



Ministerium des Inneren, für Digitalisierung und Kommunen
Baden-Württemberg

📅 19.02.2020

DIGITALISIERUNG

2. CyberSicherheitsForum in Stuttgart



📷 Steffen Schmid

Künstliche Intelligenz ist Innovationsmotor und Sicherheitsrisiko zugleich. Das 2. CyberSicherheitsForum nahm daher die Chancen und Risiken der KI für die Cybersicherheit in den Blick. Rund 350 Teilnehmerinnen und Teilnehmer sowie zahlreiche Expertinnen und Experten aus Wirtschaft, Wissenschaft und Sicherheitsbehörden folgten der Einladung zum interdisziplinären Austausch.

„Damit wir im weltweiten Wettbewerb bestehen können, muss ein Hochtechnologieland wie Baden-Württemberg Künstliche Intelligenz als eine der Schlüsselinnovationen für Wirtschaft und Gesellschaft aufgreifen. Das gilt gerade auch für den Bereich Cybersicherheit. Die riesigen Datenmengen, mit denen KI arbeitet, müssen sicher sein, damit die Menschen Vertrauen in die digitalen Anwendungen haben. Ohne dieses Vertrauen werden wir das Potenzial der Digitalisierung nicht vollständig nutzen können“.

Stuttgart: „Die Zahl der Cyberangriffe – auch unter Einsatz von KI – nimmt jedoch immer mehr zu. KI kann also Innovationsmotor und Sicherheitsrisiko zugleich sein. Wir müssen uns intensiv damit beschäftigen, welche Chancen und Risiken KI für die Cybersicherheit bereithält.“

Unter dem Motto „Künstliche Intelligenz und Cybersicherheit“ hatten das Innenministerium und das Landeskriminalamt zum 2. CyberSicherheitsForum in die Räumlichkeiten der **IHK Region Stuttgart** eingeladen. Rund 350 Teilnehmerinnen und Teilnehmer sowie zahlreiche Expertinnen und Experten aus Wirtschaft, Wissenschaft und Sicherheitsbehörden waren der Einladung gefolgt und trafen sich zum interdisziplinären Austausch. Gerade mittelständische Unternehmen sollen auf diesem Weg für die Chancen und Gefahren von KI im Zusammenhang mit Cybersicherheit sensibilisiert werden. „Für die Unternehmen im Land ist der Einsatz Künstlicher Intelligenz und die Sicherheit vor Cyberangriffen immer bedeutsamer. Umso mehr freuen wir uns, dass das 2. CyberSicherheitsForum bei uns im Haus zu Gast ist“, sagte Johannes Schmalzl, Hauptgeschäftsführer der Industrie- und Handelskammer (IHK) Region Stuttgart. Die IHK Region Stuttgart ist wie das **Landesamt für Verfassungsschutz**, der Branchenverband **Bitkom** und die **Allianz Industrie 4.0** Partner der Veranstaltung.

Das **1. CyberSicherheitsForum** hatte am 7. Februar 2019 unter dem Motto „Wirtschaft.Digital.Sicher“ im Haus der Wirtschaft stattgefunden. Wie die erfolgreiche Premiere wartete auch das 2. CyberSicherheitsForum mit hochkarätigen Referentinnen und Referenten aus dem In- und Ausland auf. **Lena-Sophie Müller**, seit 2014 Geschäftsführerin der Initiative D21 e.V. und Sachverständige der Enquete Kommission „Künstliche Intelligenz“ des Bundestags, führte das Publikum mit ihrem Impulsvortrag zunächst in das Thema KI ein. An der anschließenden Podiumsdiskussion nahmen außerdem Frau **Prof. Dr. habil. Jana Koehler**, Direktorin am Deutschen Forschungszentrum für Künstliche Intelligenz GmbH (DFKI) in Saarbrücken, **Prof. Dr. Gabi Dreo Rodosek**, Leiterin des Lehrstuhls für Kommunikationssysteme und Netzsicherheit der Universität der Bundeswehr München, und **Karl-Heinz Streibich**, Präsident von acatech – Deutsche Akademie der Technikwissenschaft München, teil.

Die vier Fachpanels setzten unterschiedliche Schwerpunkte: Diskutiert wurde die KI-Wertebasis mit Fragen rund um Ethik, Recht und Datenschutz sowie Einsatzmöglichkeiten der KI im öffentlichen Bereich aufgezeigt. Im meistbesuchten Panel gewährten Betroffene von Cyberattacken, wie Stefan Würtemberger, CIO der Marabu GmbH & Co. KG aus Tamm, spannende Einblicke in den Ablauf des Angriffs und dessen Folgen für das Unternehmen. Thomas Pilz, Geschäftsführender Gesellschafter der Pilz GmbH & Co. KG aus Ostfildern berichtete: „Wir haben aus dem Angriff gelernt, dass Investitionen in Security Software alleine nicht ausreichen, aktuell sichere Cyber-Abwehr spätestens nach drei Jahren veraltet und verwundbar wird, aber unsere Polizei bei diesem Thema bestens aufgestellt ist.“ Im vierten Panel brachten Start-ups ihre Perspektive ein und erläuterten wie sie KI und Cybersicherheit verbinden, darunter junge Unternehmen aus Israel und Baden-Württemberg. Mit BLACKPIN war auch ein Start-up vertreten, dass durch das Land gefördert wurde.

