# PROFILE

## IT-Sicherheit in der Energiewirtschaft

www.ew-online.de/fachzeitschriften I | 2016

KRITIS · ISO/IEC 27001 · Consulting · ISMS · Auditierung
IT-Sicherheitskatalog · Kryptographie · IT-Compliance
Datenschutzbeauftragter · Risikoanalyse · Zertifizierung

Eine Sonderveröffentlichung von

EUROHeat&Power ew netzpraxis

# Ihre Partner für IT-Sicherheit in der Energiewirtschaft

PROFILE

| 3 | 4–5 | 6 | 7 | 8–9 | 10 | 11 | |
|---|---|---|---|---|---|---|---|
| **KEYMILE GmbH** Hannover www.keymile.com | **mdex AG** Tangstedt www.mdex.de | **PÜG Prüf- und Überwachungsgesellschaft mbH** Gäufelden www.pueg.de | **Rhebo GmbH** Leipzig www.rhebo.com | **TÜV Rheinland i-sec GmbH** Köln www.tuv.com/informationssicherheit | **TÜV Informationstechnik GmbH** Essen www.tuvit.de | **WEMAG AG** Schwerin www.wemag.com | |
| ■ | ■ | | | ■ | | | Abhörsichere Kommunikation |
| | ■ | | | ■ | | | Access- und Identity-Management |
| | | | | ■ | | | Active Directory Domain Services (ADDS) |
| | | | | ■ | ■ | | Advanced Persistent Threat (APT) |
| ■ | ■ | | ■ | | | | Alerts |
| | | | ■ | ■ | | | Analysen (Ad Hoc, Langzeit) |
| | | | | ■ | | | Anti-Spam |
| | | | | ■ | | | Application-Management |
| | | | | | | | Archivierung |
| | ■ | | | ■ | | | Asset-Management |
| | | ■ | | ■ | ■ | | Auditierung (+Qualitätsmanagement) |
| | ■ | | ■ | ■ | | | Ausfallsicherheit |
| | ■ | | | ■ | | | Authentifizierung / Zwei-Faktor-Authentifizierung |
| | | | | ■ | | | Backup-Management |
| | | | | ■ | | | Bring your own device (BYOD) |
| | | | ■ | ■ | ■ | | Business Continuity Management (BCM) |
| | | | | ■ | | | Business Service Management (BSM) |
| | | | | ■ | | | Cloud Management |
| ■ | ■ | | | ■ | ■ | | Consulting |
| | | | ■ | | | | Content Inspection |
| | | | ■ | ■ | | | Data Leakage Prevention |
| | | | ■ | ■ | ■ | | Data Loss Prevention |
| | | | | ■ | | | Datenkorrelation |
| | | | | ■ | ■ | | Datenschutzbeauftragten stellen |
| ■ | | ■ | | ■ | ■ | | Datenschutzkonzept |
| | ■ | | ■ | ■ | | | Echtzeit Einblick |
| | | | | | | | Elektromagnetische Verträglichkeit (EMV) |
| ■ | ■ | | | ■ | | | Ende-zu-Ende-Verschlüsselung |
| | | | | ■ | | | Entdpoint Security |
| | | | | | | | Fachliteratur |
| | ■ | | | ■ | | | Firewall |
| | ■ | | | | | | Firmware Management |
| | ■ | | | | | | Full Service |
| ■ | | | | | ■ | | Hardware Security |
| | ■ | ■ | | ■ | ■ | ■ | Information Security Management System (ISMS) |
| | | | | ■ | | | Information Sharing |
| | | | ■ | ■ | | | Intrusion Detection System (IDS) |
| | | | | ■ | | | Intrusion Prevention System (IPS) |
| | ■ | ■ | | ■ | ■ | | ISO/IEC 27001 |
| | | | | ■ | | | IT-Compliance |
| | | | | ■ | | | IT-Forensik |
| | ■ | ■ | | ■ | ■ | | IT-Sicherheitsbeauftragter (ITSB) |
| | ■ | ■ | | ■ | ■ | | IT-Sicherheitsstrategie |
| | ■ | | | ■ | | | Konfiguration |
| | | | | ■ | | | Mobile Device Management |
| | ■ | | ■ | ■ | | | Monitoring |
| | | | | ■ | | | Network Access Control (NAC) |
| ■ | | | | ■ | | | Network Management System (NMS) |
| | | | | ■ | | | Notfallmanagement |
| | ■ | | | ■ | | | Outsourcing |
| | ■ | | | ■ | | | Passwortrichtlinie |
| | ■ | ■ | | ■ | | | PDCA-Zyklus |
| | | | | ■ | ■ | | Penetrationstests |
| | | | | | ■ | | Physikalische Sicherheit |
| | | | | ■ | ■ | | Projektmanagement |
| | | ■ | | ■ | ■ | | Prozessoptimierung |
| ■ | ■ | | | | | | Redundanz |
| | ■ | | | | | | Remote Access |
| | ■ | | | | | | Reporting |
| | ■ | | | ■ | ■ | | Risikomanagement |
| | ■ | | | ■ | | | Rollenmanagement |
| | | | | ■ | | | Schutzbedarfsermittlung |
| ■ | | | | ■ | ■ | | Security Awareness |
| | | | | ■ | | | Security Information and Event Management (SIEM) |
| | | | | ■ | | | Security Level Management (SLM) |
| | ■ | | | ■ | | | Server Bereitstellung |
| ■ | ■ | | | ■ | | | Service Level Agreement (SLA) \| 24/7 Service |
| ■ | | | | ■ | ■ | | Software Security |
| | | | | ■ | | | Spam-Abwehr |
| ■ | | | | | | | Überspannungsschutz |
| | ■ | | | | | | Unterbrechungsfreie Stromversorgung |
| | ■ | | | ■ | | | Update- und Patch-Management |
| ■ | ■ | | | ■ | | | Verschlüsselung / Kryptographie |
| | | | | ■ | | | Virenschutz |
| | | | | ■ | | | Vulnerability Management |
| ■ | | ■ | | ■ | | | Webinare |
| ■ | | ■ | | | | | Weiterbildung + Coaching |
| | | ■ | | ■ | ■ | | Zertifizierungen |

