Kandidat:innen

für die Wahl der Vorstandspositionen im Sicherheitsnetzwerk München e.V. am 27. November 2025.

1. **Sebastian Dännart** – Director Cybersecurity Consulting, infodas
2. **Prof. Dr. Gabi Dreo** – Lehrstul für Kommunikationssysteme und Netzsicherheit, Universität der Bundeswehr München
3. **Prof. Dr. Claudia Eckert** – Leiterin, Fraunhofer Institut AISEC und Lehrstuhl für IT-Sicherheit, Technische Universität München
4. **Markus Geier** – Gründer und CEO, COMCODE
5. **Nils Gerhardt** – CTO, Utimaco
6. **Dr. Falk Herrmann** – CTO, Funkwerk
7. **Dr. Wieland Holfelder** – Vice President Engineering und Lead of Google Engineering Center, Google
8. **Dr. Tobias Kiesling** – Head of Consulting & Professional Services Germany, Airbus Protect
9. **Dr. Andreas Kind** – Vice-President Cybersecurity & Trust, Siemens
10. **Gabriele Meier** – Head of Sales, genua
11. **Gabriel von Mitschke-Collande** – Mitglied der Konzerngeschäftsführung, Group CDO, Giesecke+Devrient
12. **Dr. Christoph Peylo** – Chief Cyber Security Officer (CCSO), Bosch
13. **Dr. Alexander Schellong** – Managing Director Cybersecurity (GL) und Mitglied des Vorstands, Schwarz Digits
14. **Prof. Dr.-Ing. Thomas Schreck** – Professor für IT-Security und Chief Information Officer (CIO), Hochschule München
15. **Philipp Spangenberg** – Director Product Development Management Suite, baramundi

Prof. Dr. Gabi Dreo Rodosek

Lehrstuhl für Kommunikationssysteme und Netzsicherheit, Universität der Bundeswehr München

Prof. Gabi Dreo leitet den Lehrstuhl für Kommunikationssysteme und Netzsicherheit an der Universität der Bundeswehr München. Sie ist Gründungsdirektorin des Forschungsinstituts CODE (Cyber Defence), Aufsichtsrats- und Beiratsmitglied der Giesecke+Devrient GmbH sowie Aufsichtsratsmitglied der BWI GmbH. Außerdem ist sie u.a. Mitglied des Digitalrats des Bundesministeriums der Verteidigung, Mitglied des Datenschutzbeirats der Deutschen Telekom AG, Mitglied des Hochschulrats der Hochschule Fresenius, Vorstand des Digitalausschusses des Wirtschaftsbeirats Bayern e.V., Mitglied des Vorstands des Sicherheitsnetzwerks München e.V., Mitglied des Beirats Deutschland Sicher im Netz e.V., Mitglied des Security Innovation Boards der Münchner Sicherheitskonferenz, Mitglied des Scientific Advisory Boards des Center for Cyber Defence and Information Security der KTH, Schweden, Mitglied des Kuratoriums der Edith-Haberland-Wagner Stiftung, Mitglied des Kuratoriums der Kunsthalle der Hypo-Kulturstiftung, Mitglied des Münchner Kreises e.V., Mitglied des Münchner Clubs der BMW-Stiftung. Mit Prof. Eckert und Herrn Ochs leitet Prof. Dreo auch das Expertengremium IT-Sicherheit (BayVFP) des Bayerischen Staatsministeriums für Wirtschaft Landesentwicklung und Energie. Ferner war sie Koordinatorin des EU-H2020-Projekts CONCORDIA (https://www.co-cordiah2020.eu) mit insgesamt 56 Partnerorganisationen aus 21 Ländern. Im Jahr 2016 wurde ihr die Bayerische Europamedaille verliehen.

