T.I.S.P./T.P.S.S.E. Community Meeting 2026

Berlin, 10. - 11.11.2026

NIS-2, KRITIS und Co. Wie Cyber Security Compliance einen echten Mehrwert bieten kann

Marcel Al-Mosawi

SVA System Vertrieb Alexander GmbH



Marcel Al-Mosawi

Head of Cyber Security GRC
ISMS ISO 27001 Auditor

Über mich

Vorstellung

Fachgebiete: Informationssicherheit, ISO 27001, GRC, Security Awareness

- ISMS ISO 27001 Lead Auditor (TÜV)
- Zusätzliche Prüfverfahrenskompetenz §8a BSIG
- Informationssicherheitsbeauftragter (TÜV)
- TeleTrust Information Security Professional T.I.S.P. (TÜV)
- Datenschutzauditor (TÜV)
- Datenschutzbeauftragter (TÜV)
- CheckPoint Certified Security Expert R77.30 (CCSE)
- ITIL V4 Foundation
- …

Unser Leistungsportfolio

AI Security



Cloud Security



Cyber Security Architecture



Digitale Forensik & Incident Response



Cyber Security GRC



OT Security



Offensive Security



Secure Infrastructure



Security Operations Center



Security Operational Services



Unser Leistungsportfolio

AI Security
- AI Security Assessment
- Shadow AI Detection & Prevention
- Data Security for AI (DSPM, DLP & Data Classification)
- Secure AI Applications
- AI Governance & Compliance



Cloud Security
- Security Posture Management
- Cloud Native App Protection Platform
- Secure Access Service Edge
- Security Service Edge
- Key Management
- Threat Intelligence
- Infrastructure as a Service Security
- Attack Surface Management



Cyber Security Architecture
- Security Architecture Design
- Continous Monitoring and Improvement
- Strategic Planning
- Cloud and Hybrid Environment Security
- Zero Trust Architecture
- Trusted Advisory



Digitale Forensik & Incident Response
- Cyber Threat Scenario Workshops
- Compromise Assessments
- Proactive Incident Response Services
- Remediation
- Emergency Planing
- Attack Simulation



Cyber Security GRC
- Standards Implementation for Information Security (ISO 27001, TISAX)
- Policy-Development
- Blueprints, Baselines & Playbooks
- Cyber Security Resilience Planing
- ISMS and Data Protection Mgmt. System
- IT Risk Management
- Risk Assessments
- Compliance Assessments
- Cyber Security Awareness



OT Security
- IoT Security Assessments
- OT Threat Detection & Response
- IoT Asset Visibility
- IoT Security Architecture Design
- IT/IoT Network Segmentation
- OT Governance
- IT/OT SOC Services



Offensive Security
- Penetration Testing for Web applications, WIFI, Active Directory, Network, Physical, Cloud, IoXT, and Mobile
- Identity-Security (Active Directory/Entra ID)
- Infrastructure Security (Netzwerk & Attack Surface Detection/WLAN)
- Red & Purple Teaming



Secure Infrastructure
- Continuous Threat Exposure Management
- Data Activity Monitoring
- Identity Management
- Network Segmentation/Segregation
- Data Management/Data Loss Prevention
- EDR/XDR/NDR
- Exposure Management
- Firewalling (OnPrem/Cloud/ Infrastructure as a Service/ Landingzone)



Security Operations Center
- 24x7 Security Monitoring
- Managed Threat Detection & Response
- EDR/NDR/XDR/SIEM
- ISO 27001 certified
- IT Security made in Germany



Security Operational Services
- 24x7 Security Operations
- Managed Security Services
- Change Management
- Problem Management
- System Monitoring
- ISO 27001 certified





Teil 1: Das Problem

Gesetze und regulatorische Anforderungen

/ Der Mythos

„Wenn ich compliant bin, bin ich auch sicher!

- Compliance allein macht keine Sicherheit
- Gesetze wie NIS-2 bilden lediglich eine **BASIS**
- Cyber Security muss immer ganzheitlich betrachtet werden





Interdisziplinäre Herausforderung

- Kombination aus Recht und Informationssicherheit
- Interpretationsspielraum ist groß
- Unpräzise Formulierungen

- Beispiel aus §30 BSIG:

> „Erstellung von Konzepten für Sicherheit des Personals […]“

Wie setzen Unternehmen NIS-2 um?

