SECURITY DAY 2026

CANCOM

Schloss Schönbrunn Tagungszentrum, Apothekertrakt, 1130 Wien

	Track 1 - Raum Maria Theresia	Track 2 - Raum Sophie	Track 3 - Raum Maximilian	Track 4 - Raum Sissi
08:30 Uhr	**Registrierung und Frühstück**			
09:15 - 09:25	**Begrüßung durch Dietmar Wiesinger** *Mitglied des Vorstands | CANCOM Austria AG*			
09:25 - 10:00	**Keynote** **Dr. Erlijn van Genuchten** *International gefragte Expertin & Visionärin für Cybersecurity und Nachhaltigkeit*			
10:00 - 10:35	**CANCOM** **Aktuelle Schwachstellen & Bedrohungen** **Kevin Mühlböck** *Senior Solution Designer | CANCOM Austria*			
10:35 - 11:10	**COFFEE BREAK IN DER PARTNER AREA**			
11:10 - 11:30	**The AI Security Blind Spot: How to Safely Use and Deploy at Scale** EN AI adoption is transforming industries, yet security often lags, creating vulnerabilities across the AI lifecycle. Learn how Prisma AIRS secures AI development and protects against critical threats like prompt injection, model exfiltration, and runtime threats. We will show you how you can safely embrace AI innovation without compromising your company's data or models. **John Harrison** *Director, Security Evangelist, NetSec and Unit 42, EMEA | Palo Alto Networks*	**From Complexity to Clarity: Managing Secure Application Connectivity with AlgoSec Horizon** Hybrid infrastructures create fragmented connectivity paths and diverse security layers, making it challenging for organizations to maintain a clear view of their application flows. The AlgoSec Horizon Platform turns that complexity into clarity. By providing a unified, application-centric view across on-premises, hybrid, and cloud environments while supporting a broad range of architectures, Horizon enables customers to easily understand and manage business-aligned connectivity. **Sidney Ross** *Solution Architect | Algosec*	**Datensicherheit im Zeitalter von KI-Agenten** Mit dem Einsatz von AI Agenten und Copiloten wachsen nicht nur Produktivität und Innovation, sondern auch Risiken wie Oversharing, Datenlecks und fehlende Transparenz. In dieser Session erfahren Sie, wie Microsoft Security Lösungen helfen, AI Interaktionen und Daten wirksam zu kontrollieren, AI Risiken frühzeitig zu erkennen und den Einsatz von AI Agenten sicher, nachvollziehbar und regelkonform zu steuern. **Klaus Reiter** *Data Security Engineer | Microsoft*	**Regulatorik aus Sicht eines Dienstleisters** Regulatorische Anforderungen wie NIS2 und Dora stellen Unternehmen vor wachsende organisatorische und technische Herausforderungen. Dieser Vortrag beleuchtet Regulatorik aus der praxisnahen Perspektive eines IT Dienstleisters und zeigt, wie Vorgaben sinnvoll interpretiert, eingeordnet und in umsetzbare Maßnahmen übersetzt werden können. Dabei stehen typische Kundenfragen, pragmatische Lösungsansätze und die Rolle des Dienstleisters zwischen Compliance, Security und operativer Realität im Fokus. **Thomas Seiler** *CISO | CANCOM Austria*
11:35 - 11:55	**Cisco Hybrid Mesh - Erleben Sie neue Möglichkeiten mit einer hochgradig verteilten Security-Fabric** Erhalten Sie Echtzeit-Transparenz, effiziente Workflows und erhöhte Sicherheit mit zentralisierter Steuerung sowie KI-gestützte Einblicke über die gesamte Cisco Security Cloud hinweg. Die hochgradig verteilte Security-Fabric ist optimiert für Zero-Trust-Segmentierung und Anwendungsschutz in Rechenzentrums-, Cloud-, Campus- und IoT-Umgebungen. **Britta Paty** *Cisco Partner Account Executive Security | Cisco*	**Zertifikatslebenszyklus – 47 Tage Gültigkeit – PKI heute modernisieren für morgen** Zertifikate von öffentlichen CAs - dieses Jahr nur noch maximal 200 Tage gültig, im kommenden Jahr nur