der direkten Förderung von IT-Sicherheitsmaßnahmen, wie beispielsweise der Einführung eines Information Security Management System (ISMS), sind weitere Varianten denkbar.
- Die zweckgebundene Bereitstellung von Fördermitteln wie zum Beispiel im Rahmen des Krankenhauszukunftsgesetz des Bundes (hier 15% der

Landesamt für Sicherheit in der Informationstechnik

Fördersumme für IT-Sicherheitsmaßnahmen) sind aus Sicht des LSI positiv zu bewerten.

- Ausbau und Festigung von Kooperationen auf Bundes- und Landesebene der Fachbehörden tragen zu einer stetigen Verbesserung des Lagebildes und zu einer schnelleren und zielgerichteteren Reaktion bei Cybersicherheitsvorfällen bei.

c) Wo werden Potenziale gesehen, die Zusammenarbeit von Staat, Wirtschaft und Forschung zur Erhöhung der Resilienz gegen Cyberbedrohungen weiter zu verbessern?

- Kooperations- und Austauschplattformen für Staat, Wirtschaft und Forschung sollten etabliert und gefördert werden: Die Stärkung bewährter Formate wie des CERT-Verbundes (CV) und der Austausch zu allgemeinen IT-Sicherheitsthemen, aktuellen Schwachstellen und Angriffstechniken sowie Bildungs- und Sensibilisierungsmaßnahmen sind nur einige Beispiele. Formate hierbei können unter anderem Informationsveranstaltungen, Workshops und Schulungspakete sein. Auch ein technischer Austausch sollte etabliert werden (beispielsweise Malware Information Sharing Platform für IOCs, Wissensdatenbank zu APT-Gruppen und Angriffsvektoren).
- Forschungskooperationen zwischen Cybersicherheitsbehörden des Freistaats und Forschungseinrichtungen sowie Hochschulen sollten weiter ausgebaut werden.

16.November 2025

Marc Luczak

BMW Group

Head of Information Security (Financial Services)
Lilienthalallee 26

80939 München

Postanschrift:
80787 München
Mobil: +49-151-601-27870
Mail: marc.luczak@bmw.de
Web: http://www.bmwgroup.com/

Bezug:

Anhörung von Sachverständigen Anhörung gemäß § 173 der Geschäftsordnung für den Bayerischen Landtag zum Thema IT-Sicherheit in der bayerischen Wirtschaft
Donnerstag, 27. November 2025

Fragenkatalog vom 29.10.2025

1. Aktuelle Bedrohungslage und Angriffsarten

   In den letzten Jahren ist die Anzahl der Cyberangriffe signifikant gestiegen. Nicht nur das Volumen, sondern auch die Komplexität und Geschwindigkeit der Angriffe haben erheblich zugenommen. Moderne Angriffsmethoden sind hochoptimiert und nutzen zunehmend Künstliche Intelligenz, um raffinierte Phishing-Versuche über gefälschte Webseiten, Nachrichten, E-Mails sowie manipulierte Benutzeridentitäten und Zugriffsrechte durchzuführen.
   Die Angriffe lassen sich grob in zwei Motivationsarten unterteilen: monetär motivierte Attacken, wie Erpressung durch Schadsoftware (z. B. Ransomware), sowie Angriffe zum Diebstahl von Daten und Informationen mit dem Ziel, sich Wettbewerbsvorteile zu verschaffen – etwa im Bereich Forschung, Technik und Finanzen. Als bedeutendes Industrieland ist Bayern in nahezu allen Angriffsvektoren betroffen, besonders die Automobil- und Finanzindustrie verzeichnen seit über einem Jahrzehnt eine signifikante Zunahme und erfolgreiche Angriffe.
   Eine besondere Herausforderung stellt die Vermischung von Social-Media-Aktivitäten im Privatbereich mit der Digitalisierung in der Wirtschaft dar, was neue Angriffsflächen schafft. Darüber hinaus stellen Bedrohungen für Netzwerke und Anwendungen, wie DDoS-Attacken mit dem Ziel der Schädigung, eine zunehmende Gefahr dar.

Auch das Internet der Dinge (IoT) – beispielsweise vernetzte Haushaltsgeräte, Gebäude mit Sensorik und Fahrzeuge – eröffnet neue Angriffsvektoren. In den letzten Monaten wurde zudem eine Zunahme bösartiger Webaktivitäten festgestellt, insbesondere sogenannte Multi-Terabit-DDoS-Angriffe, auch „Internet Tsunamis“ genannt, die deutlich an Häufigkeit und Intensität zugenommen haben.
Diese Entwicklungen verdeutlichen die steigende Bedrohungslage für bayerische Unternehmen und Privathaushalte und unterstreichen die Dringlichkeit effektiver IT-Sicherheitsmaßnahmen.

2. Stand der IT-Sicherheitsmaßnahmen

In großen Unternehmen wurden in den letzten Jahren erhebliche Ressourcen für die IT-Sicherheit aufgebaut. Ein Information Security Management System (ISMS) ist angesichts der heutigen regulatorischen Anforderungen unverzichtbar geworden.
Kleine und mittelständische Unternehmen (KMU) verfügen ebenfalls über sensible Schutzobjekte, wie beispielsweise Kundendaten. Für viele KMU stellt insbesondere die Einhaltung der Datenschutz-Grundverordnung (DSGVO) eine umfangreiche Herausforderung dar. Ein umfassendes und lückenloses Bild der Schutzobjekte und IT-Systeme ist in KMU häufig nur unzureichend vorhanden. Dies erschwert die Implementierung vorbeugender Maßnahmen erheblich, sodass erfolgreiche Angriffe oftmals spät erkannt und klassifiziert werden.
Die Bedeutung der IT-Sicherheit ist in den letzten Jahren deutlich gestiegen. KMU sind – ähnlich wie große Unternehmen – von den Folgen erfolgreicher Angriffe betroffen, die erhebliche Auswirkungen wie Produktionsausfälle, Datenverluste und den Verlust von Kundenvertrauen nach sich ziehen können. Die Transparenz über Angriffe und die effektive Abwehr stellen für KMU eine besondere Herausforderung dar.

3. Resilienz und Krisenmanagement

Stand und Fortschritte im Business Continuity Management (BCM) bei BMW SF

Für BMW SF lässt sich festhalten, dass in den letzten Jahren erhebliche Fortschritte im Bereich Business Continuity Management (BCM) erzielt wurden. Kritische Prozesse sind durch redundante Abläufe abgesichert, wodurch eine hohe Ausfallsicherheit gewährleistet wird. Notfallvorsorgekonzepte haben sich in regelmäßigen Übungen mit realen Szenarien als praktikabel und zuverlässig erwiesen.

Die regulatorischen Anforderungen wurden zunächst durch MaRisk und ISO 27001 (ISMS) abgedeckt und werden aktuell durch die EU-Verordnung DORA (Digital Operational Resilience Act) weiter gestärkt, die speziell die digitale und operative Resilienz von Finanzunternehmen verbessert.

Ein zentraler Bestandteil des BCM ist die Sicherstellung der geografischen Redundanz (Geo-Redundanz). So hat BMW SF gemeinsam mit Noris Network vor einigen Jahren ein großes Rechenzentrum in Aschheim bei München errichtet. Dieses Rechenzentrum verfügt über redundante Systeme, die im Notfall schnell und effizient einspringen können. Darüber hinaus decken die Konzepte zahlreiche Bedrohungsszenarien gemäß BSI-Standard 100-4 (Notfallmanagement) ab. Die redundante Betriebsführung von Rechenzentren ist mit hohen Kosten verbunden, dient jedoch der Sicherstellung der Handlungsfähigkeit in kritischen Situationen – vergleichbar mit dem Konzept der Geo-Redundanz bei der Bundeswehr, die die Funktionsfähigkeit wichtiger Führungsstrukturen im Notfall gewährleisten soll.

Bei BMW SF werden Risiken im Kontext von Ausfallrisiken für kritische Prozesse und Auftragsdatenverarbeitung systematisch bewertet. Dabei reicht die Bewertung von kurzen Incidents bis hin zu Emergency-Cases. Sowohl Provider als auch deren Dienstleistungen werden hinsichtlich ihrer Resilienz geprüft, wodurch ein hohes Maß an Transparenz über operative Risiken geschaffen wird. Firmeninterne operative Risiken werden ebenfalls erfasst, wobei keine Volumina genannt werden.

4. Lieferketten, digitale Resilienz und digitale Souveränität

Risiken und Herausforderungen bei der Nutzung gängiger Cloud-Anbieter

Das Risiko bei der Nutzung gängiger Cloud-Anbieter, insbesondere US-amerikanischer Anbieter, wird von vielen Unternehmen als erheblich eingestuft. Für einige Unternehmen stellt die Abhängigkeit von US-Cloud-Diensten das größte operative Risiko dar. Hierbei werden insbesondere Szenarien eines Ausfalls der Cloud-Infrastruktur in den USA – etwa bedingt durch politische oder andere unvorhersehbare Ereignisse – als potenzielle Gefahrenquelle betrachtet.

Die Cloud-Strategien in Unternehmen sind daher uneinheitlich. Es bestehen Bedenken hinsichtlich der Speicherung und Verarbeitung von Daten in der Cloud, insbesondere in Bezug auf die Kompatibilität mit lokalen gesetzlichen und regulatorischen Anforderungen.

Darüber hinaus führt die Nutzung unterschiedlicher Plattformen – wie On-Premise-Systeme, Cloud-Dienste und mobile Endgeräte – zu einer hohen

Komplexität in der IT-Landschaft. Die Mischform der Nutzung verschiedener Technologien (Hybrid- oder Multi-Cloud-Umgebungen) erschwert die ganzheitliche Steuerung und Absicherung der IT-Infrastruktur erheblich.

5. Regulatorische Anforderungen und Umsetzung

BMW Financial Services unterliegt einer Vielzahl regulatorischer Anforderungen, darunter TISAX, ISO 27001 sowie neuerdings der EU-Verordnung DORA. Diese Regularien werden von unterschiedlichen Aufsichts- und Regulierungsbehörden vorgegeben und definieren Standards zur Implementierung verschiedener Sicherheits- und Datenschutzmaßnahmen, insbesondere im Bereich IT-Sicherheit und dem Umgang mit personenbezogenen Kundendaten.
Die Umsetzung dieser Maßnahmen dient überwiegend direkt oder indirekt der Sicherstellung des Geschäftsbetriebs. Ein konsolidiertes Risikomanagement bewertet und gewichtet die Maßnahmen, sodass eine fundierte Abwägung des Risikoakzeptanzniveaus möglich ist. Die Maßnahmen werden somit überwiegend aus eigenem Interesse umgesetzt; nur ein kleiner Anteil erfolgt ausschließlich zur Erfüllung regulatorischer Vorgaben.
Eine wesentliche Herausforderung liegt in der Koordination und kontinuierlichen Aktualisierung der Maßnahmen, da die Regularien einem steten Verschärfungsprozess unterliegen. Dies führt häufig zu einem erheblichen Mehraufwand und wirkt als Hemmnis für innovative IT-Projekte, da ein großer Teil des geplanten Budgets für regulatorische Maßnahmen gebunden ist und somit nur begrenzt Mittel für andere Aktivitäten zur Verfügung stehen.
Zusammenfassend lässt sich festhalten, dass die zunehmende Regulatorik nicht zwangsläufig zu einer unmittelbaren Erhöhung der IT-Sicherheit führt, sondern zunächst Ressourcen und Budget bindet, was potenziell einen Wettbewerbsnachteil für das Unternehmen darstellt.