Zum Abschluss erhielten die Teilnehmerinnen und Teilnehmer per Liveschalte Einblick in das Cyber Defense und Security Operation Center (SOC) der Deutschen Telekom. Dort werden jeden Tag mehrere Millionen Angriffe verzeichnet werden. Das Bedrohungspotenzial durch Cyberkriminelle wurde dadurch noch einmal ganz plastisch vor Augen geführt.

Cybersicherheit made in Baden-Württemberg

„Seit Jahren wächst die Zahl der Cyberangriffe und auch die Liste betroffener Unternehmen aus Baden-Württemberg wird immer länger. Wir dürfen uns nichts vormachen: Jeden kann ein Cyberangriff treffen. Cybersicherheit ist daher ein Schwerpunkt der Landesregierung. Wir wollen ‚Cybersicherheit made in Baden-Württemberg‘ zu unserem Markenzeichen machen und arbeiten daran schon tatkräftig: Bei unserer **Polizei** verfügen wir bereits flächendeckend über spezialisierte Organisationseinheiten zur Bekämpfung von Cybercrime und mit der **Cyberwehr**, die gerade kleinen und mittleren Unternehmen bei einem Cyberangriff praktische Hilfe bietet, leisten wir bundesweit Pionierarbeit. Den nächsten logischen Schritt gehen wir mit der ganzheitlichen Cybersicherheitsstrategie und unserer Cybersicherheitsagentur,“ erklärte Innen- und Digitalisierungsminister Thomas Strobl.

Derzeit wird im Digitalisierungs- und Innenministerium eine ganzheitliche Cybersicherheitsstrategie für Baden-Württemberg erarbeitet. Das Ziel ist, Informationen zentral zu bündeln und Aufgaben dezentral wahrzunehmen. Die Koordinierung und Steuerung soll eine „Cybersicherheitsagentur“ des Landes übernehmen. Für ihren Aufbau sind im Landeshaushalt für 2020/21 insgesamt 13 Mio. Euro vor allem für 83 Personalstellen vorgesehen. Eine Vorbereitungsgruppe trifft bereits im laufenden Jahr die gesetzlichen, administrativen und strukturellen Vorbereitungen für den Start des Aufbaustabs im Jahr 2021. Minister Strobl hob hervor: „Wir wollen erreichen, dass sich Unternehmen und Bürgerinnen und Bürger in Baden-Württemberg nicht nur zuhause fühlen, sondern auch sicher. Und kein Zweifel: KI wird die Cybersicherheit massiv und nachhaltig beeinflussen, die damit verbundenen Innovationen werden sowohl für Angriff als auch Verteidigung genutzt.“

Spannungsfeld Künstliche Intelligenz

KI gilt für immer mehr Bereiche als großer Zukunftstrend und ist auch ein zentraler Baustein der landesweiten **Digitalisierungsstrategie digital@bw**. KI wird schon heute in Unternehmen genutzt, um Abläufe zu automatisieren, Anwendungsprobleme zu lösen oder Sicherheitslücken aufzuspüren. Expertinnen und Experten gehen davon aus, dass KI schon bald in nahezu allen Unternehmensbereichen Einzug hält. Sie bietet Unternehmen auch vielfältige Chancen für neue Geschäftsmodelle und Wertschöpfungsprozesse.

KI wird aber auch eingesetzt, um Anomalien aufzudecken. Anomalien sind Abweichungen von bereits bekanntem Verhalten, und solche Abweichungen können auf bösartige Absichten hinweisen, die auf verärgerte Beschäftigte, Malware oder gar Kriminelle zurückgehen. Die Attacken sind in der Regel gut vorbereitet. Zuerst spionieren die Täterinnen und Täter mit Hilfe von Spionage-Software etwa E-Mails und Finanzdaten des Unternehmens aus, sichern sich Zugriff auf alle relevanten Systeme und installieren letztendlich die Verschlüsselungssoftware. Angriff und Verteidigung stehen demnach in einem permanenten Wettkampf um die besten technologischen Instrumente.

Mit dem **Cyber Valley** um das Max-Planck-Institut für intelligente Systeme, die Universitäten Tübingen und Stuttgart hat Baden-Württemberg einen international herausragenden Forschungsstandort. Bosch beispielsweise erhöht die Investitionen in sein geplantes KI-Entwicklungszentrum in Tübingen auf 100 Millionen Euro, Amazon und andere namhafte Unternehmen wie Daimler, Porsche, ZF und BMW forschen ebenfalls vor Ort. Der Südwesten nimmt daher auch schon bei der Anwendung von KI mit bereits knapp über 80 KI-Innovationen einen der Spitzenplätze ein. Beim **Landeskriminalamt Baden-Württemberg** investieren wir ebenfalls in KI und machen es fit für die Zukunft. KI soll bei der

Kriminaltechnik und der Datenanalyse unterstützen, damit Tatzusammenhänge schneller erkannt, Ermittlungszeiten verkürzt und Straftaten besser aufgeklärt werden.

Zahlreiche Eindrücke des 2. CyberSicherheitsForums finden Sie in unserer [Mediathek](#).