# TÜV Rheinland: Kompetenz in Informationssicherheit für die Energiewirtschaft

**Die Energiewirtschaft gehört zu den Branchen, die der digitale Wandel seit einigen Jahren vor besondere Herausforderungen stellt. Neue Geschäftsmodelle, wie z.B. virtuelle Kraftwerke, setzen die Nutzung verteilter und in Teilen öffentlicher, cloudbasierter Strukturen voraus. Zugleich müssen Echtzeitsysteme wie Netzleitsysteme oder die Steuerung von Umspannwerken mit einer nahezu 100-prozentigen Ausfallsicherheit betrieben werden. TÜV Rheinland hat umfassende Erfahrung in der ganzheitlichen Absicherung Kritischer Infrastrukturen.**

Ohne IT und deren zunehmender Vernetzung ist der Betrieb kritischer Infrastrukturen (KRITIS) heute nicht mehr denkbar. Zugleich bergen die digitalen Infrastrukturen weitere Angriffsflächen und steigern die Verwundbarkeit neuralgischer Systeme z. B. der Strom- oder Wasserversorgung gegenüber immer ausgeklügelteren Cyberangriffen wie etwa gezielten komplexen Angriffen (Advanced Persistent Threats, APT).

Neben neuen Technologien und sich wandelnden Gefährdungspotenzialen sieht sich die Energiebranche auch verschärften regulatorischen Anforderungen gegenüber: Das IT-Sicherheitsgesetz erwartet von Unternehmen bis Januar 2018, einen angemessenen IT-Schutz „gemäß dem aktuellen Stand der Technik" zu implementieren, den sie auch nachweisen müssen.

Die Erfahrung von TÜV Rheinland zeigt: Kritische Infrastrukturen in Deutschland und Europa sind gegen die neuen Angriffsszenarien oft nur rudimentär geschützt. Entweder wird Informationssicherheit nicht systematisch gemanagt oder die technische Infrastruktur zum Betrieb der Netze wird noch häufig getrennt von der IT betrachtet. Ganzheitlicher Schutz gegenüber Cyber-Angriffen wird jedoch erst möglich, wenn die technische IT und die Office-IT näher aneinanderrücken und Synergien aus den beiden Welten genutzt werden. Zum nachhaltigen Gelingen eines ganzheitlichen Schutzes sind hierbei vor allem die unterschiedlichen Anforderungen der einzelnen Bereiche zu berücksichtigen. Darin kann TÜV Rheinland als führender unabhängiger Dienstleister im Bereich Informationssicherheit in Deutschland Unterstützung leisten. Darüber hinaus verbindet er die Kompetenz in Informationssicherheit mit einer langjährigen Expertise für Sicherheit in der Industrie.

Die Experten haben umfassende Erfahrung in der Absicherung kritischer Infrastrukturen und eine umfangreiche Marktkenntnis in Bezug auf nachhaltige und skalierbare Sicherheitslösungen. Die Aktivitäten reichen von der Evaluierung des aktuellen Informationssicherheitsniveaus über die Unterstützung bei der Entwicklung und Implementierung von Sicherheitslösungen und Managementsystemen bis hin zu deren kontinuierlichem Betrieb.

## TÜV Rheinland hat Stadtwerke im Fokus

Stadtwerke tragen eine hohe gesellschaftliche Verantwortung, da sie das Rückgrat der Grundversorgung in Deutschland bilden. Sie müssen sich mit Themen wie dem neuen IT-Sicherheitsgesetz, KRITIS, Informationssicherheitsmanagementsystemen (ISMS), ISO/IEC 27001, ISO/IEC 27002, ISO TR 27019, dem Smart-Meter-Gateway-Administrator (SMGWA – Technische Richtlinie TR-03109) oder dem IT-Sicherheitskatalog der Bundesnetzagentur auseinandersetzen. Viele Stadtwerke betreten hier Neuland und haben sich den neuen, in der Regel noch unbekannten Aufgaben zu stellen.