6. Wirtschaftliche Auswirkungen und Kosten

In den vergangenen Jahren ist in Bayern eine deutliche Zunahme der Anzahl von Cyberangriffen zu verzeichnen. Der Freistaat Bayern meldet aktuell etwa 45.000 bis 48.000 Fälle von Cyberkriminalität.
Ohne konkrete Einzelfalldaten zu nennen, entstehen der BMW SF sowohl direkte als auch indirekte Kosten, die im Zusammenhang mit der Abwehr und der Begrenzung von Schäden nach einem eingetretenen Vorfall stehen. Die Nennung konkreter Vorfälle ist aufgrund betrieblicher Geheimhaltungspflichten nicht möglich.

7. Sensibilisierung, Ausbildung und Fachkräftemangel.

   Die Sensibilisierung und Weiterbildung im Bereich IT-Sicherheit hat in den letzten Jahren deutlich an Bedeutung gewonnen. Viele Unternehmen erkennen die Notwendigkeit, ihre Mitarbeitenden regelmäßig zu schulen, um den wachsenden Bedrohungen im Cyberraum wirksam begegnen zu können.
   Große Unternehmen wie BMW SF verfügen dabei gegenüber kleinen und mittelständischen Unternehmen (KMU) über Vorteile. Während größere Unternehmen häufig strukturierte Programme zur IT-Sicherheitsweiterbildung etabliert haben, besteht in KMU oft noch Nachholbedarf.
   Derzeit besteht ein deutlicher Fachkräftemangel im Bereich IT-Sicherheit, wodurch geeignete Kandidaten für viele Unternehmen sehr gefragt sind. Insbesondere fehlen Experten mit tiefgreifendem Know-how in spezialisierten Bereichen wie Incident Response oder IT-Forensik. Ursachen hierfür sind unter anderem die rasante technologische Entwicklung der letzten Jahre.
   Vor diesem Hintergrund sind Unternehmen verstärkt auf externe Dienstleister angewiesen, was langfristig jedoch nicht immer eine nachhaltige Lösung darstellt und zudem mit erheblichen Kosten verbunden ist.

8. Zukunftsperspektiven und Innovation

   Aktuelle und künftige technologische Trends wie Künstliche Intelligenz (KI) und Cloud-Lösungen haben einen maßgeblichen Einfluss auf die IT-Sicherheitslage. „Wir haben ein klares Ziel, dass in absehbarer Zeit jeder unserer Prozesse von KI unterstützt wird“ (Oliver Zipse, Vorsitzender des Vorstandes der BMW AG).
   Künstliche Intelligenz ermöglicht einerseits eine verbesserte Erkennung und Abwehr von Cyberangriffen durch automatisierte Analyse großer Datenmengen und Mustererkennung. Andererseits eröffnet KI potenziellen Angreifern neue Angriffsmöglichkeiten, beispielsweise durch die Automatisierung von Phishing-Attacken oder den Diebstahl von Identitäten.
   Die BMW SF stellt kontinuierlich On-Premise-Anwendungen auf Cloud-Lösungen um. Diese bieten flexible und skalierbare IT-Infrastrukturen, bringen jedoch zugleich neue Herausforderungen hinsichtlich Datenschutz, Zugriffs- und Identitätsmanagement sowie der Absicherung verteilter Systeme mit sich.
   Die fortschreitende Digitalisierung und Vernetzung erfordern daher kontinuierliche Anpassungen der Sicherheitsstrategie im Unternehmen. Um eine adäquate Risikosteuerung zu gewährleisten, ist eine Kombination aus Ressourcen, Fähigkeiten und letztlich dem Willen zur Umsetzung erforderlich.

9. Empfehlungen für die Politik

Die Politik kann bayerische Unternehmen auf vielfältige Weise dabei unterstützen, ihre IT-Sicherheit weiter zu stärken. Dazu zählen insbesondere die Förderung von Weiterbildungs- und Sensibilisierungsprogrammen sowie die finanzielle Unterstützung von kleinen und mittelständischen Unternehmen (KMU) bei Investitionen in moderne Sicherheitstechnologien.
Besonders hilfreich ist die Verschlankung des regulatorischen Rahmens, um den Unternehmen kontinuierliche Handlungssicherheit zu gewährleisten. Bürokratische Hürden bei der Umsetzung von IT-Sicherheitsmaßnahmen könnten dadurch reduziert werden.
Darüber hinaus kann die Politik den Ausbau digitaler Infrastrukturen vorantreiben und den Zugang zu Expertenwissen erleichtern, beispielsweise durch den Aufbau von Kompetenzzentren und Netzwerken zur IT-Sicherheitsforschung.
Ein weiterer wesentlicher Hebel zur Stärkung der IT-Sicherheit in Bayern liegt im Ausbau von Studiengängen und Ausbildungsangeboten im Bereich IT-Sicherheit. Durch die gezielte Förderung und Erweiterung entsprechender akademischer und beruflicher Bildungsprogramme kann dem bestehenden Fachkräftemangel entgegengewirkt werden. Insbesondere sollten praxisnahe und interdisziplinäre Studiengänge entwickelt werden, die aktuelle technologische Entwicklungen sowie die Anforderungen der Wirtschaft berücksichtigen. Kooperationen zwischen Hochschulen, Unternehmen und Forschungseinrichtungen sind dabei von großer Bedeutung, um eine praxisorientierte Ausbildung und eine kontinuierliche Anpassung der Lehrinhalte sicherzustellen.

Fazit:

Bayerische Unternehmen stehen im Bereich IT-Sicherheit sowohl vor großen Chancen als auch erheblichen Risiken. Moderne Technologien sind essenziell, um die Wettbewerbsfähigkeit zu sichern und auszubauen, erhöhen jedoch gleichzeitig die Angriffsfläche für Cyberbedrohungen.
Die Politik ist gefordert, diesen Prozess durch gezielte Förderprogramme und strategische Maßnahmen zu begleiten, um die digitale Resilienz der Unternehmen nachhaltig zu stärken und die Innovationskraft des Wirtschaftsstandorts Bayern zu sichern.

Sachverständigenanhörung des Ausschusses für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung zum Thema

IT-Sicherheit in der bayerischen Wirtschaft

Bayerischer Landtag am 27.11.2025

Begriffsbestimmungen

Der bei der Polizei bundesweit einheitlich definierte Begriff „Cybercrime“ umfasst sämtliche rechtswidrigen Taten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Ferner umfasst Cybercrime auch solche Taten, die mittels Informations- und Kommunikationstechnik begangen werden. Diese Definition beschreibt das Phänomen Cybercrime in seiner Gesamtheit.

In der praktischen polizeilichen Umsetzung sind jedoch Differenzierungen erforderlich, die zu den Begrifflichkeiten Cybercrime (ehemals „Computerkriminalität“) und „Internet als Tatmittel“ geführt haben.

Unser Verständnis des Begriffs Cybercrime

Unter den **Begriff Cybercrime (im engeren Sinne)** fallen jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden. Aus dem Strafgesetzbuch (StGB) ergibt sich hieraus folgender Straftatenkatalog:

- Ausspähen von Daten (§ 202a StGB)
- Abfangen von Daten (§ 202b StGB)
- Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)
- Datenhehlerei (§ 202d StGB)
- Computerbetrug (§ 263a StGB)
- Fälschung beweiserheblicher Daten (§ 269 StGB)
- Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB)
- Falschbeurkundung und Urkundenunterdrückung im Zusammenhang mit Datenverarbeitung (§§ 271, 274 I Nr. 2, 348 StGB)
- Datenveränderung (§ 303a StGB)
- Computersabotage (§ 303b StGB)

In den Deliktsbereich der vorgenannten Taten fallen, unabhängig von der technischen Umsetzung, u. a. folgende Phänomene:

- Ausspähen von Zahlungskartendaten und sonstigen Daten im elektronischen Zahlungsverkehr im Internet (z. B. Prepaidkarten, Kreditkarten, Voucher)
- Abgreifen sonstiger personenbezogener Identifikations- und Zugangsdaten (z. B. durch Schadsoftware, Phishing-Seiten, E-Mail-Links)

▪ Abgreifen digitaler Signaturen (z. B. im E-Commerce und E-Government)

▪ Hacking (z. B. unberechtigtes Eindringen in informationstechnische Systeme)

▪ Überlastung von Servern durch massenhafte Anfragen, sog. Distributed-Denial-of-Service-Angriffe (DDoS)

▪ Verbreiten von Schadsoftware (z. B. Viren, Trojaner und Würmer)

▪ Aufbau und/oder Betrieb von Botnetzen (z. B. zur Verschleierung oder Anonymisierung von Täteraktivitäten)

▪ Computerbetrugsdelikte wie z. B. der Warenkredit- und Leistungskredit-Computerbetrug i. V. m. Online-Einkäufen, soweit ein automatisierter Abwicklungsprozess erfolgt, also eine Maschine und keine natürliche Person getäuscht wird

Im Unterschied hierzu umfasst die **Begrifflichkeit „Internet als Tatmittel“** sämtliche rechtswidrige Taten, bei denen das Internet zur Planung, Vorbereitung oder Ausführung eingesetzt wird. Hierbei steht das eigentliche Delikt im Vordergrund, während das Internet bzw. einzelne Komponenten des Internets nur als Tatmittel fungieren. Dabei kommen sowohl rechtswidrige Taten in Betracht, bei denen das bloße Einstellen von Informationen in das Internet bereits strafrechtlich relevante Tatbestände erfüllt, als auch Delikte, bei denen das Internet als Kommunikationsmedium bei der Tatbestandsverwirklichung eingesetzt wird. Zur Orientierung dienen folgende Beispiele:

▪ Verbreitung und Besitzverschaffung von kinder-/jugendpornografischen Schriften

▪ Betrugsdelikte wie z. B. der Waren(-kredit) - und Leistungs(-kredit)betrug in Verbindung mit Online-Auktionen bzw. Online-Shops, soweit eine natürliche Person getäuscht wird

▪ Verbreitung urheberrechtlich geschützter Werke über Internet-Tauschbörsen

▪ Beleidigung/Bedrohung mittels E-Mail

Spielt das Internet bzw. die Informationstechnologie im Hinblick auf die Tatbestands-verwirklichung allerdings eine lediglich untergeordnete Rolle, wenn beispielsweise Kontakte bzw. Kontaktversuche über das Internet zwischen Täter und Opfer der eigentlichen Tat vorgelagert sind, ist die Tat nicht der Begrifflichkeit „Internet als Tatmittel“ zuzuordnen

1) Aktuelle Bedrohungslage und Angriffsarten

a) „Wie hat sich die Bedrohungslage für bayerische Unternehmen in den letzten Jahren entwickelt, insbesondere vor dem Hintergrund zunehmender globaler Cyberattacken und geopolitischer Spannungen? Welche Branchen waren besonders betroffen?“

Die sinnbildliche Großwetterlage wird durch einleitende Worte im BKA-Bundeslagebild Cybercrime 2024 sehr treffend zusammengefasst: „Die Tatgelegenheiten steigen in Folge von zunehmend digitaler Vernetzung, die Eintrittsschwellen sinken über Cybercrime-as-a-Service-Angebote in der Underground Economy, neue KI-Möglichkeiten und nicht zuletzt die geopolitischen Entwicklungen der letzten Jahre haben sich als erheblicher Treiber für Cyberdelikte erwiesen."

