Rostocker Phishmarkt 2025 - Agenda

Zeit	Thema	Sprecher	Titel	Sprecher Information	Zusammenfassung
12:30 - 13:00	Ankunft und Kennenlernen				
13:00 - 13:15	Grußwort des Finanzministers MV	Dr. H. Geue	Finanzminister - Mecklenburg-Vorpommern	Dr. Heiko Geue ist promovierter Volkswirt und seit November 2021 Finanzminister des Landes Mecklenburg-Vorpommern (seit Juli 2025 zusätzlich zuständig für Digitalisierung). Zuvor war er unter anderem persönlicher Referent von Frank-Walter Steinmeier im Bundeskanzleramt, leitete Stationen in der Bundesverwaltung und übernahm von 2019 bis 2021 die Leitung der Staatskanzlei in Schwerin. Mit seiner Erfahrung aus Bundes- und Landespolitik steht er für solide Finanzpolitik und die digitale Transformation in Mecklenburg-Vorpommern.	
13:20 - 13:40	Cybercrime: Aktuelle Lage	M. Voss	Geschäftsführer - Cloud Ahoi GmbH	Matthias Voss ist Diplom-Informatiker und Mitgründer der Cloud Ahoi GmbH (2021). Zuvor entwickelte er im Windenergie-Sektor Software für Steuerung, Überwachung und Datenakquise und verantwortete ab 2013 in einem Operations Center in Chicago die Entwicklung zur Überwachung von >2.000 Windkraftanlagen weltweit. Ab 2015 leitete er Projekte in einem Beratungsunternehmen und war dort mitverantwortlich für Cybersicherheit. Seit März 2025 gehört Cloud Ahoi mehrheitlich zur Net Group (Estland) – damit verbindet Voss Security-Beratung mit Software- und Digitalisierungs-Expertise für kritische Infrastrukturen.	Cyberkriminalität bleibt auf hohem Niveau, wobei Ransomware weiterhin den größten Schaden verursacht. Begünstigt wird die Lage durch sinkende Einstiegshürden (Cybercrime-as-a-Service), zunehmende Vernetzung und damit wachsende Angriffsflächen – vom Einsatz neuer Technologien bis zu komplexen digitalen Infrastrukturen. Zugleich beeinflussen geopolitische Spannungen Motive und Ursprünge vieler Angriffe. Der Vortrag ordnet die aktuelle Bedrohungslage ein und beantwortet drei Leitfragen: (1) Was sagen die Zahlen und Trends? (2) Wer steht besonders im Fokus (Branchen, Funktionen, Ketteneffekte)? (3) Welche Angriffsszenarien dominieren – insbesondere Ransomware, Business-Email-Compromise und Supply-Chain-Vorfälle? Abschließend skizzieren wir praxisnahe Ansatzpunkte für Prävention, Detektion und reaktionsfähiges Krisenmanagement in Organisationen.
13:45 - 14:15	Wie funktioniert ein Phishing-Angriff?	M. Voss	Geschäftsführer - Cloud Ahoi GmbH		Trotz technischer Schutzmaßnahmen bleibt Social Engineering – insbesondere Phishing – das häufigste Einfallstor für Cyberangriffe. Ziel der Täter ist es, über gefälschte E-Mails, Webseiten oder Messenger-Nachrichten sensible Informationen wie Zugangsdaten, Zahlungsdaten oder Unternehmensinterna zu erbeuten. Dabei setzen sie auf ausgeklügelte Täuschungstaktiken: Vertrauen aufbauen, Dringlichkeit erzeugen, Marken imitieren. Der Vortrag ordnet zentrale Begriffe, erklärt den typischen Ablauf von Social-Engineering-Kampagnen und zeigt aktuelle Beispiele aus der Praxis. Abschließend werden kompakte Hinweise gegeben, woran sich Angriffe erkennen lassen und welche Sofortmaßnahmen (Melden, Isolieren, Passwort-Reset, MFA) in der Organisation greifen sollten.