noch 100 Tage um dann 47 Tagen ab 2028. Schon dieses Jahr verdoppelt sich die Arbeitslast von all jenen, die in manuellen Prozessen rund um den Lebenszyklus eines Zertifikats gefangen sind. Im Vergleich zu 2025 erhöht sich der Aufwand 2028 um mehr als das Achtfache. Wir zeigen, wie sie mit unseren Automatisierungstools öffentliche Zertifikate automatisiert ausstellen, erneuern und natürlich auch überwachen. Teil des Geheimnisses ist, die nötige Domain-Validierung ebenfalls zu automatisieren - wir zeigen, wie es geht. **Daniel Ströhmann** *Regional VP Solution Engineering | DigiCert*	**Agentic-AI: Wie legt man den KI-Agenten an die Leine?** Überall ist von Agentic AI die Rede, doch die entscheidende Frage bleibt: Wie lässt man KI-Agenten auf sensible Unternehmensdaten los, ohne die Kontrolle zu verlieren? Wie lässt sich im ERP-System noch unterscheiden, ob gerade ein Algorithmus oder ein Mitarbeiter am Steuer sitzt? In seinem Vortrag zeigt Christian Kurta, Domain Consulting Manager bei Palo Alto Networks, wie sich Multifaktor-Authentifizierung um den „Faktor Mensch" erweitern lässt. Anhand einer Live-Demo demonstriert er die Implementierung robuster Guardrails für KI-Agenten. Erfahren Sie, wie Mensch- und Maschinen-Identitäten im digitalen Ökosystem koexistieren können, ohne dass einer davon zum sprichwörtlichen Elefanten im Porzellanladen wird. **Christian Kurta** *Domain Consulting Manager | Palo Alto Networks*	**Lieferkettensicherheit unter NIS-2: Vom blinden Fleck zum Risikofaktor** Mit NIS-2 rückt die Sicherheit der Lieferkette in den Fokus regulatorischer Anforderungen – und offenbart zugleich erhebliche Herausforderungen in der praktischen Umsetzung. Der Vortrag analysiert typische Defizite im Lieferantenmanagement, zeigt zentrale Pain Points auf und ordnet diese im aktuellen Umsetzungsstand österreichischer Unternehmen ein. Dabei wird deutlich, warum gerade dieser Bereich häufig unterschätzt wird und welche Implikationen sich daraus ergeben. **Melanie Gödl & Patrick Steinhuber** *Information Security Consultant | CANCOM Austria*
12:00 - 12:20	**Effiziente und schnellste IT-Sicherheit durch Zero Trust und Unified Firewall Management** Performante, integrierte Sicherheitsarchitektur von HPE mit Hybrid Mesh Firewalls, ATP und eigener Threat Intelligence – für maximale Effizienz und minimale Angriffsoberfläche. **Michael Woduschegg** *Head of Security EMEA SP | HPE*	**Exchange Online - epic fails! Geschichten vom Schulhof der globalen Mailing Infrastruktur.** E-Mails versenden und empfangen - ein Vorgang den wir täglich nutzen uns aber wenig darum kümmern. In der globalen IT-Infrastruktur darunter spielen sich dafür Dramen ab die an einen Schulhof der Unterstufe erinnern. Die Großen machen was sie wollen, die Kleinen müssen Überperformen um mitzuspielen und der Anwender ist dem Spiel manchmal hilflos ausgeliefert. Hören Sie in diesem Vortrag, was beim Mailversand alles passieren kann und was sie jetzt tun können um auf die Seite der Guten zu wechseln. **Roman Stadlmair** *Country Manager Österreich | SEPPmail*	**Schluss mit blinden Flecken – Risiken finden, bewerten und beheben** Angreifer nutzen Sicherheitslücken schneller, als Unternehmen reagieren können – vor allem dort, wo bestehende Security Kontrollen nicht optimal zusammenspielen. Der Vortrag zeigt, wie modern Cyberbedrohungen z.b.: fehlerhafte KI-Agenten oder neue Schwachstellen frühzeitig erkannt, nach realem Risiko priorisiert und sicher geschlossen werden. Der Ansatz integriert sich nahtlos in bestehende Security Architekturen und macht vorhandene Lösungen messbar effektiver. **Philipp Slaby** *Sales Engineering Manager Austria | Check