Für Bayern stellen sich die wesentlichen Kennzahlen wie folgt dar:

Innerhalb der PKS werden für den Bereich Cybercrime im Berichtszeitraum 2024 für den Freistaat Bayern 14.830 polizeilich erfasste Fälle ausgewiesen, was einem Rückgang von -9,6 % im Vergleich zum Vorjahr und einem Anteil von 2,4 % der im Jahr 2024 polizeilich registrierten Gesamttaten entspricht. Es sei angemerkt, dass Delikte mit unbekanntem Tatort oder mit Tatort im Ausland nur in die bei Cybercrime deutlich umfangreichere „PKS Auslandstaten" einfließen und nicht von den oben genannten 14.830 Fällen umfasst sind.

In der PKS Ausland wurden im Jahr 2024 33.813 Fälle im Bereich Cybercrime im engeren Sinne erfasst.

Die Studie „Sicherheit und Kriminalität in Deutschland" (SKiD) 2 untersucht das Dunkelfeld von Straftaten auf wissenschaftlicher Basis. Die Befragung SKiD kommt zu dem Ergebnis, dass im Bereich der Cyberkriminalität ein besonders großes Dunkelfeld herrscht. Es werden hier nur 17,9 % der Straftaten angezeigt.

Im Jahr 2024 betrug die Aufklärungsquote der PKS für den Bereich Cybercrime 35,2 % und liegt damit marginal über der des Vorjahres (35,0 %).

Gemäß PKS summierte sich der durch Cybercrime verursachte Schaden im Jahr 2024 auf 20,07 Millionen Euro. Es ist jedoch anzumerken, dass in der bundeseinheitlichen PKS nur Schäden aus den Deliktsfeldern „Computerbetrug" mit Tatorten im Inland dargestellt werden. Es handelt sich bei der dargestellten Schadenssumme für 2024 ausschließlich um den sog. „Beuteschaden", welcher aus dem Deliktsbereich Computerbetrug mit Tatort Bayern resultiert und den täterseitigen Gewinn aus der rechtswidrigen Tat darstellt (z. B. relevant für Maßnahmen der Vermögensabschöpfung bei Beschuldigten).

Lösegeld, das beispielsweise nach einer Verschlüsselung von IT-Systemen für deren Entschlüsselung erpresst wurde, oder Schäden, die durch eine Kompromittierung kompletter Firmennetze mit einhergehendem Produktionsausfall entstanden sind, finden in der Statistik keinerlei Berücksichtigung.

Die über die PKS aufgeführten Schadenssummen sind somit nicht als wirtschaftlicher Gesamtschaden zu verstehen.

Besonders betroffen waren unserer Wahrnehmung nach kleine und mittelständische Unternehmen, zumeist aus dem Bereich der Industrie und des Verarbeitenden Gewerbes. Selten Betroffen waren Unternehmen aus dem Finanzsektor.

b) „Welche Cyberangriffsarten (z. B. Ransomware, Phishing, verteilter Denial-of-Service Angriff (DDoS), Advanced Persistent Threats-Angriffe (ATPs)) oder Social Engineering sind aktuell besonders relevant für Unternehmen in Bayern?“

Wir gehen davon aus, dass Ransomware-Angriffe besonders relevant für Unternehmen in Bayern sind. Mit Blick auf die Fallzahlenstatistik der Quick Reaction Teams (QRT) ist dies der mit Abstand häufigste Verständigungsgrund.

Für die Bayerische Polizei sind Ransomware-Angriffe der derzeit ressourcenintensivste Brennpunkt gemessen an den pro Fall eingesetzten Mitteln.

c) „Wie können die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben die bayerischen Unternehmen bei der Abwehr und Bewältigung von Cyberangriffen unterstützen?“

Die bayerischen Behörden mit Cybersicherheitsaufgaben unterstützen die bayerischen Unternehmen durch Präventionsarbeit (z. B. Sensibilisierung, Definition von Sicherheitsmindeststandards, Informationsaustausch, Warnungen betreffend aktuelle Bedrohungen), Unterstützung im Akutfall (z. B. taktische Betreuung, digitale Forensik, Ermittlung von Einfallsvektoren) und Ermittlungsarbeit (z. B. Take-Downs betreffend Täterseitiger Infrastruktur).

2) Stand der IT-Sicherheitsmaßnahmen

a) Inwieweit ist der aktuelle Stand der IT-Sicherheitsmaßnahmen in bayerischen Unternehmen, insbesondere bei kleinen und mittleren Unternehmen (KMU) und im Bereich der kritischen Infrastruktur transparent?

Das BLKA verfügt nicht über ein aufschlussreiches Lagebild über den aktuellen Stand der IT-Sicherheitsmaßnahmen in bayerischen Unternehmen, insbesondere bei kleinen und mittleren Unternehmen (KMU) und im Bereich der kritischen Infrastruktur. Fraglich ist aus unserer Sicht, ob ein hohes Maß an Transparenz hierüber zu einer Steigerung der Cybersicherheit beiträgt oder ob darin nicht auch ein hoher Mehrwert für potentielle Angreifer besteht.

b) „Welche typischen Schwachstellen und Defizite bestehen bei den Unternehmen? Wo werden die vordringlichen Handlungsbedarfe gesehen?“

Typische Schwachstellen finden sich sowohl auf technischer Ebene als auch in den organisatorischen Strukturen, darüber hinaus aufseiten der Beschäftigten verschiedenster Ebenen.

Veraltete Systeme, fehlende Sicherheitsupdates und unzureichend geschützte Endgeräte eröffnen Angreifern Einfallstore. Hinzu kommen u. a. unsichere Passwörter ohne Multi-Faktor-Authentifizierung (MFA), ungetestete Backups sowie falsch konfigurierte Cloud-Dienste. Auch mangelndes Sicherheitsbewusstsein der Mitarbeiter, fehlende Notfallpläne und unklare Verantwortlichkeiten stellen häufige Risiken dar. Doch es gibt auch Schwachstellen, gegen die man sich nur schwerlich aktiv schützen kann. Sogenannte Zero-Day-Exploits sind Schwachstellen in bspw. Software, die zwar Cyberkriminellen, nicht jedoch den Herstellern von Software und somit auch nicht den Kunden bekannt sind. Um auch derartige Gefahren soweit als möglich einzudämmen, ist ein allumfassender Blick auf das Thema Cyber-Security gefordert. Dieser reicht letztlich von Awareness-Steigerung der Mitarbeiter bis hin zum Umgang mit einer Krise.

Im Jahr 2023 wurden durchschnittlich täglich 78 neue **Schwachstellen** (darunter zudem eine Vielzahl kritischer Schwachstellen in Perimetersystemen, wie beispielsweise Firewalls und VPNs) bekannt. Im Rahmen des Verfahrens zur koordinierten Veröffentlichung von Schwachstellen erreichten das BSI zudem durchschnittlich monatlich 18 Meldungen über Zero-Day-Schwachstellen in IT-Produkten deutscher Hersteller.

Die größten Angriffsflächen im Cyberraum findet der Angreifer in Form von IP-Adressen, Domains und URLs sowie E-Mail-Adressen und Schwachstellen vor.[1]

Um auch derartige Gefahren soweit als möglich einzudämmen, ist ein allumfassender Blick auf das Thema Cyber-Security gefordert. Dieser reicht letztlich von Awareness-Steigerung der Mitarbeiter bis hin zum Umgang mit einer Krise.

Daraus abgeleitet ergibt sich ein klarer Handlungsbedarf: Unternehmen müssen grundlegende Schutzmaßnahmen wie Patchmanagement, MFA, Endpoint Security, Segmentierung von Netzen und Backup-Strategien konsequent umsetzen. Ebenso wichtig sind die Sensibilisierung der Mitarbeitenden, Zuständigkeitsregelungen, das Einführen klarer Prozesse im Krisenfall und ein kontinuierliches Monitoring von Systemen. Nur wenn Technik, Organisation und der Mensch zusammenspielen, lässt sich die Widerstandsfähigkeit im Zusammenhang mit Cyberangriffen nachhaltig erhöhen.

Vollständige Sicherheit lässt sich in keinem der oben genannten Einzelaspekte erreichen, weshalb sich Unternehmen möglichst breit aufstellen sollten.

[1] (BSI, 2024)

3) Resilienz und Krisenmanagement

a) „Wie gut sind bayerische Unternehmen auf größere Cybervorfälle vorbereitet? Gibt es beispielsweise Notfallpläne, Quick-Response-Teams (QRTs) und regelmäßige Übungen?“

Hierzu liegen uns keine belastbaren Informationen vor.

b) „Wie bewerten Sie die Notfallversorgung im Stromausfall (z. B. auch via Dieselgeneratoren) speziell bei Rechenzentren in Bayern?“

Die Infrastruktur der Bayerischen Polizei bzw. das Rechenzentrum ist gegen Szenarien wie beispielsweise einen Stromausfall gehärtet.

c) „Welche Erfahrungen gibt es mit der Wiederherstellung nach erfolgreichen Angriffen (Recovery-Zeit, Datenverluste)?“

Ob und in welcher Zeitspanne Daten wiederhergestellt werden können, hängt stark davon ab, welche Strategie betreffend die Segmentierung von Netzen, Backup-Speichern und Notfallplänen ein angegriffenes Unternehmen etabliert hat. Unserer Erfahrung nach führt die Zahlung von Lösegeld in vielen Fällen jedoch nicht zu einer hinreichenden Datenwiederherstellung, sondern im Gegenteil zu Folgeforderungen bis hin zu Sekundärangriffen.

d) „Liegen Erkenntnisse vor, inwieweit der kurzfristige Wegfall grundlegender digitaler Dienste von Drittstaatsanbietern wie Cloud-Diensten in den Notfallplänen/Business Continuity -Plänen der bayerischen Unternehmen durch geeignete Vorkehrungen berücksichtigt wird?“

Hierzu liegen dem BLKA keine Erkenntnisse vor.

4) Lieferketten, digitale Resilienz und digitale Souveränität

a) „Wie können einheitliche IT-Sicherheitsstandards entlang der gesamten Wertschöpfungskette etabliert und durchgesetzt werden?“

Hierzu liegen dem BLKA keine Erkenntnisse vor.

b) „Inwieweit bestehen Abhängigkeiten für bayerische Unternehmen von internationalen Cloud- und IT-Infrastrukturanbietern und ggf. welche Risiken ergeben sich hierdurch?“

Durch (zeitweisen) technologischen Vorsprung internationaler Cloud- und IT-Infrastrukturanbieter können sich Partizipationszwänge ergeben (da es ansonsten zu Wettbewerbsnachteilen kommt). Die nachfolgend abfließenden Mittel stehen im Weiteren nicht für Binneninvestitionen zur Verfügung. Ein Aufschließen ist aufgrund der „Doppeltaxierung“ (Partizipationskosten und Investitionskosten) oft nicht zu leisten.
Die durch lediglich Partizipation entstehenden Risiken bestehen insbesondere im Verlust der Datenhoheit sowie darin, dass Prozesse „Blackbox-Charakter“ annehmen.

c) „Welche Maßnahmen könnten zur Stärkung der digitalen Souveränität und zur Förderung europäischer Alternativen beitragen?“

Die Entwicklung eines technologischen Vorsprungs ist in den wenigsten Fällen effizient (z. B. aufgrund „Try and Error“). Soweit lediglich eine kleine Zahl priorer Projekte definiert wird, könnte aus unserer Sicht das jeweilige Ziel kostengünstiger Erreicht werden. Problematischer gestaltet sich die anschließende Skalierung. Eine in jedem Fall gewinnbringende Empfehlung können wir hierzu nicht abgeben.

