SEKOP2022

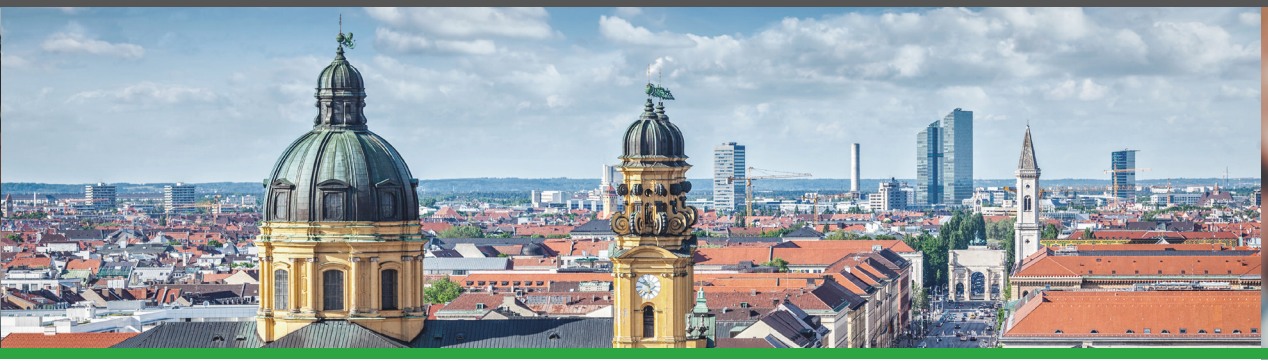
SEKOP2022
4. Cyber Security-Managementdialog
Herausforderungen | Impulse | Trends

23.- 26. Juni 2022
Hotel Andaz München Schwabinger Tor

Die CISO Agenda 2023 – Fokussieren wir uns auf die wesentlichen Themen?

LEADERS NETWORK
WE CONNECT **IT**

FINAKI



Veranstalter

FINAKI Deutschland GmbH
Inselkammerstraße 10
D-82008 Unterhaching

Tel.: +49 89 898 27 97 0
Fax: +49 89 898 27 97 9
E-Mail: info@finaki.de
Web: www.finaki.de

Alfred Luttmann
Geschäftsführer

Inhaltsverzeichnis

Grußwort der Präsidenten

COVID-19 war und bleibt das bestimmende Thema unserer aktuellen Zeit und wirkt sich weiterhin massiv auf alle Lebensbereiche aus. In der Bewältigung der Pandemie wurden uns zahlreiche Hürden, wie mangelnde Transparenz, starre Prozesse oder die stockende Digitalisierung, in den Weg gestellt. Gleichzeitig haben jedoch die Menschen, Unternehmen und Organisationen bewiesen, dass sie über eine hohe Agilität und Anpassungsfähigkeit verfügen. Veränderungen wurden schneller geplant, umgesetzt und akzeptiert als je zuvor. Eine der größten Veränderungen war dabei sicherlich die zunehmende Bedeutung des Megatrends Digitalisierung und die damit verbundene Transformation unserer Gesellschaft in nahezu allen Bereichen.

Mit mehr als 50 Milliarden internetfähigen Geräten weltweit besitzt mittlerweile fast jeder Erdbewohner durchschnittlich sieben in der Anzahl im eigenen Umfeld. Sehen Sie sich einmal in Ihrem eigenen persönlichen Bereich um. In Zeiten, in denen Home-Office zur Norm wird, finden Sie nicht nur Ihr mobiles Telefon neben dem Laptop, sondern erleichtern sich das tägliche Arbeiten mit digitalen Hilfsmitteln, wie Freisprecheinrichtungen oder anderen sogenannten Smart Devices. Dabei wird häufig vergessen, dass jedes einzelne Gerät eine Angriffsfläche für Cyberkriminelle bietet, um die Verfügbarkeit, Integrität oder Vertraulichkeit unserer persönlichen oder geschäftlichen Daten zu verletzen.

Neben dieser steigenden Abhängigkeit sollten wir auch die andere Seite nicht vergessen: die der Angreifer. Neben staatlichen Aktivitäten und den Versuchen von Script-Kiddies ist ein hoch professioneller, hoch automatisierter und äußerst lukrativer Markt entstanden. Hier werden Angriffe vorbereitet, Informationen offen getauscht, eine Arbeitsteilung und Zusammenarbeit über Länder hinweg sehr dynamisch entwickelt, ohne dabei – wie wir – auf rechtliche Rahmen wie Datenschutz oder ethische Themen der Verwendung von AI Rücksicht nehmen zu müssen. Also nicht nur die Anzahl und die Abhängigkeit steigt weiter, auch die Bedrohung.

Fast täglich werden neue Sicherheitsvorfälle bekannt, die durch eine steigende Anzahl und immer besser und kreativer werdende Angreifer verursacht werden. Um nur ein Beispiel zu nennen: Denken Sie an die erst kürzlich, auch in den Medien thematisierte, Smishing-Welle, in der Cyberkriminelle versucht haben, nicht nur Privatpersonen, sondern gezielt auch Mitarbeiter von Unternehmen und Organisationen mit einer SMS in die Falle zu locken. Der daraus resultierende Schaden ist für Personen, Wirtschaft, Politik oder Lehre meist immens. Es ist offensichtlich: **Ohne Cyber Security ist keine erfolgreiche Digitalisierung möglich.**

Jeder noch so kleine Vorfall in der Vergangenheit hat uns gezeigt, dass die bestehenden Strategien für Cybersicherheit stetig weiterentwickelt oder ausgebaut werden müssen. Der Bedarf neuer Lösungen zur Bewältigung dieser Herausforderungen ist unumstritten und das Angebot auf dem Markt für neue Lösungsansätze vielfältig. Neueste Technologien werden als Heilsbringer angepriesen, wie z. B. Cloud, Machine Learning/Artificial Intelligence, Blockchain, Robots – doch was davon hilft effektiv und effizient gegen die „Bedrohung im Netz“ und was ist nur „gutes Marketing“?