- Ignorieren
- Nur das Nötigste umsetzen
- Cyber Security ganzheitlich umsetzen



Was verändert NIS-2 in der Praxis?

Durchführung einer indikativen Befragung von 10 Unternehmen

Frage: Hat sich die Informationssicherheit durch NIS-2 in Ihrem Unternehmen verändert?

➔ **7 von 10** berichten von einer veränderten Bedeutung der Informationssicherheit

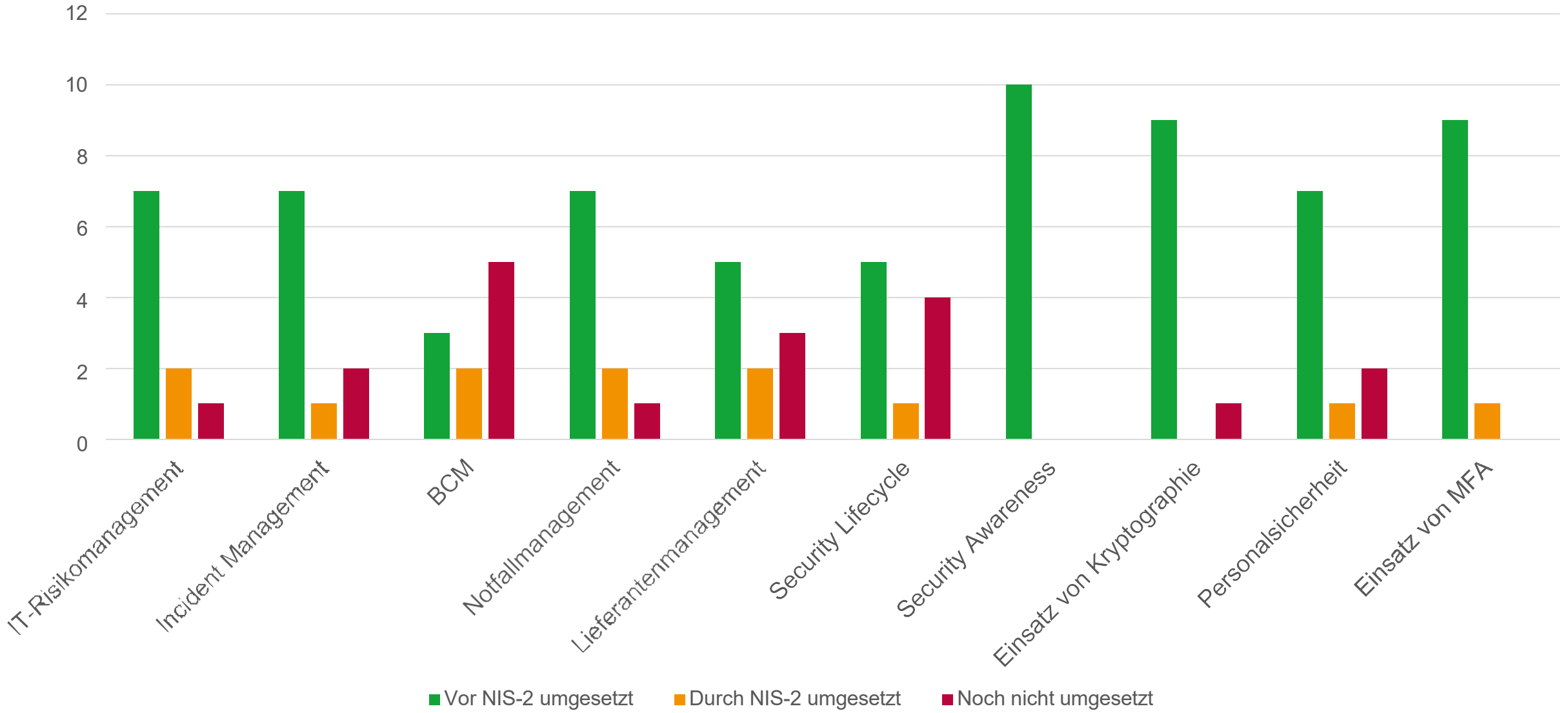
Hat mehr an Bedeutung und Wahrnehmung gewonnen

Maßnahmen wurden wegen der GF-Haftung genehmigt

Sichtbarkeit und Awareness sind gestiegen. GF setzt sich mit dem Thema auseinander!