Point* **Patrick Fetter** *Lead Sales Engineer, Check Point Evangelist | Check Point*	**Wir bauen Mauern, aber vergessen die Türen** Unternehmen investieren in Security und bauen komplexe Schutzmechanismen. In der Praxis bleiben jedoch genau dort Lücken offen, wo klare Prozesse, Zuständigkeiten und Zusammenarbeit fehlen. Angreifer nutzen nicht die stärksten Kontrollen, sondern diese offenen Türen. Der Vortrag zeigt typische Einstiegspunkte aus der Praxis und wie vorhandene Security durch klare Verantwortlichkeiten und strukturierte Umsetzung tatsächlich wirksam wird. **Malika Mataeva** *Information Security Officer*
12:20 - 13:25	**LUNCH BREAK IN DER PARTNER AREA**			
13:25 - 13:55	**Modern Daylight Robbery – Mit KI und Social Engineering in den Urlaub** KI-Tools sind aus dem modernen Arbeitsleben nicht mehr wegzudenken – warum also nicht auch damit Social Engineering automatisieren? Das CANCOM Red Team versucht sich mit KI und Phishing das diesjährige Urlaubsbudget aufzubessern. **Roman Schabus & Dominik Groß** *Pentester | CANCOM Austia*			
14:00 - 14:20	**Keine Kompromisse: Microsoft Security für den Mittelstand - Jetzt!** Microsoft 365 Business Premium wird zum Sicherheitskraftwerk: Defender und Purview bringen Schutz und Compliance auf Enterprise-Niveau. **Stefan Baresch** *Sr. Partner Solution Architect | Microsoft Österreich*	**Zurück in die Quanten-Zukunft: Warum der Hack von morgen bereits gestern stattfand.** Stellen Sie sich vor, Hacker stehlen heute Ihre verschlüsselten Daten, um sie morgen mit einem Quantencomputer zu knacken („Store Now, Decrypt Later"). In diesem Vortrag drehen wir die Uhr zu unseren Gunsten zurück: Erfahren Sie, wie Sie mit der europäischen Quanteninfrastruktur (EuroQCI) und dem hybriden Lösungsansatz von CANCOM dem Hackerangriff der Zukunft schon heute einen Riegel vorschieben können. **Lukas Seidl** *Principal SOC Release and Deployment Manager | CANCOM*	**Die Beschleunigte Gefahr: Wie evasive Angreifer AI und Cross-Domain-Taktiken im Jahr 2026 nutzen** Die Bedrohungslandschaft 2026 ist durch immer schnellere und schwer fassbare Gegner gekennzeichnet, deren durchschnittliche Ausbruchszeit auf nur 29 Minuten gesunken ist. Erfahren Sie, wie Bedrohungsakteure KI, Cross-Domain-Angriffe über Endpoint, Identität, Cloud und SaaS hinweg sowie den Missbrauch von Vertrauen in Lieferketten und Cloud-Identitäten nutzen, um traditionelle Sicherheitskontrollen zu umgehen. **Patrick Greinwald** *Corporate Sales Engineer | CrowdStrike*	**KI-Compliance im ISMS: EU AI Act effizient integrieren statt parallel verwaltenund Vulnerabilty-Management für Ihre Netzwerk-Infrastruktur** Mit dem EU AI Act wird KI-Compliance zu einer zusätzlichen regulatorischen Dimension, die außerhalb klassischer ISMS-Strukturen liegt. Eine isolierte Umsetzung führt jedoch zu redundanten Prozessen und mangelnder Transparenz. Der Vortrag zeigt, wie sich KI-Systeme und deren regulatorische Anforderungen strukturiert und interdisziplinär in bestehende ISMS-Mechanismen integrieren lassen. Im Fokus stehen die Verknüpfung von Risiken, Kontrollen und Compliance-Anforderungen sowie die durchgängige, auditierbare Umsetzung mit CRISAM®. **Mag. Julian Mairinger** Consultant | CALPANA business consulting GmbH