Auf der SEKOP2022 möchten wir uns dieser Frage widmen und gemeinsam mit Ihnen die CISO Agenda 2023 entwickeln. Dabei stellen wir allem voran, wie wir die wesentlichen Themen zur Erhöhung der Cyber Resilience angehen können. Das Programmkomitee hat hierfür insgesamt sechs spannende Workshops entwickelt:

- Cybersecurity-Strategie
- Third-Party Risk Management
- IT & OT Verschmelzung
- Security-Dashboard
- Open Source Software Management für eigene Software und Produkte
- Security in Cloud & Container-Umgebungen

Nutzen Sie die Chance, auf der SEKOP2022 durch Vorträge, Workshops, aber vor allem auch den Austausch mit anderen Teilnehmern aus Politik, Industrie und Lehre neue Impulse zu erhalten, die Ihnen dabei helfen können, Ihre Cyber Security-Strategie weiterzuentwickeln und zu optimieren.

Wir freuen uns auf den Austausch und auf drei spannende, gemeinsame Tage mit Ihnen in München.

Ihr

Daniel Eitler
Global CISO
Daimler AG

Ihr

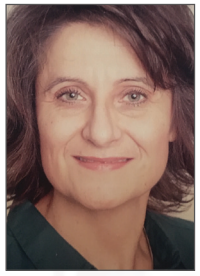
Jimmy Heschl
Head of Digital Security
Red Bull GmbH

Programmkomitee

Sergej Epp
Chief Security Officer, Central Europe
Palo Alto Networks GmbH

Peter Gerdenitsch
Head of Group Information & Cyber Security/Group CISO
Raiffeisenbank International AG

Tilo Heintzig
Head of Security Consulting GRC & Strategie
Deutsche Telekom Security GmbH



Kerstin Luck
Information Security Officer
E.ON Digital Technology GmbH

Dr. Henning Rudolf
Head of Global Cybersecurity Strategy & Business Enablement
Siemens AG

Michael Schrank
CISO
adidas AG

Thomas Tschersich
Chief Security Officer
Deutsche Telekom AG

Redner

Carsten Meywirth
Abteilungsleiter
Cybercrime (CC)

Bundeskriminalamt

Closed Door CISO Brunch

Jana Ringwald
Oberstaatsanwältin
Zentralstelle zur
Bekämpfung der
Internetkriminalität
(ZIT)

Generalstaatsanwalt-
schaft Frankfurt a. M.

Closed Door CISO Brunch

Matthias Gohl
Global Head ZEISS
Digital Partners

ZEISS

Impulsvortrag

Tobias Schrödel
IT-Sicherheitsexperte im TV
und erster Comedyhacker™

Abschlussvortrag

Format

Um gemeinsam Ideen zu entwickeln, voneinander zu lernen und neue Lösungsansätze für mehr IT-Sicherheit zu erarbeiten, bietet die **SEKOP2022 im bewährten FINAKI-Format** eine in Deutschland einzigartige Plattform. CIOs, CISOs, CSOs sowie weitere IT-Sicherheitsverantwortliche namhafter Anwenderunternehmen aller Branchen treffen das Management führender Anbieter von IT-Sicherheitslösungen zum fachlich strategischen Diskurs. Ein Programmkomitee aus Vertretern der Anwenderunternehmen definiert das Programm sowie das Leitthema der Konferenz. Unter dem Motto „**Die CISO Agenda 2023 – Fokussieren wir uns auf die wesentlichen Themen?**“ werden in sechs Workshops aktuelle Themen und Problemstellungen diskutiert, Lösungsansätze erarbeitet und Best Practices abgeleitet. Die Workshoparbeit wird durch Impulse in Form von Vorträgen, Paneldiskussionen und Use Cases im Plenum ergänzt und mit einem abwechslungsreichen Rahmenprogramm, das genügend Raum für einen vertrauensvollen Austausch auch über die Workshops hinaus gewährleistet, abgerundet.

Workshop-Teilnahme und -Organisation: Die Workshops laufen zeitlich parallel, d.h. es ist jeweils die Teilnahme an einem Workshop möglich. Die Abstracts dienen als Basis für die Workshop-Arbeit. Moderatoren und Teilnehmer entscheiden gemeinsam, welche Schwerpunkte sie in ihrem Workshop bearbeiten. Die Ergebnisse aller Workshops werden im Plenum vorgestellt und im Rahmen der Arena-Diskussion und InfoFair erörtert. FINAKI fasst diese Ergebnisse in der Ergebnisdokumentation zusammen.

Rahmenprogramm: Am Donnerstag, den 23. Juni und am Freitag, den 24. Juni (Workshop-Arbeit für die Teilnehmer) werden für die Begleitpersonen verschiedene Ausflüge angeboten. Am Samstag, den 25. Juni können alle Teilnehmer halbtägige Aktivitäten wahrnehmen, die kulturelle Exkursionen und sportliche Aktivangebote beinhalten. Die Teilnehmer werden etwa acht Wochen vor der SEKOP2022 über das gesamte Programmangebot informiert.