Die digitale Souveränität Europas liegt mir besonders am Herzen. Sie ist die Grundlage unserer technologischen Unabhängigkeit, unserer Innovationskraft und einer zukunftsfähigen digitalen Gesellschaft. Ich bin überzeugt, dass ein resilientes und zugleich sicheres digitales Europa nur durch das enge Zusammenwirken von Forschung,

Wirtschaft, Politik und Gesellschaft in einem starken, vertrauenswürdigen Ökosystem entstehen kann. Mit meiner Kandidatur möchte ich weiterhin dazu beitragen, dieses

Ökosystem, insbesondere hier in Bayern, zu stärken und auszubauen. Dabei bringe ich meine fachliche Expertise und mein Netzwerk ein, um die Sichtbarkeit des Sicherheitsnetzwerks e.V. zu erhöhen, die Brücken zwischen zivilen und sicherheitsrelevanten Anwendungen (Dual-Use) zu schlagen und einen Beitrag zur Stärkung der europäischen digitalen Souveränität zu leisten.

Prof. Dr. Claudia Eckert

Leiterin, Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit AISEC

Lehrstuhl für IT-Sicherheit, Technischen Universität München

Prof. Dr. Claudia Eckert ist Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit AISEC in Garching und Professorin der Technischen Universität München, wo sie den Chair of IT Security am Department of Computer Engineering (CE) der School of Computation, Information and Technology (CIT) innehat.

Zu ihren Forschungsschwerpunkten zählen die Entwicklung von Technologien zur Erhöhung der System-und Anwendungssicherheit, die Sicherheit eingebetteter Systeme und die Erforschung neuer Techniken zur Erhöhung der Resilienz und Robustheit von Systemen gegen Angriffe. Ihre Forschungsergebnisse wurden in über 160 begutachteten Fachbeiträgen veröffentlicht.

Seit dem 1.1.2018 ist sie die Sprecherin des Fraunhofer Clusters of Excellence Cognitive Internet Technologies CCIT, in dem die Expertisen von über 20 Fraunhofer-Instituten gebündelt werden, um neue kognitive Lösungen vom Sensor über Edge-Devices bis in die Cloud-Plattformen für die Digitalisierung insbesondere im industriellen Umfeld zu entwickeln und umzusetzen.

Seit dem 1.7.2025 ist Claudia Eckert neue wissenschaftliche Präsidentin von acatech – Deutsche Akademie der Technikwissenschaften. In dieser Funktion steht sie gemeinsam mit Ko-Präsident Thomas Weber an der Spitze der Akademie, die Politik und

Gesellschaft in Fragen technologiegetriebener Innovationen berät. Bereits seit 2010 ist sie Mitglied von acatech, seit 2014 Mitglied des Präsidiums.

Als Mitglied verschiedener nationaler und internationaler industrieller Beiräte und wissenschaftlicher Gremien berät sie Unternehmen, Wirtschaftsverbände sowie die öffentliche Hand in allen Fragen der IT-Sicherheit. In Fachgremien wirkt sie mit an der Gestaltung der technischen und wissenschaftlichen Rahmenbedingungen in Deutschland sowie an der Ausgestaltung von wissenschaftlichen Förderprogrammen auf EU-Ebene.
Als **Mitinitiatorin und Gründungsmitglied der Initiative war es von Beginn an (seit 2012)** mein Ziel, in der Metropolregion München ein Sicherheitsnetzwerk zu etablieren, das die Expertise und die Stakeholder, sowohl Anbieter, insbesondere KMUs, als auch Bedarfsträgerseite, aber auch Start-ups im Bereich Cybersicherheit zusammenzubringt. Mein Ziel ist es, weiterhin aktiv beizutragen, dass durch die Vernetzung der Akteure, über die Angebote, Veranstaltungen und über die Menschen, die sich aktiv und engagiert einbringen, ein Mehrwert für alle ergibt.

Ein zentrales Ziel für mich ist es, das SNM als Plattform weiter auszubauen, so dass die etablierten, aber auch die neu entwickelten Angebote des SNM konsequent weiter ausgebaut werden, um einen Mehrwert für die Mitglieder zu bieten. Das **„voneinander Lernen“**, wie beispielsweise über Workshops, Meet-ups oder die TechDays, um Impulse aus der Forschung zu neuen, coolen Entwicklungen, oder über Best-Practice-Erfahrungen zu Problemen und wie sie gelöst wurden, gehört hier ebenso dazu, wie das **Match-making** u.a. das Zusammenbringen von Partnern, um gemeinsam in Konsortien an Ausschreibungen mitzuwirken und das Portfolio zu erweitern oder innovative Ideen in die Umsetzung in den Unternehmen zu unterstützen.