14:25 - 14:45	**Build Fast. Stay Secure. Scale Right. Azure Platforms with CANCOM Smart Deploy** Manuelle Deployments, inkonsistente Konfigurationen und fehlende Nachvollziehbarkeit sind ein Risiko für jede Cloud Security Strategie. Diese Session zeigt, wie Smart Deploy als IaC basierte Bereitstellungsplattform eine sichere, wiederholbare und überprüfbare Azure Basis schafft. Lukas Reicher gibt einen Überblick über das Zielbild und die Security Mehrwerte, während Bernhard Flür anhand konkreter Beispiele zeigt, wie Landing Zones, Governance, Policies und Drift Detection technisch umgesetzt werden – Security by Default, nicht als Nachgedanke. **Lukas Reicher & Bernhard Flür** *Senior Director Datacenter Applications & Senior System Engineer | CANCOM Austria*	**Quantum Security – Vorbereitung auf die Post-Quantum-Kryptographie in realen IT- und Netzwerkarchitekturen** Mit der Veröffentlichung erster Post-Quantum-Standards durch das NIST beginnt für Unternehmen die praktische Vorbereitung auf eine neue Generation kryptographischer Verfahren. Klassische Public-Key-Algorithmen wie RSA und ECC gelten langfristig als angreifbar, während Szenarien wie „Harvest now, decrypt later" bereits heute ein Risiko für Daten mit langer Schutzdauer darstellen. Damit wird Post-Quantum-Security nicht nur zu einem kryptographischen Thema, sondern zu einer Architekturfrage. Der Vortrag zeigt anhand aktueller Fortinet-Implementierungen, wie Post-Quantum- und Hybrid-Kryptographie bereits heute in realen Netzwerk- und Security-Architekturen eingesetzt werden können, beispielsweise für IPsec-VPN, TLS-basierte Kommunikation und Remote-Access-Szenarien, und warum kryptographische Agilität eine zentrale Voraussetzung für zukünftige Sicherheit darstellt. **Wolfgang Gröller** Principal Solutions Architect | *Fortinet*	**Robot vs. Robot – KI greift an. Varonis verteidigt.** KI basierte Cyberangriffe agieren heute schneller, präziser und automatisierter als jede menschliche Bedrohung. Phishing, Identitätsmissbrauch, Datenexfiltration – alles in Sekunden, skaliert durch autonome Algorithmen. In diesem „Robot vs.-Robot"-Zeitalter reicht klassische Security nicht mehr. Varonis liefert die Antwort: eine daten Plattform, die erkennt, was KI Angreifer tun – noch bevor sie Schaden anrichten. Mit Machine Learning basiertem Threat Detection, automatisierter Least Privilege Härtung und vollständiger Transparenz über kritische Daten, Identitäten und Zugriffe. Wenn Angriffe von Maschinen kommen, brauchen Unternehmen eine Verteidigung, die schneller, intelligenter und fokussierter ist: Varonis. Data Security. Ready for the AI era. **Sven Carlsen** *Sales Engineer | Varonis*	**Identity Risk Review** Identitäten sind heute das zentrale Angriffsziel moderner Cyberangriffe – und damit einer der größten Risikofaktoren für Unternehmen. In diesem Vortrag beleuchten wir, wie Identitätsrisiken entstehen, wie sie sichtbar gemacht werden können und welche Rolle Identity Risk Reviews bei der Prävention, Erkennung und Reduktion dieser Risiken spielen. Wir zeigen wie Organisationen ihren aktuellen Reifegrad bewerten und konkrete Maßnahmen ableiten können, um Identitäten nachhaltig abzusichern. **Theresa Meiksner** *Solution Architect | CANCOM Austria*
14:45 - 15:20	**COFFEE BREAK IN DER PARTNER AREA**			
15:20 - 15:40	**Malware in der Blockchain - Na, bitte ned** Wer so wie ich am Rande von verschiedensten Use-Cases in der Blockchain gehört oder mal gelesen hat abseits durch Crypto reich zu werden – wird erstaunt sein wie raffiniert und smart Angreifer bzw. APT-Gruppen sich auch neuste Technologien zu Nutze machen. Erfahren Sie mehr von der unlöschbaren Malware-Staging Infrastruktur und was für ein Segen die Blockchain für Angreifer ist und wie man danach auch in seinem Unternehmen suchen kann! **Erwin Friedl** *Senior Manager Cyber Defense Center | CANCOM Austria*	**360° IT-Security: Von Zero Trust bis SASE, von Edge to Cloud** Security-Strategien von HPE die Edge, Cloud und Nutzer verbinden. Best Practices für umfassende Netzwerk- und Anwendungssicherheit mithilfe