5) Regulatorische Anforderungen und Umsetzung

Der Fragenblock 5 fällt nicht in die Expertise des BLKA.

6) Wirtschaftliche Auswirkungen und Kosten

Der Fragenblock 6 fällt nicht in die Expertise des BLKA.

7) Sensibilisierung, Ausbildung und Fachkräftemangel

Der Fragenblock 7 tangiert nur teilweise die Expertise des BLKA. Da die Bayerische Polizei jedoch ein bedeutend anderes Profil aufweist als KMU und zugleich als Wettbewerber um qualifiziertes Personal auftritt, möchten wir lediglich bestätigen, dass Engpässe in der Quantität bestehen.

8) Zukunftsperspektiven und Innovation

Die beispielhaft genannten Trends Künstliche Intelligenz und Cloud-Lösungen gehören bei der Bayerischen Polizei zu den prioren Themen. Der Schwerpunkt in unserer Herangehensweise liegt jedoch in der sicheren und rechtskonformen Integration in die eigenen Strukturen. Zur Integration und Kosten-Nutzen-Relation u. a. dieser Technologien in bayerische KMU liegen uns keine Erkenntnisse vor.

9) Empfehlungen für die Politik

Der Fragenblock 9 tangiert nur geringfügig die Expertise des BLKA.

Folgende Punkte möchten wir jedoch betonen und als Empfehlung verstanden wissen:

Die Zusammenarbeit zwischen LSI, BSI, LfV und Polizei wird durch uns als essenziell betrachtet. Gemeinsame Übungen, gemeinsame Prävention, Informationsaustausch zu IOCs, gegenseitige Unterstützung in der Beratung bei Echtfällen sowie die Fallaquise schaffen für uns die Grundlage für erfolgreiche Polizeiarbeit.

Abschließend, aber keines Falls weniger bedeutend ist für uns die Zusammenarbeit zwischen Firmen und der Polizei. Wir möchten und können ein verlässlicher Partner im Bereich der IT-Sicherheit sein. Die grundsätzliche Verständigung der Polizei - soweit möglich in zeitlicher Nähe zu einem Cyberangriff - ist immens wichtig für das **gemeinsame Ziel der IT-Sicherheit in der bayerischen Wirtschaft**.

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

- **IHK für München und Oberbayern** vertritt über 400.000 Mitgliedsunternehmen
  - davon der überwiegende Teil kleine und mittlere Unternehmen

- **Aktuelle Lage: IHK-Digitalisierungsumfrage 2024**
  - Im letzten Jahr 23% der bayerischen Unternehmen Opfer mindestens eines relevanten Cyberangriffs – Tendenz steigend.
  - Standardmaßnahmen wie Backup, Updates u. a. werden zumeist gemacht (in 94 bzw. 88 % der Unternehmen)
  - Deutlich zu wenige Unternehmen haben aber ausreichende IT-Sicherheits-Maßnahmen, wie z. B. einen IT-Notfallplan oder Tests von Backups.
  - Je weniger Mitarbeiter ein Unternehmen hat, umso unwahrscheinlicher werden wichtige Maßnahmen für die eigene Cybersicherheit durchgeführt.
    Beispiel IT-Notfallplan:
    - bis 19 Mitarbeiter: In 32 % der Unternehmen
    - 20 – 249 Mitarbeiter: 44 %
    - über 249 Mitarbeiter: 72%

- **Fazit:**
  - Unternehmen sind sich der Gefahren von Cyberattacken bewusst
  - Aber: IT-Sicherheit überfordert kleine und mittlere Unternehmen häufig
  - Gründe: Hohe Komplexität, fehlendes Knowhow, fehlende Ressourcen, unklare Pflichten, vielfältiger Dienstleister-Markt und unübersichtliche Unterstützungsangebote.

<u>Lösungsansätze für Bayern:</u>
IHK-Positionspapier „IT-Sicherheit für Unternehmen“ mit zahlreichen Vorschlägen und Forderungen für EU-, Bundes- und Landesebene - siehe IHK-Website.
Heute Fokus auf die Landesebene – mit ein paar Ergänzungen für die Bundesebene, auf die auch von Landesseite Einfluss genommen werden sollte:

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

Speziell für die bayerische Politik bestehen einige konkrete Handlungsoptionen:

- **Wirtschaft durch staatliche Einrichtungen zielgerichtet unterstützen:**
  - Neutrale, zentrale Lotsen-Einrichtung für Unternehmen (wie z. B. die Cybersicherheitsagentur Baden-Württemberg).
  Problem: Die Unterstützungsangebote in Bayern wie die „Zentrale Ansprechstelle Cybercrime“ (ZAC) beim LKA, der Verfassungsschutz, die Generalstaatsanwaltschaft Bamberg, das Bay. Landesamt für Datenschutzaufsicht sind sehr hilfreich – aber Unternehmen oftmals unbekannt und unklar in der jeweiligen Zuständigkeit. Außerdem haben diese Behörden einen sanktionierenden / strafverfolgenden Hintergrund. Das verringert die Bereitschaft von Unternehmen Vorfälle zu melden.
  Unternehmen benötigen bei Fragen zur Prävention ebenso wie bei einem Cybersicherheitsvorfall eine leicht auffindbare, bekannte Anlaufstelle, um einen schnellen Überblick über alle staatlichen Unterstützungsangebote zu IT-Sicherheit zu erhalten. Für einen möglichst offenen und neutralen Zugang ist es erforderlich, diese Lotsen-Anlaufstelle für Unternehmen unabhängig von der Strafverfolgung zu etablieren. Ggf. kann das Bayerische Landesamt für Sicherheit in der Informationstechnik (LSI) analog zum BSI diese Rolle übernehmen.
  - **Zielgruppenspezifische Angebote ausbauen:**
  Insbesondere kleine und Kleinstunternehmen benötigen einen einfachen Zugang zur Cybersicherheit. Ähnlich wie der „BSI-CyberRisikoCheck nach DinSpec 27076“ könnten weitere Standards entwickelt werden, die speziell für KMUs geeignet sind. Z. B. hat die IHK sehr nachgefragte Muster zu IT-Notfallplänen, die eingebracht werden könnten.

- Der Freistaat sollte mehr Fokus auf **digitaler Souveränität** legen, z. B.:
  - **bei öffentlichen Ausschreibungen** Cybersicherheit UND digitale Souveränität berücksichtigen, so dass hiesige Unternehmen Chancen bekommen.
  - **IT-Sicherheit in Open Source unterstützen:**
    Open Source-Software bildet die Grundlage nahezu sämtlicher Softwareprogramme. Schwachstellen in zentralen Open Source-Bausteinen können schwerwiegend sein (Log4j, xz-lib). Auf Bundesebene gibt es diverse Aktivitäten zu Open Source („Sovereign Tech Fund“, „PrototypeFund“), in Bayern besteht hier keine Aktivität.
    => Im Zusammenhang mit dem Deutschland Stack (enthält sehr viele OpenSource-Lösungen) und dem Cyber Resiliance Act (SBOM hier verpflichtend – Verzeichnis der in einem Produkt verbauten Softwarebestandteile) könnte Bayern auch auf diesem Gebiet tätig werden.

- **Schwachstellenmanagement verbessern: Ethische Schwachstellenforschung legalisieren**
  Durch §202 StGB („Hackerparagraph“) laufen verantwortungsbewusste

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

Cybersicherheitsexperten in die Gefahr der Strafverfolgung, wenn sie Betroffene über IT-Sicherheitslücken informieren. Effekt: Cybersicherheitsexperten sind hier sehr zurückhaltend, betroffene Unternehmen und Behörden erfahren nichts von IT-Sicherheitslücken.
Im Koalitionsvertrag in Berlin ist die Reform von §202 StGB („Hackerparagraph“) geplant, gerade in Bayern bestehen hierzu Bedenken.
=> Das bay. Landesamt für Sicherheit in der Informationstechnik (LSI) schreibt: “Bitte melden Sie Schwachstellen in staatlichen Webanwendungen direkt an das Bayern-CERT.“ Dies sollte zu einem kompletten Programm für „Coordinated Vulnerability Disclosure“ (koordinierte Offenlegung von Schwachstellen) ausgebaut und durch ein Bug Bounty Programm ergänzt werden.

- **Schlüsselrollen bei Cyberangriffen besser einbinden:**
  Die legalen und handelsüblichen Services von IT-Dienstleistern wie z. B. Domain-Registrare, Hosting-Anbieter oder Content Delivery Networks werden von Cyberkriminellen missbraucht und ermöglichen erst Cyberangriffe. Sie nehmen damit eine Schlüsselrolle bei Cyberangriffen ein. In Bayern sind nahezu alle maßgeblichen IT- und Internetakteure mit Niederlassungen vertreten.
  => Staatliche Stellen sollten sich stärker mit Einrichtungen in Schlüsselrollen austauschen und gemeinsam effektivere Eindämmungswege finden.

- **Domain „.bayern“ zur cybersicheren Qualitätsdomain machen:**
  Ein häufiges Cybersicherheitsproblem ist die missbräuchliche Nutzung von Internet-Domains (z. B. für Phishing-Mails) sowie unzureichende Konfiguration (Maßnahmen gegen Spam wie SPF u. ä.).
  => Zumindest für die im eigenen Gesetzgebungsbereich befindlichen Domains (z. B. „.de“ oder „.bayern“) sollten besondere Qualitätsmerkmale etabliert werden, z. B. eine zuverlässige Identifizierung bei der Beantragung einer Domain. Missbrauch wie z. B. Fakeshops unter de-Domains sollten schnell abgeschaltet werden können. Hierzu könnte eine Meldemöglichkeit analog zur TKG-Lösung für Telefon-Spam eingerichtet werden. Dazu müssen staatl. Einrichtungen kurzfristig auf die in diesem Gebiet operativ tätigen Unternehmen einwirken können.

- **Online- Anzeigen bei der Bayerischen Polizei für Cybercrime verbessern**
  Aktuell kann man in Bayern online Delikte zu KfZ und Fahrrädern sowie Online-Auktionen zur Anzeige bringen - aber z. B. keinen Cyberbetrug per E-Mail. Andere Bundesländer (z. B. „Betrug anzeigen – Onlinewache Hessen“. https://portal.onlinewache.polizei.de/de/he/betrug/) sind zugänglicher.

