



01./02. Juli 2026

#Strategiegipfel Cyber Security

Cyber Security Strategie 2030
Industrielle Sicherheit | Threat Intelligence
Sichere KI-Anwendungen
Cyber Resilience Governance
Zero Trust | Digital Sovereignty
Security Awareness | Cloud Security | NIS 2.0
Messbarkeit von Securitymaßnahmen
Cyber Incident & Emergency Management

Mit spannenden Case Studies aus Unternehmen wie:



project
networks

Mit Unterstützung von:



” Wir bringen Entscheider zusammen.



01./02. Juli 2026



Hotel Palace Berlin



Networking Dinner am Abend
des ersten Veranstaltungstages

Cyber Security Leader: Strategien für die Zukunft der Cybersicherheit

Die Digitalisierung, die Vernetzung industrieller Systeme und der explosionsartige Einsatz von KI-Technologien haben die Bedrohungslandschaft in wenigen Jahren grundlegend verändert. Cyberkriminalität ist nicht mehr nur technisches Risiko, sondern ein direktes Geschäftsrisiko, das strategische Entscheidungen beeinflusst.

Als CISO oder Head of Cyber Security tragen Sie heute die Verantwortung, eine immer komplexere IT-, Cloud- und OT-Umgebung nicht nur zu schützen, sondern resilient und zukunftsfähig aufzubauen. KI-Angriffe, Ransomware-as-a-Service, geopolitische Risiken, Compliance-Anforderungen und generative Social-Engineering-Methoden verlangen neue Strategien – und neue Führung.

Genau hier setzt unser Strategiegipfel Cyber Security 2026 an.

Diese Veranstaltung richtet sich gezielt an CISOs, Head of Cyber-/OT-Security, CSOs und strategische Entscheider, die täglich den Spagat zwischen Risiko, Innovation, Compliance und Business-Anforderungen meistern müssen.

Im Fokus stehen Praxisnähe, Führungsanspruch und ein realer Mehrwert für Ihre Organisation.

Unser Ziel: Ihnen konkrete Strategien, Best Practices und praxiserprobte Methoden an die Hand zu geben, die sofort im Unternehmen Wirkung entfalten – technisch, organisatorisch und kulturell.



Zielgruppe
CIO
CISO
Head of IT Security
Leitende IT Security Manager
mit Budgetverantwortung

Vorsitz und Moderation:



Holger Berens
Vorstandsvorsitzender
Bundesverband für den Schutz Kritischer
Infrastrukturen e.V.



Prof. Dr. Tobias Eggendorfer
Professor für Cyber Security
Technische Hochschule Ingolstadt THI



ANMELDUNG

<https://www.project-networks.com/events/cyber-security/registration/>

TAG 1 | 1. Juli 2026

- 08.00 Registrierung
- 08.30 Eröffnung der Veranstaltung durch die Vorsitzenden

08.40-
09.40

Podiumsdiskussion *

Die stille Macht der Orientierungslosigkeit: Wenn Regulierung und KI das Mandat des CISOs neu schreiben

Holger Berens, Vorstandsvorsitzender, BSKI e.V.
Thomas Strieder, VP Group IT Security & Operations Services, ANDRITZ
Dr. Manfred Boudreaux-Dehmer, Former CIO, NATO
Andy Schneider, Chief Security Officer, Palo Alto Networks



BEST PRACTICE VORTRÄGE *

09.45-
10.15

STREAM 1
From hunter to hunted - Wie wir Cyberkriminellen die Grundlagen entziehen

Carsten Meywirth, Director Cybercrime, Bundeskriminalamt



STREAM 2
Von Cybercrime bis staatliche Hacker: Die aktuelle Bedrohungslage für Unternehmen

Götz Schartner, CEO, 8com



10.15 KAFFEE- & TEEPAUSE

10.35-
11.05

Analoge Bedrohungen, neue Technologien und die digitalen Antworten

Steffen Frankl, CISO, DB Regio



11.10-
11.40

STREAM 1
CISO heute: Informationssicherheit als Führungsaufgabe

Matthias Kraft, CISO, Hauck & Aufhäuser Fund Services Group



STREAM 2
Wann kann ich einem KI-System vertrauen?
 Ein Audit-Framework für Haftung, Governance und gelebte Verantwortung

Horst Moll, CISO, Miltenyi Biotec Group



Fortsetzung Tag 1



11.45-
12.45

Networking Sessions

Gespräche mit Fachkollegen und unseren Partnern



11.50-
12.40

Workshop

Die Domestizierung der Cybersicherheit durch KI
Werbeversprechen "KI" oder echter Nutzwert für alle?