Konferenzablauf

Donnerstag, 23. Juni 2022

09:30 – 13:00 Uhr	Registrierung
10:30 – 12:30 Uhr	Closed Door CISO Brunch Impulsvorträge und Diskussion *(nur für Anwender)*
12:00 – 13:30 Uhr	Mittagessen
13:30 Uhr	Begrüßung durch Alfred Luttmann, Geschäftsführer der FINAKI Deutschland GmbH Eröffnung der Konferenz durch die Präsidenten Daniel Eiter, Global CISO der Daimler AG, und Jimmy Heschl, Head of Digital Security der Red Bull GmbH Impulsvortrag und Paneldiskussion „Cyber Security ohne Business oder doch Business mit Cyber Security – Dilemma oder Synergie?“
anschließend	Anmoderation der Workshops durch die Workshopleiter, gegenseitige Vorstellung der Teilnehmer und Definition des Ablaufs und der Vorgehensweise
20:00 Uhr	Abendessen

(nachmittags paralleles Rahmenprogramm für Begleitpersonen)

Freitag, 24. Juni 2022

08:30 – 11:30 Uhr	Workshop-Arbeit inkl. Kaffeepause
11:30 – 12:30 Uhr	Anwender-Use Cases
12:30 – 13:30 Uhr	Mittagessen
13:30 – 14:30 Uhr	Anwender-Use Cases
14:30 – 18:30 Uhr	Workshop-Arbeit inkl. Kaffeepause
20:00 Uhr	Abendessen

(tagsüber paralleles Rahmenprogramm für Begleitpersonen)

Samstag, 25. Juni 2022

vormittags	Rahmenprogramm: Kultur und Sport
12:30 – 13:30 Uhr	Mittagessen
13:30 – 14:15 Uhr	Präsentation der Workshop-Ergebnisse durch die Workshopleiter
14:15 – 16:55 Uhr	Arena-Diskussion und InfoFair
16:55 – 18:30 Uhr	Resümee der Konferenz durch den Präsidenten Abschluss und Bekanntgabe des Termins für die SEKOP2023 Abschlussvortrag Tobias Schrödel IT-Sicherheitsexperte im TV und erster Comedyhacker™ „Ich glaube, es h@ckt! – IT Security mal anders“
20:00 Uhr	Abendessen

Sonntag, 26. Juni 2022

vormittags	Frühstück und individuelle Gespräche
bis 12:00 Uhr	Hotel Check-out

Änderungen vorbehalten

WS 1: Cybersecurity-Strategie – Jetzt oder nie!

Workshopleitung: **Sergej Epp,** Palo Alto Networks GmbH
Co-Moderation: **Martin Schöpper,** BASF Digital Solutions GmbH

Was lernen wir aus der Vergangenheit und wie gelingt eine Zero-Trust-Architektur?

Als Sicherheitsverantwortliche waren wir in der Vergangenheit oft nur die Verwalter und selten die Gestalter der Geschäftsprozesse. Mit der zunehmenden Digitalisierung unserer Gesellschaft und den damit verbundenen Vertrauens- und Datenschutz-Herausforderungen steht Cybersicherheit plötzlich als ein zentraler Differenzierungsfaktor für viele Geschäftsmodelle der Zukunft da. CISOs stehen damit im Mittelpunkt, nicht nur die Bedrohungen von morgen zu antizipieren, sondern das Thema Cybersicherheit proaktiv am Geschäftserfolg von morgen auszurichten.

In der Gestaltung der Cybersecurity-Strategie sorgt aktuell kein anderes Schlagwort für mehr Gesprächsstoff als Zero-Trust. Anfangs eine kühne Vision, danach ein Marketing-Buzzword bis hin zu der ultimativen Cybersecurity-Strategie – all das assoziiert man damit. Die Gründe liegen auf der Hand: In der modernen Post-COVID-Welt, in der das klassische Rechenzentrum nicht mehr im Zentrum des Universums steht, der Perimeter sich aufgelöst hat und die Applikationen in der Multi-Cloud neu gedacht werden, in der Ransomware und Supply-Chain-Gefahren plötzlich nicht mehr greifbar sind, bietet Zero-Trust einen einzigartigen Ansatz, wie Cybersecurity gedacht und gestaltet werden kann. Jedoch fehlt es oft an praktischen Erfahrungen, wie die Transformation tatsächlich gelingt und viele Unternehmen stehen noch am Anfang.

Ziel unseres Workshops ist die Erarbeitung eines Referenzmodells auf Basis von Zero-Trust, welches aktiv zum Geschäftserfolg einer Organisation beitragen kann.

Die Teilnehmer des Workshops können Cybersecurity-Strategie auf Basis von Zero-Trust besser einschätzen und Anregungen mitnehmen, wie die Strategie in ihrer Organisation verankert werden kann.

WS 2: Third-Party Risk Management

Workshopleitung: **Peter Gerdenitsch,** Raiffeisenbank International AG
Co-Moderation: **Alexander Mitter,** Nimbusec GmbH

Wie stellen wir das notwendige Sicherheitsniveau unserer Zulieferer sicher?