von Universal ZTNA und Unified SASE. **Thomas Latzer** *SASE & Security Sales Specialist | HPE*	**Mehr als eine Firewall: Cisco Secure Firewall meets Identity Intelligence** Moderne Angriffe zielen längst nicht mehr nur auf Netzwerkgrenzen – sie kompromittieren Identitäten. In dieser Session zeigen wir, wie die Integration von Cisco Secure Firewall und Cisco Identity Intelligence eine neue Verteidigungsebene schafft: kontextbasierte Zugriffssteuerung, die nicht nur weiß, was ins Netz will – sondern wer es ist und ob diesem Wer noch vertraut werden darf. **Adil Hussain** *CISSP, Cybersecurity Specialist | Cisco Austria*	**A segmentation journey within OT networks** In diesem Vortrag wird eine praxisnahe Reise durch die Network-Segmentierung in OT-Umgebungen gezeigt – von der ersten Transparenz über Assets und Kommunikation bis hin zu klaren Zonen, Segmenten und kontrolliertem Enforcement. Anhand eines schrittweisen Modells wird verdeutlicht, warum klassische IT-Sicherheitsansätze in der OT nicht ausreichen und wie sich Security und Verfügbarkeit sinnvoll vereinen lassen. Ziel ist es, Ordnung, Kontrolle und Vertrauen in hochkritischen OT-Netzen zu schaffen, ohne den Betrieb zu gefährden. **Robert Himmerich** *OT Security Architect | CANCOM Austria*
15:45 - 16:05	**ADCS Persistenz als neuartige Zeitbombe von Ransomware-Akteuren.** Akteure nutzen ADCS seit Jahren als eine der effektivsten Techniken zur schnellen Privilegieneskalation und Unternehmenskompromittierung. Jedoch bis dato unbekannt ist, dass Ransomware Gruppen ADCS nicht nur missbrauchen, sondern aktiv selbst implementieren, manipulieren und als persistente Zeitbombe hinterlassen. Damit wird Voll- sowie Langzeit-Zugriff der Unternehmen, mit einem Click, ohne Malware, getarnt als Microsoft Service, geschaffen, welche herkömmliche Gegenmaßnahmen als unwirksam zurücklassen. Einblicke in diese Angriffe, Gegenmaßnahmen und vor allem Awareness zu diesem Angriff wird in diesem Talk aufgezeigt. **Gideon Teubert** *Senior Manager Cyber Defense Center | CANCOM Austria*	**From Packets to Intelligence: Scaling Security Through Smart Network Visibilityd** As network speeds and traffic volumes continue to grow, traditional security analytics struggle with data overload, rising ingestion costs, and slower time to insight. This session explores how smart network visibility transforms raw packet data into high value security intelligence by selectively extracting metadata and enriching flows with deep application context at high speed. By feeding only relevant, security ready data into modern analytics pipelines, organizations can enable effective threat hunting, improve operational efficiency, and scale security analytics without the burden of full packet ingestion. **Christian Lazar** *Solution Engineer | Keysight*	**CANCOM Inventory Engine (IE): Professionelles Asset-, Lifecycle- und Vulnerability-Management für Ihre Netzwerk-Infrastruktur** Wir zeigen Ihnen, wie Sie mithilfe dieses CANCOM Eigenproduktes sämtliche Hardware- und Software-Assets Ihres Netzwerks stets im Auge behalten können. Veränderungen der Installed Base werden mithilfe der IE Snapshot Technologie nachvollziehbar gemacht. Die IE ermöglicht das zentrale Management von Software-Versionen, Compliance (z.B. NIS-2, DORA) und Vulnerabilities. Alle relevanten Asset-, Lifecycle- und Sicherheitsdaten stehen flexibel über GUI, Reports und REST API auch für Drittsysteme zur Verfügung. Vereinfachen Sie das Management Ihrer Netzwerk-Infrastruktur – mithilfe der CANCOM Inventory Engine! **Thomas Gerbafczits** *Senior Director Network Solutions | CANCOM Austria*	**Industrielle Kommunikation und