Michael Schröder, Head of Product Marketing, ESET



12.45-
13.40

MITTAGSPAUSE



13.40-
14.30

Impulsvorträge und Roundtables

Roundtable 1
CISO-Evolution 2026+: Führungsverantwortung zwischen Mandat und Realität

René Koch, CISO, Emons



Roundtable 2
NIS2 & DORA in der Organisation verankern – Governance first, Tools later

Steffen Bartsch, CISO, Berenberg



Roundtable 3
Wirksame und zielgruppenorientierte Awareness in Konzernen

Ingmar Petereins, Head of Information Security / CISO,
Dussmann Group



14.35-
16.05

Networking Sessions

Fortsetzung Tag 1

BEST PRACTICE VORTRÄGE



16.10-
16.40

STREAM 1
Von Backup-Jobs zu AI-Agenten – ein praktischer Ansatz für Non-Human-Identities (NHI)

Eleni Richter, Chief Architect IDM, EnBW AG



EnBW

STREAM 2
Vom Verstehen zur Steuerung: Die CISO-Roadmap der ersten 90-180 Tage

Dennis Ritter, CISO, Geberit International AG



■ GEBERIT



16.40-
18.10

Networking Sessions



18.15-
19.15

Cyber Intelligence Tools – Hype oder Hilfe

Volker Kozok, 1. Vorsitzender, Netzwerk für Cyber Intelligence e.V.



NCI
Netzwerk für Cyber Intelligence e.V.



19.30

ABFAHRT ZUM NETWORKING DINNER



PARTNER

KnowBe4

eset
Digital Security
Progress. Protected.

wallix

VARONIS

paloalto
NETWORKS

8COM
CYBER SECURITY

opensystems | **+**

TAG 2 | 2. Juli 2026

08.30 Eröffnung des zweiten Veranstaltungstages

08.40-
09.35

Impulsvorträge und Roundtables

Roundtable 4 Zwischen Bubble und Gamechanger – Wie Cyber Security Teams sinnvoll mit KI umgehen

Daniel Sauder, Head of Offensive Security & Security Enablement, thysenkrupp



Roundtable 5 Lieferketten unter Dauerbeschuss – Shared Risk, Shared Liability

Thomas Galley, ISB, Lekkerland



Roundtable 6 Der Preis der Priorisierung: Was wir bewusst nicht absichern

Holger Berens, Vorstandsvorsitzender, BSKI e.V.



09.40-
10.40

Networking Sessions

Gespräche mit Fachkollegen und unseren Partnern

BEST PRACTICE VORTRÄGE

10.40-
11.10

STREAM 1 NIS2.0 - Der Weg vom 6. Dezember bis 30. Juni 2026 in einem Krankenhaus mit 200 Einheiten wie MVZs und andern

Jan Boykov, Gebietsleiter Informationssicherheit, Helios Kliniken



STREAM 2 Geopolitischer Rahmen und die Herausforderungen – Wie kann man mit Tools und mit Hilfe von KI Szenarien eine strategische Vorausschau bzw. das Krisenmanagement ableiten?

Dr. Konstantinos Tsetsos, Head of Foresight, Metis Institute / Bundeswehr University Munich



11.15-
12.45

Networking Sessions

Fortsetzung Tag 2

BEST PRACTICE VORTRÄGE



12.45-
13.15

STREAM 1
Krieg? Gibts nicht! Und wenn doch...? Hybride Kriegsführung und deren Folgen neu gedacht.

Nico Schönfeld, Leiter Konzernsicherheit/ CSO,
R+V Allgemeine Versicherung AG



R+V

STREAM 2
End-to-End-Sicherheit im Verbund: Cybersecurity und Resilienz zusammen denken

Tareq Ahmadi, CISO/Head of Cybersecurity & Resilience
Management, BITMARCK



BITMARCK®

13.15-
14.15

MITTAGSPAUSE



14.15-
14.45

STREAM 1
People leave bosses – or stay for culture

Marcus Beyer, Security Awareness Officer, Swisscom (Schweiz) AG



swisscom

STREAM 2
IT-Governance: Zwischen Pflicht und Überlebensnotwendigkeit

Ralf Kimpel, Director Corporate Audit, Risk & Insurance,
Hubert Burda Media Holding KG



Hubert Burda Media



14.45-
15.15

STREAM 1
Post-Quantum Security 2026+: Vom kryptografischen Risiko zur Migrations-Roadmap

Dr. Jochen Dinger, CISO, Atruvia AG



ATRUVIA

STREAM 2
Schön reden ist nicht schön machen – wenn Sicherheit nur auf dem Papier steht

Prof. Dr. Tobias Eggendorfer, Professor für Cyber Security,
TH Ingolstadt



**Technische Hochschule
Ingolstadt**



15.15-
15.45

Overarching Control Risk Assessment: Strengthening Entity Level Risk Awareness Across the Group

Yana Khrapkovskaya, Risk Manager, Munich Re



Munich RE



15.45-
16.25

Digitale Souveränität – wo stehen wir wirklich? Eine Bankenperspektive

Astrid Freier, Direktorin Informationstechnologie,
VÖB - Bundesverband Öffentlicher Banken Deutschlands



VÖB

16.25

WRAP UP