„Schaden in Millionenhöhe – Hacker verschaffte sich Zugang über Lieferanten“ – so oder so ähnlich könnte eine Schlagzeile auf dem Ticker großer News-Webseiten lauten, wenn das Third-Party Risk nicht unter Kontrolle ist.
Unsere Unternehmen verlassen sich immer mehr auf ihre Zulieferer – speziell in der IT. Den Sicherheitsrisiken der Zulieferer und Partner wird jedoch im Einkauf nicht die notwendige Aufmerksamkeit geschenkt, da die Sicherheit der eigenen Systeme im Vordergrund steht. Das Risiko geht meist über die Third-Parties hinaus und erstreckt sich teilweise vier, fünf Ebenen tief in die Zulieferkette. Zusätzlich zu GDPR und NIS 2.0 greift auch die Regulatorik verschiedener Branchen das Thema verstärkt auf (z.B. Finanz/DORA).

Durch das Thema Third-Party Risk wird der Alltag einer CISO Organisation daher um Aufgaben wie

- eine laufende Einschätzung der Third-Party Risiken,
- eine Sensibilisierung der Fachbereiche – insbesondere des Einkaufs,
- die Überprüfung des Sicherheitslevels der Zulieferer und auch
- das Management des erwarteten Sicherheitslevels jedes einzelnen Zulieferers

erweitert.

Ergänzend kommen in regulierten Branchen Vorgaben der Aufsicht hinzu, welche ein nachvollziehbares Management des Third-Party Risikos erfordern.

In unserem Workshop wollen wir die Risiken, welche durch die Kontrahierung von Third-Parties eingegangen werden,

- priorisieren,
- geeignete Maßnahmen zur Adressierung und Minimierung bzw. Beseitigung der Risiken erarbeiten,
- einen beispielhaften Prozess für Third-Party Risk Management definieren und
- Praxiserfahrungen teilen – insbesondere mögliche Anpassungen und Formulierungen in Lieferantenverträgen.

Die Diversität der Branchen der Teilnehmer wird für viele unterschiedliche Blickwinkel sorgen. Als Anschauungsbeispiel stellen die zwei Moderatoren ihre Erfahrungen als CISO und als Co-Entwickler eines national anerkannten Cyber Risk Ratings dar.

WS 3: IT & OT – Cyber Security, wenn Silos verschmelzen

Workshopleitung: **Kerstin Luck,** E.ON Digital Technology GmbH
Co-Moderation: **Dr. Sebastian Schmerl**, Arctic Wolf Networks

Eine Verschmelzung, die Chancen und Risiken für die Informationssicherheit in sich trägt.

IT und OT waren in der Vergangenheit getrennte Bereiche. In der Ära von IoT, Big Data und Fernwartung löst sich diese Trennlinie immer weiter auf. Zusätzlich wirkt der Umstand der Pandemie als Katalysator hinsichtlich der Fernwartungs- und der „kontaktfreien" Zugänge (Home-Office etc.) auf die Aufweichung der Trennung ein.

OT war bislang auf Produktions- und Industrieanlagen konzentriert, die in der Regel in geschlossenen Bereichen platziert waren. Dazu zählen unter anderem industrielle Kontrollsysteme (ICS) wie Prozessleitsysteme, SCADA-Systeme sowie industrielle Geräte, die inzwischen nicht nur untereinander, sondern zusätzlich mit dem Internet vernetzt sind. Die IT befasst sich klassischerweise mit Hardware, Software, Kommunikationstechnologien und den damit verbundenen Services. Somit ist auch die Ausrichtung der Informationssicherheit unterschiedlich. Für die OT lag der Fokus auf der Verfügbarkeit und für die IT darauf, die Datensicherheit zu gewährleisten.

Produktions- und Anlagennetzwerke sind zu attraktiven Zielen für Cyberattacken geworden und somit erleben OT-Systeme Cyber-Angriffe ähnlich wie IT-Systeme. Schwachstellen und Sicherheitsprobleme bieten Hackern Möglichkeiten, Zugang zu beiden Netzwerken zu erhalten und systematisch wichtige Daten und Assets auszuforschen und lebenswichtige Prozesse zu stören. Durch die immer stärker fortschreitende Verschmelzung sehen sich nun gerade die Betreiber automatisierter Produktionsanlagen (Stichwort: IoT) und Kritischer Infrastrukturen (Stichwort: Energieversorger) der Herausforderung gegenüber, die Angriffsvektoren beider Welten zu betrachten und den verschiedensten Anforderungen wie dem IT-Sicherheitsgesetz und der Europäischen Datenschutzgrundverordnung sowie Herausforderungen wie überholten Technologien oder unsicheren Verbindungen Genüge zu tun.

Ziel des Workshops ist die gemeinsame Erarbeitung der verschiedenen An- und Herausforderungen an und durch die Cyber Security. Die Teilnehmer haben die Möglichkeit, die Chancen und Risiken aus der Konvergenz der IT- und OT-Netzwerke herauszukristallisieren und daraus eine Strategie zu entwickeln, wie die Ansichten der jeweils anderen Seite zu berücksichtigen sind und das Know-how beider Seiten gebündelt werden kann.

WS 4: Das Security-Dashboard

Workshopleitung: **Thomas Tschersich,** Deutsche Telekom AG
Tilo Heintzig, Deutsche Telekom Security GmbH
Co-Moderation: **Frank Koelmel,** Cybereason

Wie bekomme ich als Entscheider eine End-to-End-Transparenz?