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

Überblick über das IHK-Positionspapier zur IT-Sicherheit:

Das IHK-Positionspapier (https://www.ihk-muenchen.de/ratgeber/digitalisierung/informationssicherheit/positionspapier-it-sicherheit/) gibt eine Reihe von Vorschlägen, die zur Verbesserung der Cybersicherheitslage beitragen würden:

1. **Unternehmen in IT-Sicherheitsmaßnahmen praxisnah unterstützen**
    a. Gesetzliche Verpflichtungen angemessen und rechtssicher umsetzen
    b. Wirtschaft durch staatliche Einrichtungen zielgerichtet unterstützen
    c. Verlässliche Anbieter, Dienstleister und Produkte kennzeichnen
2. **Ökosystem für innovative IT-Sicherheitsprodukte und -Services stärken**
    a. Forschungstransfer verbessern
    b. Innovationspotenzial von Startups stärken
    c. Entwicklung von Schlüsseltechnologien zur IT-Sicherheit vorantreiben
    d. Faire Marktchancen für EU-Anbieter sicherstellen
    e. IT-Sicherheit in Open Source unterstützen
3. **Gemeinsam IT-Sicherheitsbedrohungen entgegentreten**
    a. Schlagkraft der Sicherheitsbehörden erhöhen
    b. Ethische Schwachstellenforschung legalisieren
    c. Mit IT-Sicherheitslücken verantwortungsbewusst umgehen
    d. Austausch aller Betroffenen fördern - Lagebild und Nutzen verbessern
    e. Schlüsselrollen bei Cyberangriffen besser einbinden
4. **Kompetenzen für IT-Sicherheit auf allen Ebenen ausbauen**
    a. IT-Sicherheits-Kompetenzen in allen Phasen umfassend stärken
    b. Neue Generation von IT-Sicherheitsfachkräften entwickeln

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft" am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

Fragenkatalog des Landtags & IHK-Antwortvorschläge

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 Branchen waren besonders betroffen?***

  IHK: Die Bedrohungslage für bayerische Unternehmen hat sich deutlich verschärft – sowohl durch mehr Vorfälle als auch durch professionellere und gezieltere Angriffe. Laut BSI ist die Lage „angespannt".
  Nach IHK-Digitalisierungsumfrage waren im letzten Jahr 23% der bayerischen Unternehmen Opfer mindestens einen relevanten Cyberangriffs – Tendenz steigend.
  Seit dem Ukrainekrieg treten neben finanziell motivierter Cyberkriminalität verstärkt Hacktivismus und destruktive Angriffe auf, etwa im Umfeld der Münchner Sicherheitskonferenz oder als Folge geopolitischer Konflikte.
  Zudem vergrößert die fortschreitende Digitalisierung die Angriffsfläche, während künstliche Intelligenz neue Möglichkeiten für Angreifer wie Verteidiger schafft.

- ***Welche Cyberangriffsarten (z. B. Ransomware, Phishing, verteilter Denial-of-Service Angriff (DDoS), Advanced Persistent Threats-Angriffe (ATPs)) oder Social Engineering sind aktuell besonders relevant für Unternehmen in Bayern?***

  IHK: Unternehmen werden ständig vollautomatisch angegriffen.
  Websites, Netzwerke, Geräte etc. werden fortlaufend auf Schwachstellen gescannt. Die allermeisten Angriffe werden abgewehrt - das Problem ist, dass ein einziger erfolgreicher Angriff ausreicht.
  Um z. B. mit einem Ransomware-Angriff erfolgreich zu sein, greifen Cyberkriminelle auf einen breiten Werkzeugkasten zu, der durch KI deutlich vergrößert wird.
  Das BSI berichtet, dass v. a. Ransomware und Denial-of-Service-Angriffe die häufigsten Angriffsarten sind. Wobei für diese Angriffe wiederum Social Engineering, Schwachstellen etc. herangezogen werden.

  Konkret berichteten Unternehmen zuletzt der IHK für München und Oberbayern von Vorfällen mit Rechnungsbetrug, Ransomware-Erpressung und Denial-of-Service-Angriffen:
  - Eine gefälschte Rechnung per E-Mail führte zu einer Überweisung an Betrüger statt an den eigentlichen Empfänger
  - Unternehmen werden verschlüsselt (Ransomware) und erpresst.
  - Mit einem Denial-of-Service-Angriff wurde ein Onlineshop lahmgelegt.

  Die IHK selbst wird ungewollt involviert in Phishing-Angriffe: Immer wieder kommt es zu E-Mailwellen, mit denen Unternehmen aufgerufen werden mit „Achtung: Letzte Erinnerung

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

aufgrund unbehandelter Unternehmensdaten". Die IHKs klären dazu auf (IHK warnt vor betrügerischen Mails an Unternehmen, https://www.ihk-muenchen.de/presse/news/News-Detailseite-(%C3%BCberregional)_87681.html), allerdings berichten immer wieder Unternehmen, dass sie hereingefallen sind.

- ***Wie können die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben die bayerischen Unternehmen bei der Abwehr und Bewältigung von Cyberangriffen unterstützen?***

  IHK: In der **Prävention** arbeiten die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben sehr gut mit den IHKs zusammen. Mit Webinarreihen und Präsenzveranstaltungen konnten viele Unternehmen sensibilisiert werden.
  Besonders hervorheben kann man die Arbeit des Bayerischen Landesamtes für Datenschutzaufsicht: Dieses bietet zahlreiche Checklisten und sehr konkrete Hilfestellungen z. B. zum Schutz vor Ransomware an. Hier fließt die Erfahrung aus konkreten Vorfällen in nützliche Hinweise ein.
  Auch sehr gut ist die Arbeit des LSI (Landesamt für Sicherheit in der Informationstechnik), die sehr konkret für einzelne Kritis-Branchen (Kliniken , Trinkwasserversorgung, Abwasserentsorgung…) Unterstützungs- und Austauschangebote anbietet.

  Im **Krisenfall** bei von Cyberangriffen maßgeblich betroffenen Unternehmen rät die IHK immer, sich an das ZAC („Zentrale Ansprechstelle Cybercrime für die Wirtschaft in Bayern“) beim LKA zu wenden. Das funktioniert mittlerweile auch sehr gut.

  Was verbessert werden sollte:
  - **Zentrale Anlaufstelle für IT-Sicherheit für Unternehmen**:
    Unabhängige, zentrale Lotsenstelle etablieren: Staatliche Unterstützungsangebote auf Bundes- und Landesebene (z. B. BSI, ZAC) müssen sichtbarer und bekannter gemacht sowie die Zuständigkeiten besser vermittelt werden. Unternehmen benötigen bei Fragen zur Prävention ebenso wie bei einem Cybersicherheitsvorfall eine leicht auffindbare, bekannte Anlaufstelle, um einen schnellen Überblick über alle Unterstützungsangebote zu IT-Sicherheit zu erhalten. Für einen möglichst offenen und neutralen Zugang ist es erforderlich, diese Lotsen-Anlaufstelle für Unternehmen unabhängig von der Strafverfolgung zu etablieren. Beispiele dafür sind die Cyberwehr Baden-Württemberg, Cyberwehr Nordrhein-Westfalen oder die Cyberhotline Berlin.

  - **Schlagkraft der Sicherheitsbehörden erhöhen:**
    Unternehmen benötigen kompetente Ansprechpartner und Schutz vor Cyberkriminalität. Sicherheitsbehörden müssen technisch und personell besser ausgestattet werden. Spezialeinheiten sollten föderal und behördenübergreifend, z. B. mit der Bundeswehr, zusammenarbeiten. Bei massiven Cyberangriffen sind klare Zuständigkeiten und eine schnelle Koordination zwischen Bund und Ländern

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

entscheidend.

- **Online-Anzeige und Meldemöglichkeit für Cybercrime in Bayern verbessern:**
  In Bayern kann man an digitalen Delikten nur „Betrug mittels Online-Auktion“ online zur Anzeige bringen (siehe Anzeigeerstattung bei der Bayerischen Polizei online - BayernPortal, https://www.bayernportal.de/dokumente/onlineverfahren/305652977295). In anderen Bundesländern kann man z. B. auch „Missbräuchliche Verwendung eines bestehenden Kundenkontos“ online zur Anzeige bringen (siehe Onlinewachen der Polizeien der Länder – Offizielles Portal bzw. Betrug anzeigen – Onlinewache Hessen, https://portal.onlinewache.polizei.de/de/).
  Als Grund für weniger Online-Anzeigemöglichkeiten wird die nicht ausreichende Personalausstattung angeführt, da man eine **Flut von Anzeigen befürchtet**.

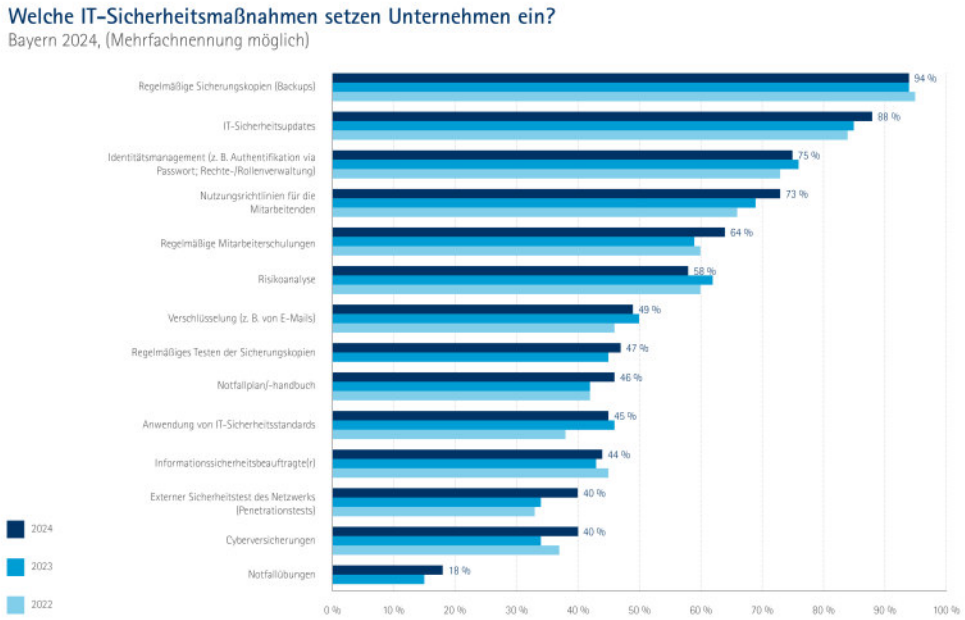
2. Stand der IT-Sicherheitsmaßnahmen

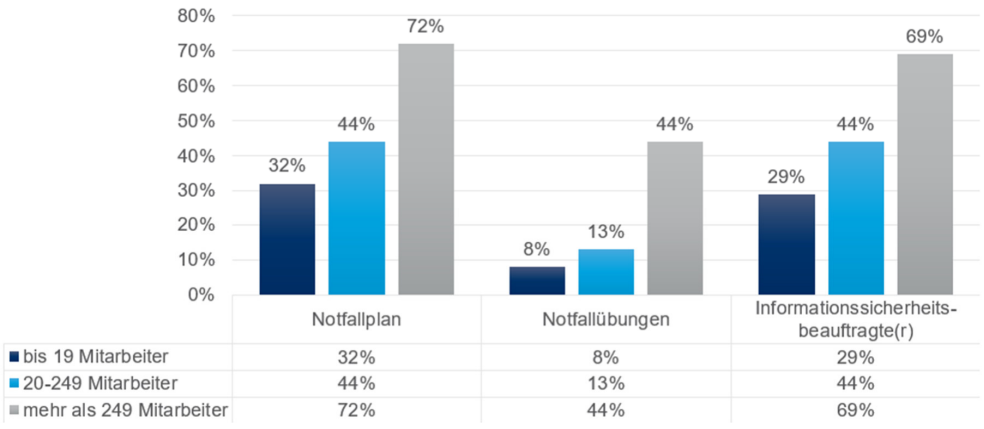
- ***Inwieweit ist der aktuelle Stand der IT-Sicherheitsmaßnahmen in bayerischen Unternehmen, insbesondere bei kleinen und mittleren Unternehmen (KMU) und im Bereich der kritischen Infrastruktur transparent?***

