PILS
Cyber Defence

EVENT CYBER RESILIENCE

Strategisches Cyber-Risikomanagement für Großveranstaltungen,
Sport-Events & Internationale Summits

Wir haben Erfahrung mit der Gesamtabwicklung bei Mega Projekten wie dem **Eurovision Song Contest**. 2026 haben wir im Auftrag des ORF in Wien die Rolle des **Head of Cybersecurity** übernommen und verantworten das gesamte Cyber-Risk-Management und die Strategisch-Taktische Abwicklung des gesamten Cyber-Defence Einsatzes.

EVENT CYBER RESILIENCE

Strategisches Cyber-Risikomanagement für Großveranstaltungen, Sport-Events & Internationale Summits

Wir liefern das „Betriebssystem" für die digitale Sicherheit Ihres Events – unabhängig, objektiv und weltweit skalierbar.

Großevents wie Weltmeisterschaften, Olympische Spiele oder politische Gipfeltreffen sind heute digitale Hochrisikoumgebungen: Extremer Zeitdruck, komplexe Lieferketten und globale Aufmerksamkeit schaffen Einfallstore, die mit klassischer Unternehmens-IT kaum zu schützen sind. Ein Cybervorfall ist hier kein technisches Problem, sondern eine unmittelbare Gefahr für den Ablauf, die Reputation und in weiterer Folge auch für die öffentliche Sicherheit.

Unser Ansatz: Cyber-Führung statt Verkaufsinteressen

Pils Cyber Defence unterstützt Veranstalter als externer CISO und Head of Cybersecurity – von der frühen Planungsphase bis zum Abschlussbericht. Im Fokus steht ausschließlich das Cyber-Risikomanagement und die dazugehörige Governance, nicht der Verkauf von Technik oder Betriebsleistungen.

Der entscheidende Unterschied:

- **Reine Cyber-Führungsebene:** Wir agieren bewusst ohne eigene operative Cyber-Teams (z. B. SOC-Analysten oder Hardware-Techniker), die ausgelastet werden müssen.
- **Radikale Neutralität:** Wir verkaufen keine Hardware und keine Stundenpakete. Empfohlen wird, was für das Cyber-Risikoprofil Ihres Events notwendig ist – nicht, was interne Umsätze generiert.
- **Best-of-Breed Strategie:** Für jedes Event und jedes Gastland wählen wir die passenden Cyber-Spezialisten oder lokalen Partner aus und steuern diese zentral – unabhängig von Hersteller- oder Dienstleisterinteressen.
- **Vernetzung in die Gesamtsicherheit:** Unser Mandat ist der Cyberraum. Für physische Sicherheit, Crowd Management, Brandschutz oder Anti-Terror-Maßnahmen arbeiten wir mit spezialisierten Partnern zusammen und stellen gerne Kontakte her oder übernehmen die technische Gesamtkoordination der Schnittstellen.

Cyber Risk Command & Platform

(Managed Cyber Risk Management für Events)

Auf Wunsch übernehmen wir nicht nur Konzeption und Governance, sondern auch den laufenden Betrieb eines „Cyber Risk Command" – als gemanagte Lösung für Ihr Event:

- **Zentrale Cyber-Risk-Plattform:** Konsolidierte Sicht auf alle Cyberrisiken, Maßnahmen, Verantwortlichkeiten und Deadlines – modular erweiterbar, sodass sie bei Bedarf auch das gesamte Event-Risikomanagement (inkl. Non-Cyber-Risiken) abbildet.
- **Laufende Betreuung:** Regelmäßige Risiko-Reviews, Aktualisierung der Maßnahmen, Eskalationsmanagement und Reporting an Eventleitung, Stakeholder und Behörden.
- **Integrierte Kollaboration:** Aufgaben, Dokumente und Entscheidungen werden in der Plattform nachvollziehbar gesteuert – von Lieferanten-Onboarding über Freigaben bis hin zu „Lessons Learned" nach dem Event.
- **Wiederverwendbare Struktur:** Die Plattform kann nach dem Event auf Folge-Veranstaltungen, Serien-Events oder die Linienorganisation übertragen werden.

Das Cyber-Leistungs-Framework

Wir konzentrieren uns konsequent auf Cyber-Risiken und digitale Angriffsflächen. Das Framework ist modular und bei internationalen Hochsicherheits-Events erprobt.