Die Digitalisierung verbindet Menschen, vereinfacht und automatisiert Arbeitsprozesse und treibt den Wandel voran. Kurzum: Wir alle profitieren von der fortschreitenden Digitalisierung. Gleichzeitig wird jedoch auch alles ein Stück weit komplexer. Vor allem in der „Cyberwelt" ist es schwierig geworden den Überblick zu behalten: Das ständige Katz- und Maus-Spiel zwischen Angreifern auf der einen Seite und uns auf der anderen scheint eine *Never-Ending Story* zu sein. Eine größere Vernetzung bedeutet eben auch weitaus mehr potenzielle Schwachstellen. Und diese werden ausgenutzt – die Frage ist nur wann und in welcher Form. Wie also behält man hier als Chief Security Officer/Chief Information Security Officer noch am besten die Kontrolle – und wie macht man die Informationen Entscheidungsträgern transparent?

Ein geeignetes Mittel hierfür könnte ein *Security-Dashboard* sein: eine zentrale Übersicht der relevanten Informationen aus den einzelnen Reportings der Bereiche. Das Dashboard könnte die Darstellung der klassischen Sicherheit sowie Cybersicherheit vereinen und eine klare Priorisierung und Bewertung der Risiken ermöglichen. Als graphische Abbildung könnte das Dashboard einen Überblick aller Themen im Verantwortungsbereich des CSOs/CISOs geben. Der Vorteil wäre hierbei: Menschen können Graphiken weitaus schneller erfassen als Texte oder Excel-Tabellen. Die Hauptseite könnte beispielsweise alle aktuellen Risiken, die eine sofortige Handlung erfordern, aufzeigen. Ziel ist es, einen möglichst schnellen Überblick des Status quo zu geben. Was hat absolute Priorität, wie sieht der nächste Schritt aus? All das müsste aus einem vollständigen Dashboard hervorgehen – und zwar ohne langes Durchscrollen des E-Mail-Postfachs. Darüber hinaus sollte es bei Bedarf möglich sein, detailliertere Informationen zu erhalten.

In unserem Workshop erarbeiten wir, welche einzelnen Bestandteile für ein *Security-Dashboard* wichtig sein könnten. Beispielsweise könnten je nach Themengebiet und Sicherheitsabbildung die Graphiken die klassische Ampelbewertung bis hin zu Welt- und Wetterkarten beinhalten. Mit den gemeinsam erarbeiteten Ergebnissen können Sie anschließend Ihr eigenes Dashboard implementieren. Damit übernehmen Sie ab sofort wieder die nötige Kontrolle als Sicherheitsverantwortlicher in Ihrem Unternehmen.

WS 5: Open Source Software Management für eigene Software und Produkte

Workshopleitung: **Dr. Henning Rudolf,** Siemens AG
Marcel Kulicke, Siemens AG
Co-Moderation: **Alexios Fakos,** Synopsys GmbH

Wie meistern Sie die sich stetig ändernden regulatorischen Rahmenbedingungen und die zunehmende Anzahl von veröffentlichten Sicherheitsschwachstellen?

Die Anzahl der Schwachstellen in Softwareprodukten ist laut BSI in den letzten Jahren unverändert hoch. Auch gibt es keine Anzeichen, dass sich dies in absehbarer Zeit ändern wird. Erfolgreiche Angriffe basieren meist auf der Ausnutzung bekannter, aber nicht behobener Schwachstellen, beispielsweise durch Einsatz von nicht mehr sicherheitsaktuellen Open Source-Bibliotheken wie z.B. OpenSSL Heartbleed. Oftmals fehlen Verantwortlichkeiten und Prozesse in Unternehmen, um diesen Herausforderungen erfolgreich zu begegnen. In unserem Workshop werden Best Practices von Softwareanbietern und Anwendern dargestellt und in Kleingruppen abhängig von den speziellen Herausforderungen bearbeitet und im Plenum vorgestellt.

Gemeinsam Cyber Security entwickeln ist das Leitthema der diesjährigen SEKOP. Zusammen wollen wir erarbeiten, wie ein holistisches Open Source Software Management definiert werden kann, welche Lösungswege erfolgreich und mit einem geringen Aufwand umsetzbar sind. Viele Unternehmen stehen vor ähnlichen Herausforderungen, weil sie beispielsweise entweder selbst als Kritische Infrastruktur eingestuft sind oder Endkunden vertraglich auf die Einhaltung von Vorgaben einfordern.

Unser Workshop gibt Einblicke aus der Praxis für die Praxis und liefert einen entscheidenden Impuls für die Umsetzungen im eigenen Unternehmen. Hierbei gilt: „kapieren statt kopieren“, weil unterschiedliche Aufbau- und Ablauforganisationen in Unternehmen existieren. Die Teilnehmer erhalten einen praxisnahen Einblick, welche Herausforderungen bezüglich eines Open Source Software Managements zu meistern sind. Nach dem Workshop wissen Sie, wie andere Unternehmen dieses Thema umgesetzt und was sie dabei gelernt haben. Abschließend erhalten Sie einen Impuls, was die direkten nächsten Schritte in Ihrem Unternehmen sein könnten, wenn Sie nach der SEKOP2021 wieder Ihr Tagesgeschäft angehen. Open Source Software Management ist eine neue Herausforderung. In unserem Workshop erhalten Sie einen guten Einblick, wie andere Unternehmen dieses Thema adressieren und welche Handlungsmöglichkeiten – mit den jeweiligen Vor- und Nachteilen – existieren. Durch den Austausch mit anderen Unternehmen werden Sie von diesen lernen und wichtige Impulse für die eigene Umsetzung erhalten.

WS 6: Automatisch sicher, dank moderner Cloud & Container-Umgebungen?!

Workshopleitung: **Michael Schrank,** adidas AG
Co-Moderation: **Torsten Jüngling,** Capgemini Outsourcing Services GmbH

Security by Design effizient und skalierbar umsetzen und Altlasten beseitigen.