Mir ist aber auch wichtig, Unternehmen und Partner des SNM in den frühen **Austausch mit Nachwuchstalenten** im Bereich der Cybersicherheit zu bringen. Dafür haben wir im SNM Formate wie die TechDays entwickelt, um neuen Ideen und insbesondere auch Start-ups eine Bühne, Sichtbarkeit und eine Plattform für den Austausch zu verschaffen. Last but not least liegt mir auch der enge Schulterschluss mit der politischen Ebene sehr am Herzen. Als Wissenschaftlerin und Leiterin eines Forschungsinstituts ist es mir ein Anliegen, dass das **SNM Beiträge zur sachkundigen Beratung der Politik** liefert und dort auch Gehör findet, wie beispielsweise über Parlamentarische Abende. Die **MCSC** hat sich aus diesem Anspruch entwickelt, nicht nur national sondern auch international auf hoher politischer Ebene die Stakeholder zusammenzubringen. Diese Konferenz hat sich zu einer echten Success Story des SNM entwickelt.

Mein Ziel ist es, auch weiterhin aktiv zusammen mit den Partnern des SNM einen Beitrag dazu zu leisten, dass die Wirtschaft besser geschützt wird. Die Ausweitung der SNM-Aktivitäten auf den Bereich Cyberdefense gehört aus meiner Sicht dazu.

Gabriele Meier

Head of Sales, genua GmbH

Gabriele Meier ist seit 20 Jahren in der IT-Sicherheit tätig. Sie arbeitet bei der genua GmbH, einem Tochterunternehmen der Bundesdruckerei, und verantwortet dort als Abteilungsleiterin Sales und Prokuristin das Projektgeschäft für hochsichere IT-Security-Lösungen. Mit ihrer langjährigen Erfahrung verbindet sie tiefes Branchenwissen im Bereich kritischer Infrastrukturen mit strategischem Leadership in einem technologiegetriebenen Umfeld.

Im Sicherheitsnetzwerk München sehe ich einen essenziellen Ort des Austauschs zwischen Anbietern, Anwendern und Forschungseinrichtungen – und genau diese Zusammenarbeit möchte ich weiter stärken. Besonders wichtig ist mir dabei das Thema digitale Souveränität: Mein Ziel ist es, vertrauenswürdige und unabhängige Sicherheitslösungen zu fördern, die sowohl technisch führend als auch gesellschaftlich relevant sind. Mit meiner Erfahrung im Umfeld kritischer Infrastrukturen und meinem Netzwerk möchte ich aktiv zur strategischen Weiterentwicklung des SNM beitragen.

Sebastian Dännart

Director Cybersecurity Consulting, infodas

Sebastian Dännart ist 40 Jahre alt, Vater eines 1,5-jährigen Sohnes und lebt im Münchner Umland.

Er verfügt über mehr als 15 Jahre Berufserfahrung in der Informationssicherheit. Als Mitglied der Geschäftsleitung verantwortet er aktuell den Geschäftsbereich Cybersecurity Consulting der infodas mit rund 50 Beraterinnen und Beratern, mit Schwerpunkt auf stark regulierten Branchen, dem öffentlichen Sektor und kritischen Infrastrukturen. Ein besonderer Fokus seiner Arbeit liegt dabei auf wirksamem Stakeholder-Management, um Sicherheit in Organisationen nachhaltig zu verankern.

Sebastian ist seit Anfang 2023 wieder bei der infodas tätig, für die er bereits zuvor als IT-Security-Consultant arbeitete. In der Zwischenzeit verantwortete er mehrere Jahre als Information Security Officer bei Giesecke+Devrient die Informationssicherheit der gesamten Wertschöpfungskette von Sicherheitspapier und Banknoten an verteilten Hochsicherheitsstandorten – eine Aufgabe, die ein enges Zusammenspiel zwischen Produktion, IT, OT und Geschäftsführung erforderte.