  IHK: Ergebnisse der jährlichen IHK-Digitalisierungsumfrage:
  - Standardmaßnahmen (Backups, Updates, Rechtemanagement, Nutzungsrichtlinien) sind in Unternehmen häufig anzutreffen
  - Deutlich seltener sind weitergehende Maßnahmen wie Backuptests, Notfallpläne oder externe Sicherheitstests.
  - Die Zunahme der eingesetzten IT-Sicherheitsmaßnahmen über die letzten drei Jahre ist deutlich geringer als die Situation erwarten lassen würde.
  - Je weniger Mitarbeiter ein Unternehmen hat, umso weniger IT-Sicherheitsmaßnahmen sind vorhanden:
    - Große Unternehmen betreiben eine komplexe IT und haben Ressourcen für deren Absicherung.
    - Sehr kleine Unternehmen haben eine einfache IT, aber kaum Know-how zu Cybersicherheit und wenig Ressourcen dafür.
    - Besonders problematisch sind kleinere Unternehmen mit schon etwas umfangreicherer IT aber noch ohne eigene IT-Ressourcen. Diese verlassen sich oft komplett auf IT-Dienstleister, die mitunter auch nur eingeschränktes Cybersicherheits-Know-how haben.

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

Aus der IHK-Digitalisierungsumfrage November 2024 für Bayern:





	Notfallplan	Notfallübungen	Informationssicherheits-beauftragte(r)
bis 19 Mitarbeiter	32%	8%	29%
20-249 Mitarbeiter	44%	13%	44%
mehr als 249 Mitarbeiter	72%	44%	69%

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft" am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

- ***Welche typischen Schwachstellen und Defizite bestehen bei den Unternehmen? Wo werden die vordringlichen Handlungsbedarfe gesehen?***

  IHK:
  - **Bei der Auswahl und Nutzung externer IT müssen Unternehmen noch viel mehr Wert auf Cybersicherheit legen:**
    Bei der Auswahl von IT-Dienstleistern und IT-Produkten spielt die Cybersicherheit (wie digitale Souveränität) eine wachsende, aber nach wie vor zu geringe Rolle. Viele Geschäftsmodelle von Unternehmen verlassen sich auf externe, nicht schnell ersetzbare IT: Fällt diese aus, kommt es zu großen Problemen (aktuelles Beispiel: Ausfall der Amazon-AWS-Cloud bzw. lahmgelegte Flughäfen durch Ausfall einer Software bei einem Dienstleister).

  - **In den Unternehmen selbst ist besonders die Notfallvorbereitung oft sehr unzureichend:**
    Ist man auf den Ausfall von IT mit einem Plan B vorbereitet? Welche Handlungsoptionen gibt es im Krisenfall? Etc.
    Diese Fragen stellen sich Unternehmen zu selten!

3. Resilienz und Krisenmanagement

- ***Wie gut sind bayerische Unternehmen auf größere Cybervorfälle vorbereitet? Gibt es beispielsweise Notfallpläne, Quick-Response-Teams (QRTs) und regelmäßige Übungen?***

  IHK: Ergebnisse der jährlichen IHK-Digitalisierungsumfrage zeigen, dass zu diesen Themen in vielen Unternehmen Verbesserungsbedarf besteht:
  - Notfallübungen: In 18 % der Unternehmen
  - Quick-Response-Teams: 40 % der Unternehmen geben an eine Cyberversicherung zu haben. Kernbestandteil dieser ist normalerweise ein Quick-Response-Team, welches im Notfall zu Hilfe kommt.
  - Informationssicherheitsbeauftragte: In 44 % der Unternehmen
  - Notfallpläne: 46 % (v. a. in den größeren Unternehmen)

- ***Wie bewerten Sie die Notfallversorgung im Stromausfall (z. B. auch via Dieselgeneratoren) speziell bei Rechenzentren in Bayern?***

  IHK: Die Notfallversorgung bei Stromausfall ist üblicherweise eine Standardmaßnahmen in allen Rechenzentren, die allerdings unterschiedlich ausgeprägt ist.
  Es gibt in Bayern viele unterschiedliche Rechenzentren: Diese reichen von kleineren Unternehmensrechenzentren in mittelständischen Unternehmen bis hin zu großen, professionellen Rechenzentren. Je nach Bedarf, Notwendigkeit etc. nutzen Unternehmen Rechenzentren: Z. B. Kritis-Unternehmen legen hierfür viel höhere Standards bzgl. Verfügbarkeit, Redundanz, Energieeffizienz und Sicherheit an als kleinere Unternehmen.

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

Über die Klassifizierung mit „Tier I“- bis „Tier IV“-Klassen und Zertifizierungen (EN 50600, ISO 27001) besteht hier eine Transparenz für die Nutzer von Rechenzentrumsdienstleistungen. Große Rechenzentren (München: Noris Network, Spacenet etc.) bieten hier ein sehr gutes Angebot.

- ***Welche Erfahrungen gibt es mit der Wiederherstellung nach erfolgreichen Angriffen (Recovery-Zeit, Datenverluste)?***

  IHK: Die Wiederherstellung bei einem erfolgreichen Angriff ist kein fixer Zeitraum, sondern zusammen mit dem Notbetrieb eine kontinuierlicher, im Idealfall schnell asymptotisch abnehmender Aufwand. Die Zeiträume sind i. d. R. viele Monate.
  Bei einem erfolgreichen größeren Angriff (z. B. Ransomware, Kompromittierung des Netzwerkes o. ä.) erfolgt im Regelfall zunächst ein Notbetrieb, der über Wiederanlaufmaßnahmen in einen Regelbetrieb übergeht. So wie die Cyberangreifer vorher oft schon Monate an dem Angriff gearbeitet haben, müssen sich Unternehmen auch oft auf eine monatelange Herausforderung einstellen.
  Mitunter wird auch die IT auf neue Füße gestellt, was auch ein sehr schmerzhafter, teurer, aber doch spürbarer Innovationsschub sein kann. D. h. meistens ist die IT nach einem Cybervorfall besser als vorher.

- ***Liegen Erkenntnisse vor, inwieweit der kurzfristige Wegfall grundlegender digitaler Dienste von Drittstaatsanbietern wie Cloud-Diensten in den Notfallplänen/Business Continuity - Plänen der bayerischen Unternehmen durch geeignete Vorkehrungen berücksichtigt wird?***

  IHK: Angesichts seltener Notfallpläne (46%, dies v. a. in größeren Unternehmen) und immer wieder zu beobachtender Schadensfälle mit ausfallenden Drittdienstleistern wird dieses Ausfallrisiko in vielen Unternehmen noch vernachlässigt. Das Thema Verortung („Drittstaatsanbietern“) ist hierbei ein Teilthema, was bzgl. digitaler Souveränität wichtiger sein sollte.
  In der Regel sind die großen Hyperscaler (also „Drittstaatsanbietern“) bzgl. Leistungsfähigkeit und Cybersicherheit sehr gut aufgestellt.
  Allerdings gibt es hier auch bei Hyperscalern Ausfälle, die dann zu ungleich gravierenderen Folgen führen.

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

4. Lieferketten, digitale Resilienz und digitale Souveränität

- ***Wie können einheitliche IT-Sicherheitsstandards entlang der gesamten Wertschöpfungskette etabliert und durchgesetzt werden?***

  IHK:
  Aktuelle Situation: Gute IT-Sicherheit kostet IT-Produktanbietern Geld, was Produkte verteuert. Beim Einkauf von IT-Produkten spielt IT-Sicherheit ggf. eine untergeordnete Rolle. Daher erscheinen Investitionen in gute IT-Sicherheit als Wettbewerbsnachteil, allen Lippenbekenntnissen zum Trotz.
  Nahe Zukunft: Mit dem Cyber Resiliance Act (CRA) werden Cybersicherheitsstandards von den Anbietern eingefordert. Die NIS2-Umsetzung und DORA verpflichten Anwender zur Cybersicherheit. D. h. gute IT-Sicherheit soll für Anbieter wie Anwender Pflicht werden. Damit sollen Wettbewerbsnachteile abgeschafft werden.
  Damit diese Idee zum Erfolg führt ist es nötig, dass für alle IT-Anbieter (in der EU und besonders außerhalb) die gleichen Regeln für Cybersicherheitsstandards gelten. Und die IT-Anwender (z. B. die öffentliche Hand) die Kriterien Cybersicherheit (und digitale Souveränität) viel mehr berücksichtigen.
  Aus Anwendersicht ist die Kennzeichnung verlässlicher Anbieter, Dienstleister und Produkte sehr hilfreich:
  Unternehmen benötigen verlässliche Entscheidungshilfen für IT-sichere Produkte und Dienstleistungen. Eine Kennzeichnung, ähnlich der CE-Kennzeichnung, sollte weiterentwickelt werden, basierend auf Hersteller-Selbsterklärungen und möglichen Prüfmechanismen durch Behörden. Ziel ist ein robustes „Basispaket“ für den Alltag. Akzeptanz und Sichtbarkeit solcher Kennzeichnungen müssen gesteigert werden. Ansätze wie die APT-Liste des BSI und DinSpec 27076 sollten ausgebaut werden, ebenso wie Befähigungsnachweise für IT-Sicherheitsdienstleister.

  Konkretes Beispiel: Domains & E-Mails
  Sehr berechtigt hat das BSI das „E-Mail-Sicherheitsjahr 2025“ ausgerufen.
  Staatliche Stellen sollen stärker in den Austausch mit Einrichtungen in Schlüsselrollen (Domain-Registrare, Hosting-Anbieter oder Content Delivery Networks) gehen und gemeinsam Wege zur effektiveren Eindämmung von Cyberangriffen finden.
  Besonders kritisch ist die Rolle von Internetdomains, die bei Phishing-Mails eine wesentliche Rolle spielen. **Zumindest für die im eigenen Gesetzgebungsbereich befindlichen Domains (z. B. „.de“ oder „.bayern“) sollten besondere Qualitätsmerkmale etabliert werden, z. B. eine zuverlässige Identifizierung bei der Beantragung einer Domain.** Missbrauch wie z. B. Fakeshops unter de-Domains sollten schnell abgeschaltet werden können. Hierzu könnte eine Meldemöglichkeit analog zur TKG-Lösung für Telefon-Spam eingerichtet werden. Dazu müssen staatliche Einrichtungen kurzfristig auf die in diesem Gebiet operativ tätigen Unternehmen einwirken können.

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

In Unternehmen müssen IT-Sicherheitsstandards für E-Mail (DKIM, DMARC, SPF, DNSSEC) bekannter gemacht und zur umfangreicheren Nutzung motiviert werden. Hier besteht viel Potenzial für Absicherung.