Cybersecurity mit Siemens** Im Rahmen dieses Fachvortrags erhalten Sie einen umfassenden Einblick, wie SIEMENS Digital Industries seine Kunden auf dem Weg zu einer sicheren, resilienten und zukunftsfähigen OT Netzwerkarchitektur begleitet. Unser Experte zeigt auf, welche strategischen und technologischen Ansätze Siemens verfolgt, um industrielle Netzwerke ganzheitlich abzusichern – von modernster OT Networking Hardware über leistungsfähige Security Softwarelösungen bis hin zu skalierbaren Services entlang des gesamten Anlagenlebenszyklus. **Ferdinand Strauss** *Sales Specialist Industrial Networks| Siemens*
16:10 - 16:30	**Der Anruf kommt aus dem Haus – ein realitätsnäherer Blick auf Insider Threats** Zwischen Shadow-IT, ignorierten Arbeitsanweisungen und pauschal weitergeleiteten E-Mails entstehen die meisten Insider Threats nicht á la Hollywood durch kriminelle Energie, sondern vor allem aufgrund der Entfernung zwischen „uns" und „denen". Dieser leichtherzige Vortrag betrachtet alltägliche Situationen und bemüht sich zukünftige Bemühungen aus dem Akademischen in die Realität zu ziehen. **Dan Jung** *Senior Security Operations Consultant | CANCOM Austria*	**Schluss mit Alchemie: Der richtige Wirkstoff für Analyse im Security Apothekertrakt heißt Network Evidence** Analyse: Von der Alchemie zur digitalen Evidenz Rezeptur: Die perfekte Wirkstoff-Kombination für Ihr SOC Heilung: Präzise Intervention statt langwieriger Quarantäne **Timo Jobst** *Senior Sales Engineer | Corelight*	**Asset-, Lifecycle- und Vulnerability-Management in der Praxis: Live Demo, Deep-Dive zu Funktionen & Integrationen sowie exklusive Roadmap-Einblicke zur CANCOM Inventory Engine (IE)** Die CANCOM Experten zeigen live, wie die Inventory Engine als zentrale Single Source of Truth alle Hardware-, Software-, Firewall- und Endpoint-Assets automatisiert inventarisiert und übersichtlich aufbereitet. Per Knopfdruck erhalten Kunden einen klaren Überblick über Lifecycle- und Vulnerability-Status und setzen darauf aufbauend Lifecycle-, Patch-, Compliance- und Reporting-Prozesse effizient um. Über Risk Register, REST API und bestehende Integrationen lässt sich die Lösung nahtlos in Drittsysteme einbinden und wird durch einen Ausblick auf die zukünftige Roadmap abgerundet. **Thomas Gerbafczits,** *Senior Director Network Solutions, CANCOM Austria* **Rudolf Puffing**, *Manager SI Software Development, CANCOM Austria* **Jasmin Zukic**, *Systems Engineer Network Solutions, CANCOM Austria*	**Wandel in der OT und die Rolle von modernem PAM** OT fremdelt nicht mehr mit der IT. Neue Architekturen in der Produktion nutzen Daten aktiv und bereiten den Weg für den Einsatz digitaler Agenten in selbstorganisierenden Anlagen. Dabei bleibt der Vorrang der Verfügbarkeit der Produktionsprozesse und der funktionalen Sicherheit bestehen. Privileged Access Management erhält in der industriellen Automatisierung eine wichtigere Rolle. Es geht nicht mehr nur um den Fernzugriff für die Wartung, sondern um die Kontrolle und Verwaltbarkeit menschlicher und nichtmenschlicher Identitäten in kritischen Umgebungen. **Jamie Wilkins** *Account Manager DACH & OT | SSH Communications Security*
16:40 - 17:00	**Abschlussvortrag** *CANCOM Austria*			
17:00-17:10	**Recap und Verlosung**			
Im Anschluss (18:00 Uhr)	**Chill & Cheers: Der perfekte Abschluss. Food, drinks, networking.**			

PLATINUM SPONSORS

Security Solutions Track

AI & Security Track

Information Security & Management Track

PLATINUM SPONSORS

Quantenkryptographie

AI & Security Track

Information Security & Managment Track

TRENDS & NEWS

Security & Connectivity Track

Security Solutions Track

OT Security Track