Der studierte Wirtschaftsinformatiker und MBA diente zwölf Jahre als Offizier der Deutschen Marine. Dort war er sowohl für IT- und Waffensysteme an Bord verantwortlich als auch in der wissenschaftlichen Forschung zur IT-Sicherheit Kritischer Infrastrukturen an der Universität der Bundeswehr München tätig.

Sebastian studierte Wirtschaftsinformatik an der Universität der Bundeswehr München und absolvierte seinen MBA in IT-Management an der Technischen Hochschule Ingolstadt. Seit vielen Jahren lehrt er zu den Themen IT-Security-Management, IT-Governance und Geschäftsprozessmanagement und tritt regelmäßig als Keynote-Speaker, Moderator sowie im Programmbeirat verschiedener Fachkonferenzen auf – insbesondere zu Fragen der praktischen Umsetzung von Cybersicherheit und dem erfolgreichen Zusammenspiel ihrer Stakeholder.

Ich durfte das Sicherheitsnetzwerk München in den vergangenen zehn Jahren aus sehr unterschiedlichen Rollen aktiv begleiten – zunächst als Soldat und Forscher an der Universität der Bundeswehr München, später als CISO in der Industrie bei Giesecke+Devrient und heute aus der übergreifenden Perspektive der Beratung. Diese Vielfalt an Erfahrungen gibt mir einen breiten, systemischen Blick auf das Ökosystem der Cybersicherheit in München.

Was mich dabei seit jeher begleitet, ist die Überzeugung, dass erfolgreiche Cybersecurity vor allem dort entsteht, wo Menschen miteinander ins Gespräch kommen, Perspektiven teilen und gemeinsam Verantwortung übernehmen. Stakeholder-Management und der Aufbau vertrauensvoller Beziehungen sind für mich deshalb zentrale Elemente moderner Cybersicherheit – und genau hierin sehe ich auch die besondere Stärke des Sicherheitsnetzwerks.

Gerade im Großraum München bin ich tief verankert und schätze das Netzwerk als Plattform, die fachliche Expertise mit persönlicher Nähe verbindet. Als Vorstandsmitglied möchte ich frische Impulse einbringen, Perspektiven aus Wissenschaft, Industrie und Beratung zusammenführen und die Community weiter stärken. Ich möchte dem Netzwerk etwas von dem zurückgeben, was ich in den vergangenen Jahren durch Austausch, Kooperation und gelungene Zusammenarbeit gewinnen durfte.

Markus Geier

Gründer und CEO, COMCODE

Markus Geier ist Gründer und CEO von COMCODE. Mit mehr als 30 Jahren Führungserfahrung im Bereich Cybersecurity gilt er als führender Experte für resiliente digitale Architekturen, sichere digitale Transformation und Cyber-Krisenmanagement.

Unter seiner Leitung hat sich COMCODE als vertrauenswürdige Boutique-Beratung für Betreiber kritischer Infrastrukturen und internationale Unternehmen aus den Bereichen Real Estate, Construction, Biotech, Manufacturing und High-Tech etabliert. Markus' Expertise umfasst den gesamten Lebenszyklus der Cyber-Resilienz – von der Entwicklung von Zielbildern und Operating Models bis hin zu Incident Response und Business Continuity.

Aktuelle thematische Schwerpunkte liegen in der sicheren Transformation zu cyber-physischen Ökosystemen – einschließlich deren KI-gestützter Steuerung – sowie in der Next Generation Cyber Defense.

Seit über zehn Jahren betreibt er das transatlantische Munich Cyber Security Program mit einem führenden US-College – eine Initiative, aus der auch die Gründung von COMCODE North America (New York City) hervorging.

Sein Ansatz verbindet strategische Weitsicht mit operativer Umsetzung – vom Vorstand bis an die technische Frontlinie.

Vertreter des bayerischen Cyber-Mittelstands

COMCODE steht für den agilen, innovationsgetriebenen Mittelstand. Diese Perspektive möchte ich stärker im Vorstand verankern und als „Speedboat“ Impulse in einem Umfeld großer Cybersecurity-Tanker setzen.