- I***nwieweit bestehen Abhängigkeiten für bayerische Unternehmen von internationalen Cloud- und IT-Infrastrukturanbietern und ggf. welche Risiken ergeben sich hierdurch?***

  IHK: Viele bayerische Unternehmen – besonders Mittelstand, Industrie 4.0-Betriebe, Logistik- und Softwarefirmen – nutzen Public-Cloud-Dienste von großen internationalen Anbietern wie AWS, Microsoft Azure, Google Cloud.
  Risiken dabei:
  - Störungen oder Ausfälle beim internationalen Anbieter (z. B. AWS-Ausfall)
  - Datenhoheit: Daten können außerhalb der EU gespeichert werden (DSGVO-konforme Verarbeitung muss gewährleistet sein)
  - US-Clouds unterliegen z. B. Cloud Act / US-Gesetzen, wodurch Behörden Zugriff auf Daten erhalten könnten.
  - Abhängigkeit von Technologie und Schnittstellen, Lock-in-Effekt: Migration zu alternativen Cloud-Anbietern kann teuer und aufwendig sein.
  - Geopolitische und wirtschaftliche Risiken: Sanktionen, Exportkontrollen oder politische Konflikte könnten Dienstleistungen oder Datentransfers einschränken.
  - Bitkom-Umfrage: 90 % Unternehmen vom Import digitaler Technologien & Services aus anderen Ländern abhängig, insb. USA & China

- ***Welche Maßnahmen könnten zur Stärkung der digitalen Souveränität und zur Förderung europäischer Alternativen beitragen?***

  IHK:
  - Produktionskapazitäten strategischer Hardwarekomponente & Infrastruktur steigern
    - Europäische Cloud- und Rechenzentrumskapazitäten optimieren und ausbauen
    - Produktionskapazitäten essenzieller Infrastruktur- und IT-Komponenten stärken (EU Chips Act, sichere Lieferketten etablieren, bürokratiearme Standortbedingungen,…)
    - IKT-Infrastruktur-Ausbau beschleunigen
  - Europa als internationalen Leitstandort für die Entwicklung und wirtschaftliche Nutzung innovativer Softwarelösungen aufbauen
    - Schlüsseltechnologien entwickeln und globale Standards setzen
    - Open Source als strategischen Baustein nutzen
  - Handlungs- und Gestaltungsrahmen für die Digitale Souveränität schaffen:
    - Öffentliche Beschaffung für Produkte unter europäischer Kontrolle
    - Digitale Kompetenzen flächendeckend vermitteln
    - Umfassenden Cybersicherheitsrahmen aufbauen
    - Innovationsfreundlichen regulatorischen Rahmen gestalten

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

- Einen funktionierenden europäischen Binnenmarkt für Daten entwickeln
  - Europäische Datenräume etablieren
  - Datenmarktplätze und Datenvermittlungsdienste schaffen

5. Regulatorische Anforderungen und Umsetzung

- ***Welche gesetzlichen Vorgaben zur Einhaltung von IT-Sicherheit, insbesondere zu Standards und Zertifizierungen, bestehen für bayerische Unternehmen?***

  IHK: Standards und Zertifizierungen (ISO 27001, EN 50600, TISAX…) dienen als Compliance-Nachweis und ggf. als Marktzugangsvoraussetzung.
  Neben den grundsätzlichen gesetzlichen Regelungen zur ordnungsgemäßen, sicheren und verantwortungsvollen Unternehmensführung (z. B. GmbHG „§ 43 Haftung der Geschäftsführer“) gibt es mehrere Cybersicherheitsspezifische Vorgaben:
  - **IT-Sicherheitsgesetz 2.0** (seit Ende 2021): Betrifft Kritis-Unternehmen mit Meldepflichten, Mindeststandards.
  - **Datenschutz-Grundverordnung (DSGVO):** Technische und organisatorische Maßnahmen (TOMs) zur Datensicherheit personenbezogener Daten.
  - **Cyber Resiliance Act** (seit 11.12.2024, ab September 2026 Meldepflichten, ab Dezember 2027 vollständig): Mindeststandards für digitale Produkte IKT-Anbieter müssen diese erfülle, IT-Anwender ggf. einfordern
  - **NIS2-Umsetzung (noch im Gesetzgebungsverfahren)**: Ca. 30.0000 Unternehmen betroffen bzgl. Mindestmaßnahmen zur Cybersicherheit, Melde- und Registrierungspflichten.
  - **DORA** („Digital Operational Resilience Act“): Sicherstellung, dass Finanzunternehmen in der EU digital widerstandsfähig sind. IHK prüft hier einige bayerische Unternehmen.
  - **§202 StGB: Vorbereiten des Ausspähens und Abfangens von Daten („Hackerparagraph“):** Wenn ein IT-Sicherheitsunternehmen ein anderes Unternehmen darauf hinweist, dass ggf. Schwachstellen vorliegen, kann dies zu strafrechtlichen Ermittlungen führen.
  - Keine gesetzlichen, aber oft Marktzugangsvoraussetzung über vertragliche Pflichten: z. B. **TISAX** in der Automobilindustrie

- ***Welche Herausforderungen bestehen für bayerische Unternehmen aus Expertinnen- und Expertensicht bei der Umsetzung? Wo bestehen ggf. Unterstützungsmöglichkeiten durch staatliche Stellen?***

  IHK: Insbesondere bei der (Ende 2025 oder Anfang 2026 zu erwartenden) NIS2-Umsetzung sind Unternehmen unsicher, ob sie direkt betroffen sind und was exakt ggf. getan werden muss. Hier ist an erster Stelle das BSI gefragt, welches für Bayern mit dem LSI eng kooperiert (FÜRACKER, PLATTNER UND GEISLER: BAYERN UND BUND IM SCHULTERSCHLUSS FÜR MEHR IT-SICHERHEIT,

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

https://www.stmfh.bayern.de/internet/stmf/aktuelles/pressemitteilungen/26025/).
Daher sollte das LSI (in enger Abstimmung mit dem BSI) Unternehmen unterstützen können bei der NIS2-Umsetzung, z. B. mit Informationsveranstaltungen, ggf. individueller Beratung und Hinweisen für die konkrete Umsetzung.

In ähnlicher Weise ist eine Zusammenarbeit des LSI mit dem BSI bzgl. CRA vorstellbar: Das BSI ist hier für Deutschland die marktüberwachende Behörde gegenüber der Europäischen Kommission.

IHK Forderung: Ethische Schwachstellenforschung legalisieren
Der §202 StGB („Hackerparagraph“) kann IT-Sicherheitsforscher bei der Schwachstellenmeldung kriminalisieren, was die Zusammenarbeit erschwert. Das Identifizieren und Melden von Schwachstellen zum Schutz Betroffener muss legalisiert werden. Ein „Coordinated-Vulnerability-Disclosure (CVD)-Prozess“ nach niederländischem Vorbild sollte klare Schritte für Forscher und Betroffene definieren, um eine sichere Zusammenarbeit zu ermöglichen.
Konkret könnte das LSI aufrufen „Bitte melden Sie Schwachstellen in staatlichen Webanwendungen direkt an das Bayern-CERT.“ und in einen CVD- oder BugBounty-Prozess überführen (linke Spalte auf Landesamt für Sicherheit in der Informationstechnik, https://www.lsi.bayern.de).

- ***Welche möglichen Nachteile ergeben sich für die Wettbewerbsfähigkeit bayerischer Unternehmen im Bereich IT- und Cybersicherheit durch nationale oder europäische Regulierung (z. B. zusätzliche Bürokratie)?***

IHK: Gleiche Spielregeln – aber auch Durchsetzung - für alle!
Wenn nicht-bayerische Unternehmen in der Lage sind, die Regulierungen zur Cybersicherheit zu unterlaufen, haben hiesige Unternehmen einen Wettbewerbsnachteil. Daher müssen die Regulierungen konsequent durchgesetzt werden. Dies betrifft insbesondere Produkte, die über internationale Plattformen bestellt und importiert werden und dabei den hiesigen Sicherheitsanforderungen nicht entsprechen.

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft" am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

6. Wirtschaftliche Auswirkungen und Kosten

- ***Welche wirtschaftlichen Schäden entstehen durch Cyberangriffe auf Unternehmen in Bayern? Inwieweit kam es dadurch bisher zu spürbaren Einschränkungen der laufenden Produktion?***

  IHK: Bundesweit geht die Bitkom-Studie „Wirtschaftsschutz 2025" von ca. 202 Mrd. € Schaden durch Cyberattacken aus. Diese Zahl ist in Relation zu den Vorjahreszahlen (2024: 179 Mrd. €) zu sehen, aber weniger als absolute Zahl (z. B. im Vergleich zum BIP). Grund: Die Angaben der Befragten Unternehmen erscheinen als zu hoch, z. b. werden 53 Mrd. € als „Kosten für Rechtsstreitigkeiten" angeben. Die gesamte Branche „Rechtsberatung" macht jährlich aber nur einen Gesamtumsatz von ca. 29 Mrd. €.

  Für Bayern schreibt das Bay. Innenministerium: „Im Jahr 2024 wurden allein in Bayern 44.917 Fälle registriert, bei denen das Internet als Tatmittel bei Straftaten eingesetzt wurde. Dabei entstand ein Gesamtschaden in Höhe von 48,9 Millionen Euro. Darüber hinaus muss von einer hohen Dunkelziffer ausgegangen werden, da viele Straftaten aus dem Bereich Cybercrime nicht zur Anzeige gebracht werden."

- ***Welche Dunkelziffer ist bei gemeldeten Schäden realistisch anzunehmen?***

  IHK: Laut BSI und Bitkom-Studien melden nur etwa 20–25 % der betroffenen Unternehmen ihre Vorfälle. Das bedeutet eine Dunkelziffer von ca. 75–80 %. Das erschein realistisch.

- ***Wie bewerten Sie die Kosten-Nutzen-Relation von Investitionen in IT-Sicherheit, insbesondere für KMU?***

  IHK: Die Herausforderung gerade für KMU ist es, eine angemessene IT-Sicherheit zu realisieren. D. h. **mit angemessen Investitionen die Wahrscheinlichkeit für Schäden durch Cybersicherheitsvorfälle deutlich zu reduzieren**.

  Grundsätzlich gilt: Die Kosten der IT-Sicherheitsmaßnahmen reduzieren nur die Eintrittswahrscheinlichkeit oder die Schadenshöhe:
  - Kosten von IT-Sicherheitsmaßnahmen:
    Personalkosten für Kümmerer um IT-Sicherheit, Firewalls, Antivirus, Endpoint Protection, Backup- und Recovery-Systeme, Mitarbeiterschulungen & Awareness, Mitarbeiterschulungen & Awareness, Monitoring & Incident Response…
    Ein kleiner Betrieb (10–50 MA) könnte zwischen 5.000 – 50.000 € pro Jahr für eine grundlegende Sicherheitsstrategie ausgeben.

  - Nutzen von IT-Sicherheitsinvestitionen:
    Vermeidung von Schäden, Reputationsschutz, Reputationsschutz, Produktivitäts- und Betriebsstabilität….

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

- Die Kosten-Nutzen-Relation ist sehr individuell. Wichtig ist, dass sie überhaupt gemacht wird. Angemessene Kosten von IT-Sicherheitsmaßnahmen liegen vor, wenn die Investition in IT-Sicherheit die wahrscheinlichen Kosten eines Vorfalls reduziert.