1. Cyber Governance & Strategic Command

Wer entscheidet, wenn es digital brennt?

- **Interim CISO & Cyber-Stab:** Aufbau der Cyber-Stabsstelle und Einbindung in die bestehende Sicherheitsarchitektur (Safety & Security, Krisenstab).
- **Cyber-Risikomanagement:** Identifikation der digitalen „Kronjuwelen" (z. B. Akkreditierungssysteme, Zeitmessung/Scoring, Ticketing, Broadcast, Payment) und Bewertung der Cyberrisiken in Management-Sprache.
- **Cyber-Lage & Schnittstellen:** Definition der Schnittstellen zu physischer Sicherheit, Behörden und Notfallorganisationen, ohne diese selbst zu ersetzen.

2. Supply Chain Cyber Security

Ihr Cyber-Risiko ist nur so niedrig wie das schwächste Glied in Ihrer digitalen Lieferkette.

- **Cyber-Onboarding für Lieferanten:** Strukturierte Vorab-Prüfung und Rating der digitalen Sicherheitsreife (Konfigurationen, Zugriffskonzepte, Logging, Patch-Stand).
- **Risikoklassifizierung:** Trennung cyberkritischer Partner (z. B. Zutritt, Regie-Technik, Ticketing-Plattform) von unkritischen Gewerken und Ableitung verbindlicher Cyber-Mindeststandards.
- **Cyber Security Riders:** Vertragsbausteine zu Themen wie MFA, Netzwerksegmentierung, Monitoring, Incident-Meldepflichten und „No Unknown Device"-Policy.

3. Cyber Incident Command & Readiness

Digitale Einsatzbereitschaft für den Worst Case.

- **Cyber Action Cards:** Rollenbasierte Checklisten für Szenarien wie Ransomware, Ausfall der Einlasssysteme, Data Leak, Account-Übernahme oder DDoS-Angriffe auf kritische Plattformen.
- **Tabletop-Übungen (Cyber-Fokus):** Simulation von Cybervorfällen mit Geschäftsführung, Eventleitung und IT, abgestimmt mit physischer Sicherheit und Krisenstab.
- **Steuerung der Cyber Operations:** Konzeption und Führung der Cyber-Meldewege (SOC/NOC, CERT, Dienstleister), inklusive klarer Eskalations- und Kommunikationspfade.

4. Awareness & Human Cyber Risk

Reduktion menschlicher Fehler als Einfallstor für Cyberangriffe.

- **„The Secure 10" (Cyber):** Die wichtigsten Cyber-Verhaltensregeln auf einer Seite – verständlich für Volunteers, Technik-Teams und Staff.
- **IP & High Profile Cyber Protection:** Diskrete Cyber-Briefings für VIPs, Künstler oder Athleten (Phishing, Account-Schutz, Social Media, Deepfakes).
- **Anti-Fraud & Social Engineering:** Spezielle Formate für Finanz-, HR- und Akkreditierungs-Teams zur Abwehr von CEO-Fraud, Ticket-Betrug und Social-Engineering-Attacken.

Ihr Nutzen

- **Fokussiertes Cyber-Risikomanagement:** Klare Priorisierung aller digitalen Risiken und Maßnahmen, abgestimmt mit physischer Sicherheit und Gesamt-Sicherheits-konzept.
- **Managed Cyber Risk Command & Platform:** Ein durchgängiges, gemanagtes System, das Cyberrisiken transparent macht und – wenn gewünscht – als Rückgrat Ihres gesamten Event-Risikomanagements dienen kann.
- **Haftungsminimierung:** Lückenlose, cyberbezogene Dokumentation aller Sicherheits-entscheidungen („Due Diligence") für Stakeholder, Behörden und Versicherungen.
- **Flexible Kostenstruktur:** Sie beziehen High-End-Cyber-Expertise genau dann, wenn Sie sie brauchen – operative Teams und physische Sicherheit ergänzen wir bei Bedarf über unser Netzwerk.
- **Geschwindigkeit:** Durch bestehende Cyber-Templates (Prozesse, Richtlinien, Action Cards) verkürzen Sie die Konzeptionsphase deutlich.

Sichern Sie das Cyber-Risikoprofil Ihres Events mit System.

Lassen Sie uns über Ihre Cyber-Sicherheitsarchitektur und Ihr Cyber Risk Command & Platform sprechen.

martin@cyber-defence.at