Expertise für Zukunftsthemen

Cyber-physische Ökosysteme, KI-gestützte Steuerung und NextGen Cyber Defense sind Schlüsselthemen der kommenden Jahre – hier kann ich substanzielle Beiträge leisten.

Internationale Erfahrung & starke Netzwerke

Zehn Jahre Munich Cyber Security Program sowie enge Kontakte in die USA und darüber in die israelische Startup-Landschaft ermöglichen wertvolle Impulse und öffnen neue Kooperationsmöglichkeiten für das Netzwerk.

Nils Gerhardt

Chief Technology Officer, Utimaco

Advisory Board Member, ISITS AG

With more than 20 years of experience in cybersecurity, I have worked across many of the technologies shaping today's digital landscape. As Chief Technology Officer at Utimaco, I focus on building solutions that protect critical data, systems, and services worldwide. I also serve on the advisory board of ISITS AG, supporting advanced education for future IT security professionals.

Prior to joining Utimaco, I held senior leadership roles at Giesecke+Devrient in Germany, Canada, and the United States. I have been active at the board level in several industry organizations, including the IoT M2M Council and the Smart Payment Association. A particularly meaningful role was serving as Chairman of the Board at GlobalPlatform, where I helped bring together more than 100 global companies to define standards for secure digital services and devices.

I am putting forward my candidacy for the board of the Security Network Munich because I value bringing people together to collaborate on cyber security and digital trust. I hope to contribute my experience to advance key topics such as Sovereign and National Secure Cloud, Post-Quantum Cryptography and its first large-scale deployments, and AI security - from infrastructure to models and data.

Dr. Falk Herrmann

CTO, Funkwerk AG

Ich kandidiere erneut für den Vorstand des Sicherheitsnetzwerk München, um den Austausch zwischen Industrie, Forschung und Behörden weiter zu stärken. Als CTO eines mittelständischen Konzerns liegt mein besonderer Fokus dabei auf praxisorientierter Cybersicherheit sowie auf der Verbindung von physischer Sicherheit mit IT-Sicherheit.

Werdegang

B.Sc. in Engineering (Glasgow University, 1994)
Dr.-Ing. Mikrosystemtechnik (TU Braunschweig, 1999)

1999 – 2018

Verschiedene Management-Funktionen im Bosch-Konzern (Sicherheitssysteme, Elektrowerkzeuge, Forschung) in Deutschland, USA und China

2019 – 2022

Geschäftsführer
Rohde & Schwarz Cybersecurity GmbH

Seit 2023

Vorstand der Funkwerk AG
CTO, GB Security Solutions, Querschnittsbereich IT

Sicherheitsnetzwerk München e.V.: Gründungsvorstand, seit 2019 Schatzmeister

Dr. Wieland Holfelder

Vice President Engineering & Lead of Google Engineering Center, Google

Dr. Wieland Holfelder is Vice President Engineering and leads the Google Engineering Center in Munich, also home to the Google Safety Engineering Center. He also leads the engineering activities around Digital Sovereignty for Google in Europe. Prior to Google, Dr. Holfelder worked in Silicon Valley for more than 12 years, among others as Vice President and Chief Technology Officer of Mercedes-Benz Research and Technology North America, Inc. As part of his Ph.D. research, he worked at IBM's European Networking Center in Heidelberg, Germany, the International Computer Science Institute in Berkeley, CA, and the University of Mannheim. He holds a master's in computer science and economics and a doctorate in computer science from the University of Mannheim, Germany. In 2020 Dr. Holfelder was recognized as a "GI Fellow" by the German Computer Science association (gi.de). Among others, Dr. Holfelder is a member of the senate of en.acatech.de, a member of the supervisory board of dfki.de/en, a member of baiosphere.org/en/ai-council, a member of the supervisory board of mri.tum.de, a member of the Board of Trustees of deutsches-museum.de, a member of the Board of Directors of muenchner-kreis.de/en, a member of the advisory board of mdsi.tum.de/en, and a member of the advisory board of bidt.digital/en.