- ***In welchen wirtschaftlichen Nischen im Bereich Cybersicherheit haben bayerische IT-Unternehmen besondere Stärken oder Chancen in der internationalen Arbeitsteilung?***

  IHK:
  - **Stärke:** Bayern hat eine gute Ausgangslage – starke Industrie, ausgezeichnete Forschung, gute Netzwerke im Bereich Cybersicherheit.
  - **Chancen:** Besonders in Nischen mit hohem Spezialisierungsgrad (z. B. Industrielle / „Industrial Security“ für Fertigung und Anlagen, kritische Infrastruktur, Compliance-Dienstleistungen, KI, Quantencomputer, Verteidigung) können bayerische Unternehmen internationale Rollen übernehmen.

7. Sensibilisierung, Ausbildung und Fachkräftemangel

- ***Wie ist der Stand der Sensibilisierung und Weiterbildung im Bereich IT-Sicherheit in Unternehmen?***

  IHK: In den Unternehmen fehlen oftmals IT-Sicherheitsexpertise ebenso wie digitale Anwendungs-Kompetenzen. Dabei sind gerade Mitarbeitende trotz technischer Sicherheit ein großes Risiko für die IT-Sicherheit. Ohne entsprechendes Knowhow im Unternehmen kann ein ausreichender Cyberschutz nicht sichergestellt werden. Ziel muss sein, dass in Unternehmen alle IT-Anwendenden über grundlegendes Wissen in IT-Sicherheit und KI verfügen und ausreichend IT-Sicherheitsfachkräfte für Entwicklung wie Einsatz im Unternehmen vorhanden sind.

- ***Gibt es ausreichend qualifiziertes Personal, um die IT-Sicherheit in Unternehmen zu gewährleisten? Wo sehen Sie etwaige Engpässe und deren Ursachen?***

  IHK: Das Angebot spezialisierter Bildungswege zu IT-Sicherheitsfachkräften muss ausgeweitet und attraktiv gestaltet werden. Der Staat soll zudem mehr hochqualifizierte IT-Sicherheitsfachkräfte ausbilden. Dabei sollte er – über eine angemessene Bezahlung hinaus - seine besondere Attraktivität als Arbeitgeber in der IT-Sicherheit stärker hervorheben: Arbeitserfahrungen bei BSI, Strafverfolgungsbehörden oder Militär zielen direkt auf die nationale Sicherheit und den Schutz der Gesellschaft und können besonders lehrreich sein. Von Mitarbeitenden mit solchen Erfahrungen können auch Unternehmen anschließend profitieren.

- ***Wie kann die Aus- und Weiterbildung von IT-Sicherheitsfachkräften an bayerischen Hoch- und Berufsschulen verbessert werden?***

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

IHK: IT-Sicherheits-Kompetenzen in allen Phasen umfassend stärken:
Digitale Fähigkeiten, insbesondere zur IT-Sicherheit und KI müssen frühzeitig und umfassend in Schulen, Ausbildung, Studium und in den Betrieben vermittelt werden.

8. Zukunftsperspektiven und Innovation

- ***Welche technologischen Trends (z. B. Künstliche Intelligenz, Cloud-Lösungen) beeinflussen die IT-Sicherheitslage aktuell und künftig?***

  IHK: Entwicklung von Schlüsseltechnologien zur IT-Sicherheit vorantreiben.
  Technologische Fortschritte wie KI fördern sowohl Cyberangriffe als auch Abwehrmöglichkeiten. Der Staat sollte die Entwicklung von Schlüsseltechnologien wie IoT, KI, Blockchain und Quantencomputing für die IT-Sicherheit durch Initiativen wie die Agentur für Sprunginnovationen bzw. auf Landesebene als Fokus der Arbeit der KI-Agentur Bayerns oder des Munich Quantum Valley vorantreiben, innovative Anwendungen fördern und als Pilotnutzer neue Technologien selbst einsetzen.

- ***Wie kann Bayern als Wirtschaftsstandort die digitale Souveränität stärken und Abhängigkeiten von internationalen IT-Anbietern verringern?***

  IHK:
  - **Forschungstransfer verbessern:**
    Deutschland ist führend in der IT-Sicherheitsforschung, jedoch fehlt oft die Umsetzung in marktfähige Produkte und der Transfer zu KMU. Wichtig sind verstärkter Wissenstransfer, Kooperationen zwischen Wissenschaft und Wirtschaft sowie Vermittlung von Entrepreneurship-Knowhow. Die Forschungsförderung sollte stärker auf Produktentwicklung und die Einbindung von Unternehmen ausgerichtet werden.
  - **Innovationspotenzial von Startups stärken:**
    Startups benötigen bessere Finanzierungsmöglichkeiten, etwa durch größere Venture-Capital-Fonds oder steuerliche Vorteile, besonders beim Übergang von der Frühphase in die Unternehmensphase. Regulierungen wie AI-Act, NIS2 und CRA müssen startupfreundlich gestaltet werden, um Entwicklungsspielraum zu sichern. Die öffentliche Hand sollte das Innovationspotenzial von Startups gezielter in Vergabeverfahren nutzen.
  - **IT-Sicherheit in Open Source unterstützen:**
    Open Source-Software ist zentral für die IT, wird aber oft von kleinen Communities getragen, was Sicherheitsrisiken birgt. Daher braucht es verstärkte Unterstützung, etwa durch Initiativen wie den „Sovereign Tech Fund“ und den „PrototypeFund“. Projekte wie die „Codeanalyse von Open Source Software“ des BSI sollten ausgebaut werden, um die Sicherheit im Open-Source-Ökosystem zu stärken.

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft“ am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

9. Empfehlungen für die Politik

- ***Inwieweit kann die Politik bayerische Unternehmen dabei unterstützen, ihre IT-Sicherheit weiter zu stärken?***

  IHK:
  Die Wirtschaft soll durch staatliche Einrichtungen zielgerichtet unterstützt werden.
  Unternehmen benötigen gezielte staatliche Unterstützung bei IT-Sicherheit. Maßnahmen umfassen:
  - Zentrale Lotsenstelle: Eine unabhängige, zentrale Anlaufstelle soll Unternehmen Präventions- und Notfallhilfe bieten.
  - Zielgruppenspezifische Angebote: Branchenspezifische IT-Sicherheitsstandards und -hilfen, z. B. nach dem Vorbild des BSI-CyberRisikoChecks, sollen ausgebaut werden, besonders für kleine Unternehmen.
  - Sensibilisierung stärken: Selbsthilfe-Angebote, Musterunterlagen und Weiterbildung (z. B. DSiN-Digitalführerschein) sollen den Knowhow-Aufbau fördern.
  - Schwachstelleninfo: Staatliche Warnungen und Handlungsempfehlungen zu Schwachstellen müssen ausgebaut werden.

- ***Wie werden aktuell verfolgte Maßnahmen auf Bundes- und Landesebene dahingehend bewertet?***

  IHK:
  - Zentrale Lotsenstelle:
  Es gibt sehr viele Akteure zum Thema Cybersicherheit, sowohl auf staatlicher Seite (Übersichtskarte: Cybersicherheitsarchitektur, https://www.cybersicherheitsarchitektur.de/) als auch im privatwirtschaftlichen Bereich.
  Für Unternehmen ist es aber nicht einfach, passende Kontakte zu finden. Insbesondere die Sicherheitsbehörden agieren immer mit dem Aspekt der Strafverfolgung, was zumindest in der Prävention die Akzeptanz bei Unternehmen einschränkt.
  Hier würde eine neutrale Lotsen-Einrichtung (wie z. B. die Cybersicherheitsagentur Baden-Württemberg, https://www.cybersicherheit-bw.de/) helfen, die begleitet und informiert.
  Wichtig ist es den Austausch aller Betroffenen zu fördern und das Lagebild mit dessen Nutzen zu verbessern.

IHK für München und Oberbayern
Interfraktioneller Fragenkatalog
Anhörung „IT-Sicherheit in der bayerischen Wirtschaft" am 27.11.2025
Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung
Stand: 20.11.2025

- Zielgruppenspezifische Angebote:
Positive Beispiele hierfür sind die Unterstützungsangebote des Bayerischen Landesamt für Sicherheit in der Informationstechnik (LSI), die für einzelne Branchen wie Wasserkraftwerke oder Kliniken entwickelt werden. Kleine Unternehmen benötigen besondere Unterstützung. Zielführend wäre es, nach dem Vorbild des BSI-CyberRisikoChecks nach DinSpec 27076 gemeinsam mit IT-Sicherheitsunternehmen weitere Standards und Hilfen zur IT-Sicherheit zu entwickeln.
- Sensibilisierung stärken:
Der dringend notwendige Knowhow-Aufbau in Unternehmen muss durch zielgerichtete Sensibilisierungs- und Selbsthilfe-Angebote unterstützt werden wie z. B. durch die Vermittlung technischer Standards, Angebote zu anerkannten Musterunterlagen (z. B. Checklisten, IT-Notfallpläne), Gütesiegel für Weiterbildungsangebote (z. B. DSiN-Digitalführerschein) oder durch Gamification-Ansätze.
- Mit IT-Sicherheitslücken verantwortungsbewusst umgehen:
Grundsätzlich müssen alle Anstrengungen unternommen werden, bekannt gewordene Schwachstellen möglichst schnell zu schließen. Nur in außergewöhnlichen Fällen nationaler Sicherheit dürfen Schwachstellen temporär geheim gehalten werden. Der CVD-Prozess dafür muss klar und verbindlich definiert sein

- ***Wo werden Potenziale gesehen, die Zusammenarbeit von Staat, Wirtschaft und Forschung zur Erhöhung der Resilienz gegen Cyberbedrohungen weiter zu verbessern?***

IHK:
- Der Freistaat sollte bei öffentlichen **Ausschreibungen** Cybersicherheit und digitale Souveränität als entscheidungsrelevantes Kriterium berücksichtigen, so dass lokale Unternehmen Chancen bekommen.
- **Forschungstransfer verbessern:**
Maßnahmen hierfür sollten verstärkte Vermittlung von Entrepreneurship-Knowhow in der Wissenschaft und mehr Kooperationen mit der Wirtschaft, vor allem kleinen und mittleren Unternehmen, sein. Die Forschungsförderung muss die Produktentwicklung mit in den Fokus nehmen, z. B. durch stärkere Einbindung von Unternehmen.
- Innovationspotenzial von Startups stärken:
Compliance und Finanzierung sind für Startups wesentliche Herausforderungen: Die Finanzierungsmöglichkeiten für Startups müssen verbessert werden, z. B. durch großvolumige Venture-Capital Fonds oder eine attraktive steuerliche Behandlung von Investitionen in sie (z. B. für Mitarbeiter). Das gilt insbesondere beim Übergang aus der Frühphase (z. B. Ende Exist-Gründerstipendium) in die Unternehmensphase.
Strenge und umfangreiche Complianceanforderungen führen dazu, den Standort Deutschland und EU für Startups unattraktiv zu machen: Daher müssen alle Regulierungen (z. B. AI-Act, NIS2, CRA) so gestaltet sein, dass sie Startups genügend Spielraum für die Entwicklung lassen.
Die öffentliche Hand sollte das Innovationspotenzial von Startups bei Vergabeverfahren besser nutzen können.