Kaum ein Unternehmen spricht derzeit nicht über die Cloud und moderne Container-Laufzeitumgebungen. Die einen sind bereits „in der Cloud angekommen“, andere machen gar „Cloud first“ und ein paar wenige bereiten sich noch auf den Weg in die Cloud vor. Doch das Feld, von dem gesprochen wird, ist oft ein weites – der CISO steht vor der Aufgabe, IaaS, PaaS, SaaS, On Premise, Hybrid sowie Hyperscaler Cloud-Umgebungen abzusichern. Hinzu kommt, dass mit der Nutzung dieser Angebote oft auch gleich noch neue Technologien eingeführt werden.

In unserem Workshop beleuchten wir gemeinsam die Handlungsfelder, die sich für uns ergeben. In Bezug auf die Technologien, die oft im Zusammenhang mit verstärkter Cloud-Nutzung in Erscheinung treten, fokussieren wir uns vor allem auf Container-Umgebungen.

Auf Basis eines kurzen Impulsvortrags werden in unserem Workshop in kleineren Gruppen die verschiedenen Cloud-Arten sowie deren spezifische Security-Herausforderungen erarbeitet. Die Gruppenergebnisse werden anschließend in der gesamten Workshopgruppe vorgestellt und diskutiert. Zum Abschluss werden die gesammelten Ideen und Vorschläge zu einem Gesamtergebnis zusammengefügt.

Unser Workshop dient dazu den CISOs die Herausforderungen, aber vor allem auch die Chancen, die mit dem Trend Cloud verbunden sind, aufzuzeigen. Denn eine gezielte Verlagerung von Services in die Cloud und Modernisierung hin zu Container-Umgebungen, flankiert durch die richtigen Sicherheitskonzepte, bietet die einmalige Chance die Unternehmens-IT auf eine neue, moderne und vor allem sichere Basis zu heben.
Zudem erlauben diese neuen Ansätze Security by Design einzuführen und konsequent anzuwenden.

Die Teilnehmer des Workshops haben nach diesem ein klares Bild, welche Chancen und Risiken sich durch die Verlagerung in die Cloud ergeben. Sie haben zudem durch die Eindrücke der Diskussionen, gesammelten Informationen und Empfehlungen einen besseren Startpunkt, um die bevorstehenden Herausforderungen zu meistern.

Vier gute Gründe, warum Sie bei der SEKOP2022 dabei sein sollten:

Aus der Praxis. Für die Praxis.

Schwerpunkt der SEKOP sind sechs parallel stattfindende, von Plenarvorträgen begleitete, Workshops zu topaktuellen IT Security-Themen. Die Workshops sind mit Vertretern der Anwender- und Anbieterunternehmen besetzt und werden professionell moderiert. Im Rahmen der Ergebnispräsentation und der Arena-Diskussion sowie auf der abschließenden InfoFair haben Sie Gelegenheit, die Ergebnisse aller Workshops detailliert zu begutachten.

Einsichten. Aussichten. Ansichten.

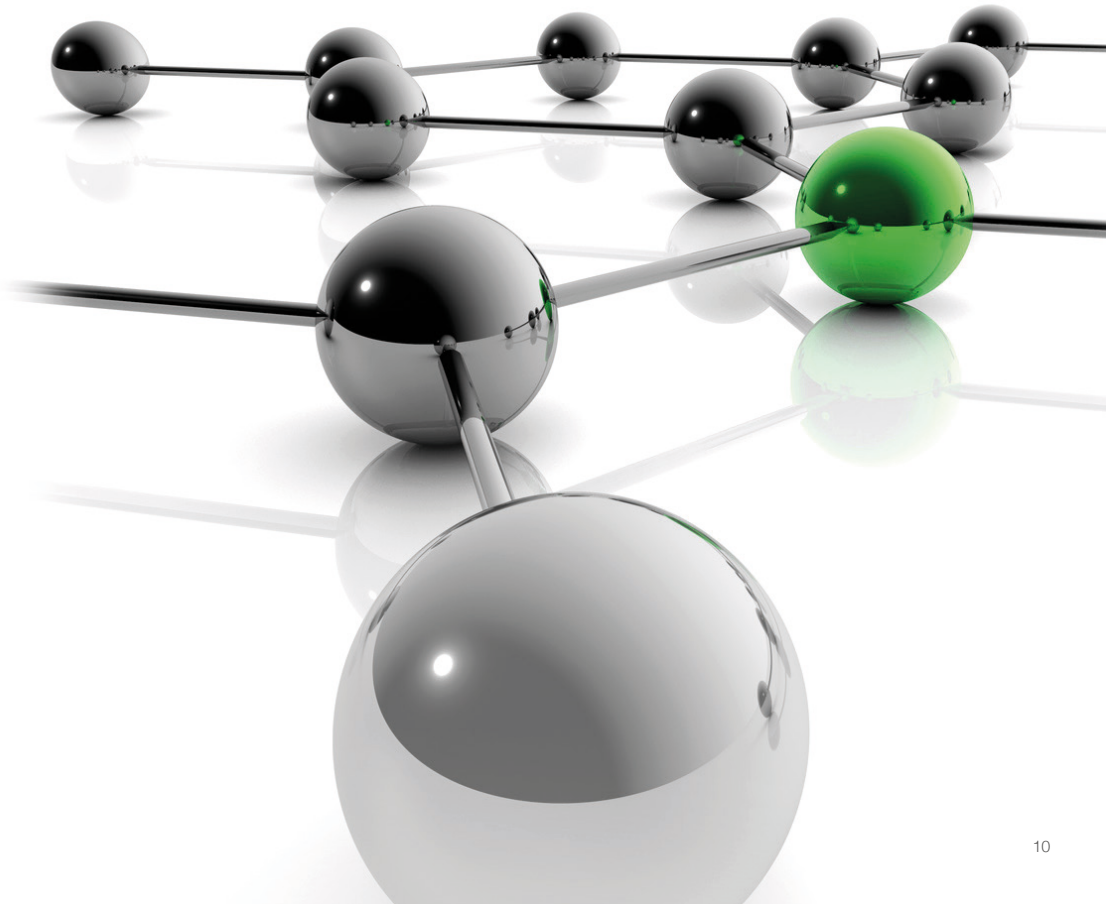
Ziel der SEKOP ist es, Impulse, Anregungen und Weichenstellungen für die IT von heute und morgen zu erarbeiten. Gemeinsam beleuchten wir Zukunftsszenarien unter technischen und wirtschaftlichen Aspekten, um Positionen zu bestimmen, Chancen und Risiken abzuwägen, Eckwerte für Entscheidungen zu konkretisieren sowie neue kreative und effektive Wege für eine moderne Infrastruktur und eine gesicherte Kommunikation im Unternehmen zu erörtern.