I have been deeply involved in Privacy and Security engineering and product development for more than 17 years at Google and have worked in Cloud Security and Sovereignty for more than 5 years now. The future of our society and our democracy depends on a cyber secure and sovereign digital world and it would be my honor to continue to drive these efforts within the Security Network Munich, a fantastic community of true experts in these fields.

Dr. Tobias Kiesling

Cybersecurity Technical Officer, Airbus Protect

Dr. Tobias Kiesling ist eine dynamische Führungspersönlichkeit, die Cyber-sicherheitsstrategien in kritischen Industriebereichen vorantreibt und sich seit Langem aktiv für das Sicherheitsnetzwerk München engagiert.

Aktuell steuert er als Cybersecurity Technical Officer bei Airbus Protect das länderübergreifende Technische Büro im Bereich Cybersecurity Consulting und trägt die fachliche Verantwortung für das gesamte Beratungsportfolio. Zuvor prägte er maßgeblich die deutsche Beratungslandschaft bei Airbus Cybersecurity.

Als Leiter des Consulting Delivery Center Germany war er für das Beratungsgeschäft zuständig und etablierte erfolgreich den Bereich OT Security von Grund auf.

Seine umfassende strategische Erfahrung sammelte er auch als Senior Programme Manager Cyber Defence bei der IABG mbH, wo er die Geschäftsentwicklung in den anspruchsvollen Segmenten Militär und Luftfahrt vorantrieb. Dr. Kiesling verfügt über fundierte Erfahrung im Innovations- und Forschungs-Management. Bei Airbus sowie der IABG koordinierte er strategische R&T- und Innovations-Programme. Er war zudem verantwortlich für das Management strategischer Partnerschaften mit Forschungsinstituten und Universitäten.

Dr. Kiesling untermauert seine Expertise durch eine herausragende akademische Laufbahn mit einer Promotion und einem Diplom von der LMU München, beides im Bereich Informatik.

Er blickt auf zwei erfolgreiche Amtsperioden in Folge als Mitglied des Vorstands des Sicherheitsnetzwerk München zurück. In der letzten Amtsperiode hatte er die Rolle des Stellvertretenden Vorsitzenden inne. Sein Fokus lag dabei stets auf der zukunftsfähigen Aufstellung des Netzwerks: Er wirkte aktiv an der Gestaltung des Strategieprozesses sowie an der Erweiterung der Geschäftsstelle mit und setzte sich damit für die Stärkung der Cybersicherheits-Community in der Region ein.

Dr. Andreas Kind

Vice-President Cybersecurity & Trust, Siemens AG

Ich leite den globalen Bereich Cybersecurity & Trust von Siemens – ein Team von 200 Forschern und Entwicklern in Nordamerika, Europa und Asien, das die sichere technologische Grundlage für die Siemens-Angebote in industrieller Automatisierung, intelligenter Energieversorgung, Gebäudetechnik und Transport – einschließlich KI- und SaaS-Lösungen – bereitstellt. Wir sichern das digitale Rückgrat des industriellen und infrastrukturellen Portfolios von Siemens und gewährleisten Vertrauen, Resilienz und Sicherheit in jedem vernetzten System.

Ich möchte in das Netzwerk die Stimme der industriellen Cybersecurity bringen. Die Themen und Prioritäten aus dem Bereich der Operationalen Technologien und Infrastrukturen sind nicht immer deckungsgleich mit den Themen und Prioritäten der IT-Industrie. Mit meinem Hintergrund als Verantwortlicher für Cybersecurity Technology in Siemens möchte ich daher dem Verein helfen, seine Aufgaben bei der Sensibilisierung, dem Kompetenzaufbau, dem verbesserten Schutz der Wirtschaft, den Behörden und der Öffentlichkeit sowie der Förderung von Innovation und Vernetzung verstärkt durchzuführen.

Gabriel von Mitschke-Collande

Mitglied der Konzerngeschäftsführung,
Group CDO von Giesecke+Devrient

Als Group Chief Digital Officer (CDO) bei Giesecke+Devrient, einem weltweit führenden Security-Tech-Unternehmen, verantworte ich die Bereiche Digitalisierung, IT, Innovation, neue Technologien sowie ESG, Informationssicherheit, Qualitätsmanagement und G+D Ventures.