Fokus auf Informations-sicherheit hat sich geschärft!

Welche Maßnahmen wurden durch NIS-2 umgesetzt?



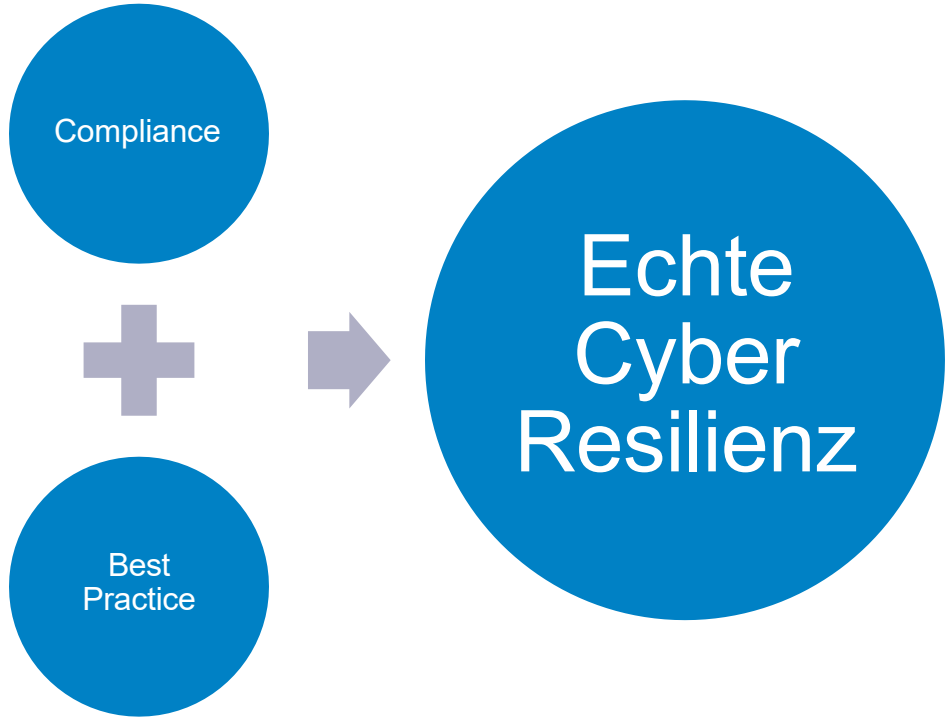


Teil 2: Die Lösung

Wie macht man aus Compliance echte Cyber Resilienz?

Compliance allein reicht nicht

- Compliance ist nur der Anfang
- Gelebte IT-Sicherheit und Cyber Resilienz durch Best Practices
- Stand der Technik
- Kontinuierliche Verbesserung
- Verbesserung von Unternehmensprozessen
- Marktvorteil (z.B. durch Zertifizierung)
- Lieferkettensicherheit



/ ISMS

ISO 27001 bildet eine gute Grundlage

- Deckt die meisten gesetzlichen Anforderungen ab
- Angemessenheit beachten
- Interpretationen und Stand der Technik beachten
- Grundlage muss durch Best Practices ergänzt werden (z.B. ISO 27002, NIST, BSI-Grundschutz)



Umsetzung


Anforderung verstehen
Geschäfts-kontext bestimmen
Risiken und Szenarien bewerten
Fähigkeiten aufbauen Maßnahmen umsetzen
Wirksamkeit überprüfen
Cyber Resilienz

/ Key Take Aways

Fazit

- Compliance ist eine Chance
- Ein Zertifikat verhindert keinen Angriff
- Anforderungen sind eine Grundlage
- Interpretation oft schwierig
- Best Practices sind notwendig für ganzheitliche Sicherheit



Vielen Dank für die Aufmerksamkeit

Fragen und Antworten.



/ Ihr Weg zu uns

Kontakt



Marcel Al-Mosawi
Head of Cyber Security GRC

Marcel.Al-Mosawi@sva.de
www.sva.de

Standort Düsseldorf
Kennedydamm 24
40476 Düsseldorf