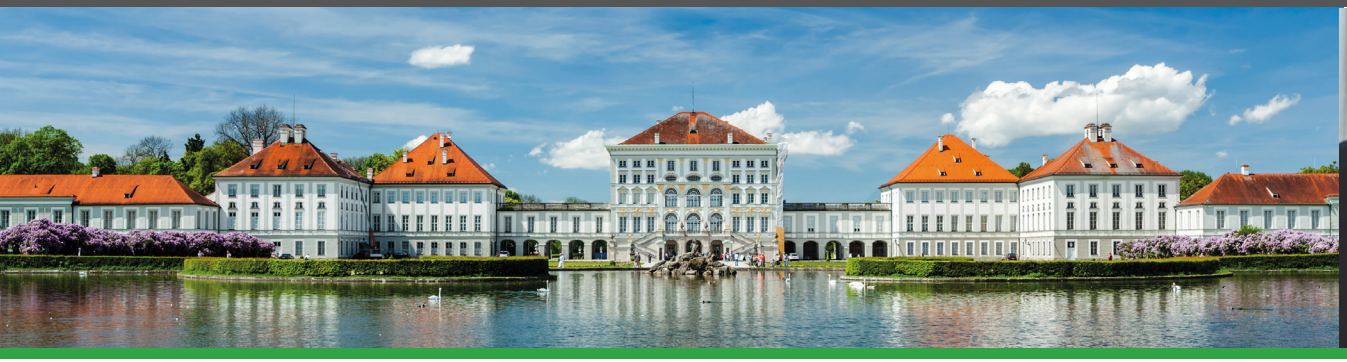
Kompetenzen bündeln. Synergien nutzen.

Seit 1997 vernetzen wir die IT-Entscheider der großen Anbieter- und Anwender-unternehmen. Hierzu wurde eine einzigartige Struktur von Top Level-Managementdialogen im In- und Ausland entwickelt. Als branchenneutrale Plattform für einen strategischen fachlichen Diskurs bringen wir seit Jahren erfolgreich Anwenderunternehmen der ITK-Branche mit den Experten der Anbieter- und Dienstleistungsunternehmen zusammen.

Kontakte. Kommunikation. Kooperation.

Die SEKOP lebt von ihren und für ihre Teilnehmer. Vor Ort haben Sie ausreichend Gelegenheit, sich mit Ihren Branchen- und Fachkollegen auszutauschen, Gleichgesinnte kennenzulernen sowie Ihr professionelles Netzwerk auszubauen.





Konferenzteilnahme

Konferenzgebühren

Anwenderunternehmen (pro Person)	
Anmeldung bis 22.04.2022	€ 1.990,- zzgl. MwSt.
Anmeldung ab 23.04.2022	€ 2.390,- zzgl. MwSt.
Anbieterunternehmen (pro Person)	
Standard-Ticket	€ 9.790,- zzgl. MwSt.
mit Co-Moderation	€ 14.990,- zzgl. MwSt.
mit Use Case	€ 14.990,- zzgl. MwSt.

Für Paketpreise (Anmeldung für mehrere Veranstaltungen) kommen Sie bitte direkt auf Sebastian Stürzl, Sales Director zu. E-Mail: sebastian.stuerzl@finaki.de, Tel.: +49 89 898279728

Eingeschlossene Leistungen

Die Konferenzgebühren beinhalten die Kosten für Logis und Bewirtung während der Konferenz. Ebenfalls eingeschlossen sind pro Teilnehmer die Kosten für eine private Begleitperson und alle angebotenen Rahmenprogramme. In Abstimmung mit dem Veranstalter können maximal zwei Personen pro Unternehmen, mit je einer privaten Begleitperson, teilnehmen. Die Konferenzgebühr wird von der FINAKI Deutschland GmbH in Rechnung gestellt, eine Teilnahme ist erst nach Eingang des Rechnungsbetrages möglich. Änderungen und Stornierungen der Anmeldung müssen schriftlich erfolgen und sind empfangsbedürftig.