Den Master in TUM-BWL (Technologie und Management) mit den Schwerpunkten Maschinenbau, Innovation und Entrepreneurship absolvierte ich an der TU München. Bevor ich schließlich zu G+D wechselte, war ich in mehreren operativen und leitenden Positionen rund um Strategie und Innovation tätig.

Echte Innovation beruht für mich auf starken Werten – deshalb sehe ich Technologie als Werkzeug, um menschliches Potenzial zu entfalten und Vertrauen in einer digitalen Welt zu stärken. Als Vertreter der sechsten G+D-Eigentümer-generation und Chief Digital Officer verbinde ich technologische Neugier mit klarer Menschenorientierung.

Mein Leitmotiv: **Be Digital. Stay Human.**

Als Chief Digital Officer von Giesecke+Devrient, einem international agierenden Security-Tech-Unternehmen, und Mitinitiator sowie Gründungsmitglied des Sicherheitsnetzwerks München beschäftige ich mich täglich mit der Frage, wie wir die Sicherheit von morgen schon heute gestalten können.

Mein beruflicher Fokus liegt auf der Verbindung von technologischer Exzellenz und ethischer Verantwortung – unter anderem in den Bereichen Cybersecurity, Künstliche Intelligenz, Ethics by Design, sowie Post-Quantum-Kryptografie.

Das Sicherheitsnetzwerk München verstehe ich als eine zentrale Plattform, auf der sich Wissenschaft, Wirtschaft und Politik in einem gemeinsamen Sicherheitsverständnis begegnen. Die dort aktiven Thought Leader können neue Perspektiven in einer Zeit setzen, in der Sicherheit wichtiger ist denn je.

Genau hier möchte ich meine Erfahrung einbringen – mit dem Ziel, Kooperationen bei Sicherheitsfragen zu stärken, Innovation zu fördern und den Werteerhalt im digitalen Zeitalter aktiv mitzugestalten.

Als Vorstand möchte ich dazu beitragen,

- *den Dialog zwischen Start-ups, Industrie und Forschung weiter zu vertiefen,*
- *ethisch fundierte Innovationen bei Künstlicher Intelligenz und Cybersecurity zu fördern,*
- *sowie strategische Impulse zu setzen, um unsere digitale Souveränität zu stärken.*

Ich bin überzeugt, dass Sicherheit im 21. Jahrhundert nicht nur eine technologische, sondern auch eine gesellschaftliche Aufgabe ist. Mit dieser Haltung möchte ich mich im Vorstand des Sicherheitsnetzwerks München einbringen – als Gestalter, der Innovation aktiv vorantreibt, und als Brückenbauer, der Kooperation über Grenzen hinweg lebt.

Ich freue mich darauf, die Zukunft der digitalen Sicherheit gemeinsam mit Ihnen zu prägen.

Dr. Christoph Peylo

Chief Cyber Security Officer (CCSO), Robert Bosch GmbH

Dr. Christoph Peylo ist Global Technology Executive mit Schwerpunkt auf Cybersecurity, Künstlicher Intelligenz und Digital Trust. Führt komplexe Organisationen, entwickelt und implementiert Strategien an der Schnittstelle von Technologie, Governance und Geschäftstransformation, mit nachweisbarem Impact auf Sicherheit, Innovation und Wertschöpfung.

Cybersecurity ist für mich nicht nur eine technische, sondern eine gesellschaftliche Aufgabe. Im Sicherheitsnetzwerk München sehe ich die Chance, Wirtschaft, Forschung und öffentliche Akteure enger zusammenzubringen, um gemeinsam Vertrauen und Resilienz in der digitalen Welt zu stärken. Mit meiner Erfahrung in der globalen Cybersecurity- und KI-Governance möchte ich Impulse geben, wie wir Innovation fördern und zugleich Schutz und Verantwortung verankern können.