14:20 - 15:10	ZAC MV: Beispiele aktueller Angriffe und Techniken	T. Voß	ZAC Polizei - Mecklenburg-Vorpommern	Die Zentrale Ansprechstelle Cybercrime Mecklenburg-Vorpommern (ZAC MV) ist beim Landeskriminalamt angesiedelt und seit Jahren Ansprechpartner für Unternehmen, Institutionen und Verbände zum Thema „Cyberkriminalität“. Sie wirkt präventiv durch konkrete Sicherheitswarnungen und unterstützt im Ernstfall bei Erpressungs- und Betrugslagen. Damit verbindet die ZAC MV polizeiliche Ermittlungs- und Strafverfolgungskompetenz mit praxisnaher Beratung zum Umgang mit digitalen Bedrohungen.	Jedes Unternehmen ist von Cybercrime bedroht. Die Täter bedienen sich fortwährend an neuen Ideen und technologischen Hilfsmitteln, um Unternehmen zu täuschen und Schwachstellen in der IT-Landschaft auszunutzen. Die Vorgehensweise der Täter ist stets Teil der polizeilichen Ermittlungen.Der Vortrag der Zentralen Ansprechstelle Cybercrime Mecklenburg-Vorpommern (ZAC MV) zeigt, welche Aufgaben die Polizei in Bezug zu Cyber-Sicherheitsvorfällen inne hat und wie die Zusammenarbeit mit Unternehmen in der Praxis aussieht. Anhand realer Fälle wird veranschaulicht, wie Unternehmen auf Cybercrime reagieren sollten und welche Unterstützung Betroffene erwarten können. Hinzu gibt die ZAC MV Tipps zu der Anzeigenaufnahme.
15:10 - 15:50	Kaffee-Pause				
15:50 - 16:25	Wie läuft eine Krisen-Simulation ab?	H. Schilling	Berater - mata solutions GmbH	Henrik Schilling ist Berater bei mata solutions (seit 2018) mit Schwerpunkt BCM, Notfallmanagement sowie Konzeption und Durchführung von Krisenmanagement-Simulationen. Er unterstützt Betreiber Kritischer Infrastrukturen und Kommunen beim Aufbau und der Weiterentwicklung individueller Krisenstabs- und Entscheidungsprozesse. Schilling hat einen Master in Internationaler Politik & Recht, promoviert zur Rolle Kritischer Infrastruktur in hybriden Bedrohungen und forscht am Institut für Sicherheitspolitik (ISPK), Universität Kiel u. a. zu maritimer KRITIS. Er steht für methodisch saubere Stabsarbeit und praxisnahe Übungen, die Regelwerke in geübtes Handeln übersetzen.	Sabotage, Spionage, Erpressung – Angriffe krimineller oder staatlicher Akteure erfordern ein flexibles Krisenmanagement. Prävention und Systemhärtung sind unverzichtbar, reichen jedoch nicht aus. Tritt der Ernstfall ein, braucht es klare Strukturen, stringente Stabsarbeit und schnelle, nachvollziehbare Entscheidungen – zugeschnitten auf die individuellen Anforderungen der Organisation. Der Vortrag zeigt exemplarisch, wie Unternehmen Übungen und Simulationen selbst oder mit externer Unterstützung aufsetzen: von Scoping & Szenario-Design über Rollen & Verantwortlichkeiten bis zu realitätsnahen Injects (E-Mails, Anrufe, Medien/Behörden). Anhand eines Beispiel-Falls werden Ablauf, Beteiligte und der sinnvolle Grad der Individualisierung erläutert. Abschließend erhalten Teilnehmende konkrete Hinweise, wie sie durch klare Strukturen und regelmäßiges Üben ihre Krisenmanagementprozesse wirksam schärfen – und offene Fragen werden im Anschluss gemeinsam diskutiert.
16:30 - 17:00	NIS-2 - Was ist das und was muss getan werden?	Dr. M. Kaulke	CISO - Cloud Ahoi GmbH	Dr. Matthias Kaulke ist ausgebildeter Physiker und seit mehr als 25 Jahren in der IT tätig. Er ist Mitgründer der Cloud Ahoi GmbH (2021) und war davor Gründer und viele Jahre Geschäftsführer der BEKAST IT Consulting. Seit 2013 arbeitet er als Berater in Entwicklungsprojekten, in der Organisationsentwicklung und baut Systeme für das Qualitäts- & Informationssicherheitsmanagement (ISO 9001 und ISO 27001) auf. Seit 2021 ist er bei der Cloud Ahoi als CISO für die Informationssicherheit und deren Management nach ISO 27001 und TISAX zuständig.	Die NIS-2-Richtlinie stellt Unternehmen und Organisationen vor erhebliche Pflichten in Bezug auf IT-Sicherheit und Governance. Im Vortrag gibt Dr. Kaulke einen praxisnahen Überblick: Welche Organisationen sind betroffen, welche Kernpflichten ergeben sich, und wie lassen sich Menschen, Prozesse und Technologien in einem ISMS sinnvoll verankern? Typische Fallstricke und pragmatische Ansätze zur Umsetzung runden den Beitrag ab.
17:00 - 17:45	Diskussionsrunde: Fragen an die Referenten				
18:00 - 20:00	Networking Dinner				