Verantwortliche stehen u. a. vor folgenden Fragen:

- Was steht hinter den Begriffen und Themen der regulatorischen Anforderungen?
- Welche Auswirkungen haben die Gesetze und Standards auf unser Geschäft und unsere Organisation?
- Wo stehen wir aktuell und was müssen wir noch unternehmen?
- Mit welchen Kosten müssen wir für die Umsetzung von IT- und Informationssicherheitsmaßnahmen rechnen?
- Wie können wir die Themen effizient und pragmatisch angehen?
- Welche Mehrwerte lassen sich aus IT- und Informationssicherheitsmaßnahmen generieren – neben der Erfüllung der gesetzlichen Anforderungen?

### Unsere Leistungen und Services auf einen Blick:

**Informationssicherheitsmanagement**

- Strategische Informationssicherheit
- Analyse, Konzeption, Implementierung von ISMS
- Business Continuity Management
- IT-Notfallmanagement
- Managed Services

**Konzeption von IT-Sicherheit**

- Beratung und Umsetzung gesetzlicher Vorgaben (Governance, Risk & Compliance)
- Schutz vor gezielten Angriffen und Sabotage

**Überprüfung des IT-Sicherheitsniveaus**

- Technische Prüfungen und Sicherheitsaudits
- Penetrationstests für Applikationen und Systeme

## Der Weg zu einer nachhaltigen IT- und Informationssicherheitsstrategie: die modulare Methode

Aus der Erfahrung heraus empfiehlt TÜV Rheinland eine mehrstufige, modulare Herangehensweise:

- Durch gezielte ISMS-Basis-Workshops wird allen Beteiligten das Thema ISMS näher gebracht und die erforderliche Transparenz für das weitere Vorgehen geschaffen.

- Über qualifizierte ISMS-Gap-Analysen wird der aktuelle Stand der Informationssicherheit erhoben, der für die Konzeption und Implementierung eines ISMS Voraussetzung ist.
- Die Konzeption und Implementierung eines ISMS sowie der kontinuierliche Betrieb runden die mehrstufige Vorgehensweise ab.

Im Folgenden sind die Themen ISMS-Basis-Workshop und ISMS-Gap-Analyse beschrieben. Weitere Informationen zur Konzeption und Implementierung eines ISMS finden sich unter **www.tuv.com/isms.**

## Der ISMS-Basis-Workshop: ein Fundament schaffen durch Grundlagen-Wissen

Im Rahmen unseres ISMS-Basis-Workshops erhalten die für die IT verantwortlichen Mitarbeiter das Wissen, um die notwendigen Entscheidungen zu treffen und die richtigen Schritte einzuleiten:

- Grundlagen zur Definition eines Anwendungsbereiches (Scopes)
- Definition der erforderlichen Aktivitäten und Priorisierung relevanter Themen
- Kenntnisse im Bereich der Managementsysteme sowie des Risikomanagements
- Praxislösungen und Beispiele aus langjähriger Branchenerfahrung

## Die ISMS-Gap-Analyse: die Roadmap zu mehr Informationssicherheit und Compliance auf allen Ebenen

Die ISMS-Gap-Analyse dient der Identifikation des aktuellen Umsetzungsstandes zur Informationssicherheit. Neben der ISO 27001 lassen sich auch die Anforderungen der ISO TR 27019, des IT-Sicherheitskataloges gemäß § 11 Absatz 1a Energiewirtschaftsgesetz und bei Bedarf weitere Standards wie z. B. die TR-03109 für den SMGWA, einbeziehen. Die fachliche Bewertung der Abweichungen enthält Aussagen zu Kritikalität, Relevanz sowie entsprechende Empfehlungen.

Die Gap-Analyse umfasst

- eine Dokumentenanalyse
- Vor-Ort-Überprüfungen
- die Identifikation und Bewertung vorhandener Gaps inkl.
- einem aussagekräftigen Bericht und einer Präsentation vor den Entscheidern des Stadtwerkes.

Übrigens ist TÜV Rheinland auch in der Forschung rund um die Sicherheit kleinerer und mittlerer Energieversorger engagiert, unter anderem als einer von fünf Verbundpartnern im Forschungsprojekt SIDATE, einem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungsprojekt. **www.tuv.com/sidate**

SIDATE hat das Ziel, Werkzeuge und Konzepte zu entwickeln, die dabei helfen, die IT-Sicherheit kleiner und mittlerer Betreiberfirmen zu verbessern. Für TÜV Rheinland liegt ein besonderes Augenmerk auf der Praxistauglichkeit der Werkzeuge und Konzepte, die unabhängig von wirtschaftlichen, organisatorischen und personellen Besonderheiten in den Stadtwerken anwendbar sein sollen.

Mehr Informationen unter **www.tuv.com/informationssicherheit** und **www.tuv.com/referenzen**

TÜVRheinland®
Genau. Richtig.

**TÜV Rheinland i-sec GmbH**
Am Grauen Stein
51105 Köln
Telefon: +49 221 / 806-0
E-Mail: service@i-sec.tuv.com
Web: www.tuv.com/informationssicherheit