Alexander Schellong

Managing Director Cybersecurity (GL) und Mitglied des Vorstands, Schwarz Digits

Als Mitglied im Board der Schwarz Digits und u.a. Leiter des Instituts für Cybersicherheit und Digitale Souveränität bringe ich über 15 Jahre Erfahrung in der Cybersicherheit oder Digitalen Transformation im öffentlichen und privaten Sektor im In- und Ausland mit. Durch meine Mitarbeit im Vorstand von 2021-2023 sowie langjähriger inhaltlicher Unterstützung der MCSC, bin ich mit der Arbeit des SNM vertraut. Ich stehe für Kontinuität und eine zukunftsorientierte Stärkung des Sicherheitsnetzwerk München.

Dr. Alexander Schellong ist Managing Director (GL) und Mitglied des Vorstands bei Schwarz Digits. Er leitet unter anderem das Institut für Cybersicherheit & Digitale Souveränität. Alexander Schellong verfügt über umfassende Erfahrung in der Leitung von Geschäftsbereichen und im Management von weltweiten Aktivitäten für das U.S. Department of State, deutsche Behörden, die Europäische Kommission, die NATO und Unternehmen. Im Jahr 2019 gründete Alexander die gemeinnützige Initiative CYBERWOMEN, um das Wachstum weiblicher Expertinnen für Informationssicherheit zu unterstützen. Er ist Autor eines Buches über CRM im öffentlichen Sektor sowie über 60 Publikationen zu Technologie, Gesellschaft und digitaler Transformation. Er studierte und lehrte an der Goethe-Universität Frankfurt am Main, der Harvard Kennedy School, der Universität Tokio, dem Tec de Monterrey, der Brandt School of Public Policy, der Zeppelin Universität, der Salzburg Management Business School und der Stanford University.

Prof. Dr.-Ing. Thomas Schreck

Professor für IT-Sicherheit und Chief Information Officer (CIO), Hochschule München

Dr.-Ing. Thomas Schreck ist seit 2019 Professor für IT-Sicherheit und Chief Information Officer (CIO) an der Hochschule München. Zuvor war er von 2007 bis 2019 Principal Security Engineer bei Siemens und leitete das Siemens CERT. Von 2015 bis 2021 war er Mitglied im Board of Directors von FIRST.org, wo er von 2017 bis 2019 als Vorsitzender fungierte.

Dr.-Ing. Schreck studierte Informatik an der Hochschule für angewandte Wissenschaften Landshut. Seinen Dr.-Ing. in Informatik erwarb er an der Friedrich-Alexander-Universität Erlangen-Nürnberg mit dem Schwerpunkt IT-Sicherheit.

Mit meiner langjährigen Erfahrung in der IT-Sicherheit – sowohl in der Industrie bei Siemens als auch in der akademischen Lehre und Forschung an der Hochschule München – bringe ich fundiertes Fachwissen und praktische Expertise mit, um die Arbeit des Security Network Munich voranzutreiben. Als ehemaliger Vorsitzender von FIRST.org habe ich nachgewiesen, dass ich in der Lage bin, internationale Netzwerke und Organisationen strategisch zu leiten und dabei unterschiedliche Stakeholder zu vereinen. In meiner Rolle als CIO der Hochschule München sammle ich täglich Management- und Führungserfahrung, die es mir ermöglicht, die Vorstandsarbeit effizient zu gestalten und das Security Network Munich strategisch weiterzuentwickeln.

Philipp P. Spangenberg

Director Product Development Management Suite, baramundi software GmbH

Tech-Founder, führender Digital Security Berater, agiler Produktentwicklungsleiter: Philipp Spangenberg gründete und führte im Laufe seiner Karriere verschiedene innovative Software-Unternehmen.

2000 die PPS-Systems GmbH, Spezialist auf mobile Sicherheitslösungen und 2006 die BlueID GmbH in München, ein Scale-Up für Cloud-basierte Zutrittskontrolle.

Seit 2023 leitet er als Director Product Development Management Suite die Produktentwicklung und das Produktmanagement des Kernprodukts Management Suite bei baramundi. Philipp ist zudem Mitglied des Vorstands des Sicherheitsnetzwerks München e. V. und berufen in das Expertengremium »IT-Sicherheit« der bayerischen Staatsregierung.