Compliance

In vielen Unternehmen bestehen Compliance-Systeme. Auch FINAKI nimmt Compliance als wichtige Aufgabe ernst und verpflichtet sich zu verantwortungsvollem Handeln. Die IT-Managementkongresse von FINAKI wurden von unserer Seite hinsichtlich bestehender Compliance-Anforderungen geprüft. Sollten Sie zum Zwecke der Übereinstimmung mit den Compliance-Richtlinien Ihres Unternehmens eine separate Rechnung für die Begleitperson benötigen, so bitten wir Sie dies bei der Anmeldung zu vermerken.

Stornobedingungen

keine Stornierungskosten	bis 22.04.2022
50% der Konferenzgebühr	bei Absage ab 23.04.2022
100% der Konferenzgebühr	bei Absage ab 20.05.2022

Sollte die SEKOP2022 aufgrund behördlicher Verfügungen im Kontext der COVID-19-Pandemie nicht stattfinden können, räumen wir unseren Teilnehmern das Recht ein, von ihrer Konferenzteilnahme zurückzutreten.

Anreise/Abreise

Die Reisekosten werden von den Teilnehmern selbst getragen. Für einen kostenlosen Transfer am Anreisetag (23. Juni 2022) vor Konferenzbeginn vom Flughafen München zum Konferenzhotel und am Rückreisetag (26. Juni 2022) vom Konferenzhotel zum Flughafen München ist gesorgt.

Veranstaltungsort

Hotel Andaz München Schwabinger Tor
Leopoldstrasse 170
80804 München

Zur Verlängerung Ihres Aufenthalts kontaktieren Sie bitte das Konferenzhotel mit Hinweis auf Ihre SEKOP2022-Teilnahme:

Tel.: +49 89 262027 1234
E-Mail: munich@andaz.com

Rahmenbedingungen

Tagungsinhalte und Programmkomitee – Die Vertreter der Anwenderunternehmen definieren das Programm mit dem Motto und den Workshop-Inhalten. Sie bilden das Programmkomitee. Die Mitglieder des Komitees repräsentieren einen Querschnitt durch alle Branchen.

Präsident – Aus dem Programmkomitee rekrutiert sich der Vorsitzende, der in seiner Eigenschaft als Präsident die Tagung eröffnet und schließt.

Teilnehmer – Die IT-Verantwortlichen der Anwenderunternehmen treffen die Mitglieder des Managements und Technologieexperten der Anbieterunternehmen. Die Teilnahme setzt die Bereitschaft zur aktiven Mitarbeit in den Workshops voraus.

Teilnehmerbeschränkung – Die Zahl der Konferenzteilnehmer ist auf 130 Personen beschränkt. Diese Beschränkung gewährleistet Transparenz und effektives Arbeiten in den Workshops. Pro Unternehmen können maximal zwei Teilnehmer angemeldet werden. Bei größeren Organisationen gilt diese Begrenzung für einen Geschäftsbereich. Des Weiteren ist die Teilnahme pro Anwenderunternehmen auf zwei Personen, bei Anbieterunternehmen auf einen Unternehmensvertreter eingeschränkt.

Tagungsstil – Die Tagung ist geprägt durch ihren herstellerunabhängigen und neutralen Charakter. Das ungestörte und ungezwungene Arbeitsklima auf unseren Veranstaltungen hat oberste Priorität. Hierfür ist es erforderlich, dass die Teilnehmer auf diskreten Umgang vertrauen können und ihre Daten in dem von ihnen autorisierten Rahmen verbleiben bzw. nur nach ausdrücklicher vorheriger Genehmigung durch den jeweils Betroffenen verwendet werden.

Vertriebs- und Marketingaktivitäten sind weder vor Ort noch nach den Veranstaltungen erwünscht. Insbesondere Dritten ist es untersagt, Teilnehmer unserer Veranstaltungen auf dieser Basis zu kontaktieren. Die Daten der Teilnehmer dürfen nur nach ausdrücklicher Genehmigung des jeweiligen Teilnehmers sowie des Veranstalters an Dritte weitergegeben werden. Gleiches gilt für die Inhalte der Veranstaltungen im weitesten Sinne.

Teilnehmerinformationen – In einer App wird jeder Teilnehmer mit seinem Foto, Namen, Firmenzugehörigkeit, Funktion im Unternehmen und E-Mail veröffentlicht; in einer Teilnehmerliste die Namen, Firmenzugehörigkeit und Position. Diese Details werden ausschließlich zu Informationszwecken im Zusammenhang mit den FINAKI-Veranstaltungen verwendet. Alle darüber hinausgehenden Nutzungen sind ausgeschlossen.

Ergebnisdokumentation – Jeder Teilnehmer erhält von FINAKI nach der Tagung eine Ergebnisdokumentation. Diese enthält:

- die Plenarvorträge (soweit vom Redner genehmigt)
- die Dokumentation der Workshop-Ergebnisse
- die Teilnehmerliste

Für die Erstellung der Ergebnisdokumentation werden die Ergebnisse der Workshops sowie Zusammenfassungen der Vorträge anhand von Videoaufnahmen dokumentiert. Mit der oben genannten Aufnahme und Verwendung, ausschließlich zu diesem Zweck, erklären sich die Teilnehmer einverstanden.

Wir, das gesamte Team der FINAKI Deutschland GmbH, nehmen den Schutz Ihrer persönlichen Daten sehr ernst und halten uns strikt an die Regeln der Datenschutzgesetze (insbesondere EU-DSGVO und BDSG).

FINAKI Deutschland GmbH
Inselkammerstraße 10
D-82008 Unterhaching

Tel.: +49 89 898 27 97 0
Fax: +49 89 898 27 97 9
E-Mail: info@finaki.de
Web: www.finaki.de