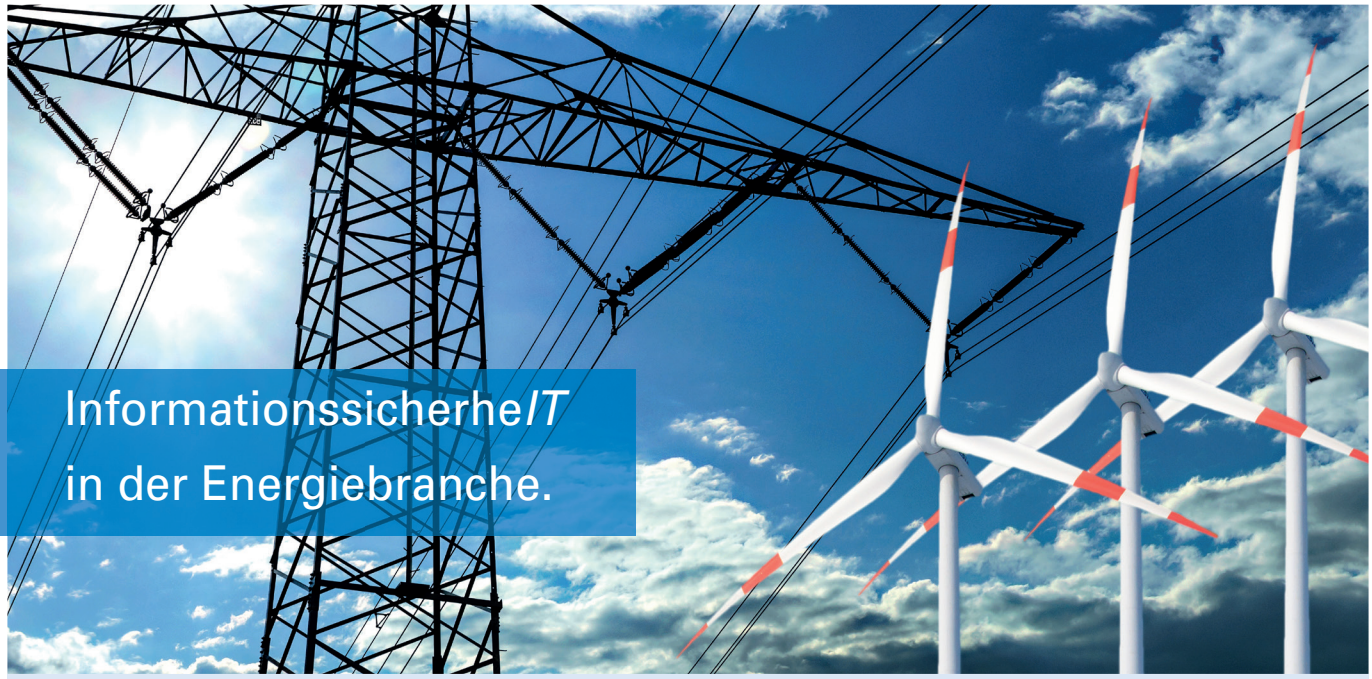


Informationssicherhe*IT* in der Energiebranche.

Herausforderungen der Branche

Die Gefahr von Cyber-Angriffen wächst. Attraktive Ziele für Hacker sind vor allem neuralgische Systeme wie die Strom- oder Wasserversorgung.

Energie- und Datennetze werden heute digital gesteuert. Der Vernetzungsgrad und die Datenmenge wachsen ständig – somit auch die Verwundbarkeit der IT-Infrastruktur durch Cyber-Attacken.

Die Infrastruktur im Energiesektor unterliegt aktuell einem starken Wandel. In den Bereichen des Netzbetriebes und der Netzführung kommen neben den ehemals proprietären Systemen immer mehr Standard-IT-Systeme und Technologien zum Einsatz, wie sie in den Office-IT-Bereichen schon lange genutzt werden. Zusätzlich entstehen neue Geschäftsmodelle, wie z.B. virtuelle Kraftwerke, welche eine Nutzung verteilter und in Teilen öffentlicher Strukturen voraussetzen.

Schutz vor Cyber-Angriffen

Neben den Herausforderungen in Bezug auf neue Technologien, sich wandelnde Gefährdungspotenziale sowie mögliche Angreifer stellen vor allem auch die regulatorischen Anforderungen und Standards neue Aufgaben an die Energiebranche.

Unsere Erfahrung zeigt, dass kritische Infrastrukturen in Deutschland und Europa gegen die neuen Angriffsszenarien oft nur rudimentär geschützt sind. Entweder wird Informationssicherheit nicht systematisch gemanaged oder die technische Infrastruktur zum Betrieb der Netze wird noch häufig getrennt von der IT betrachtet.

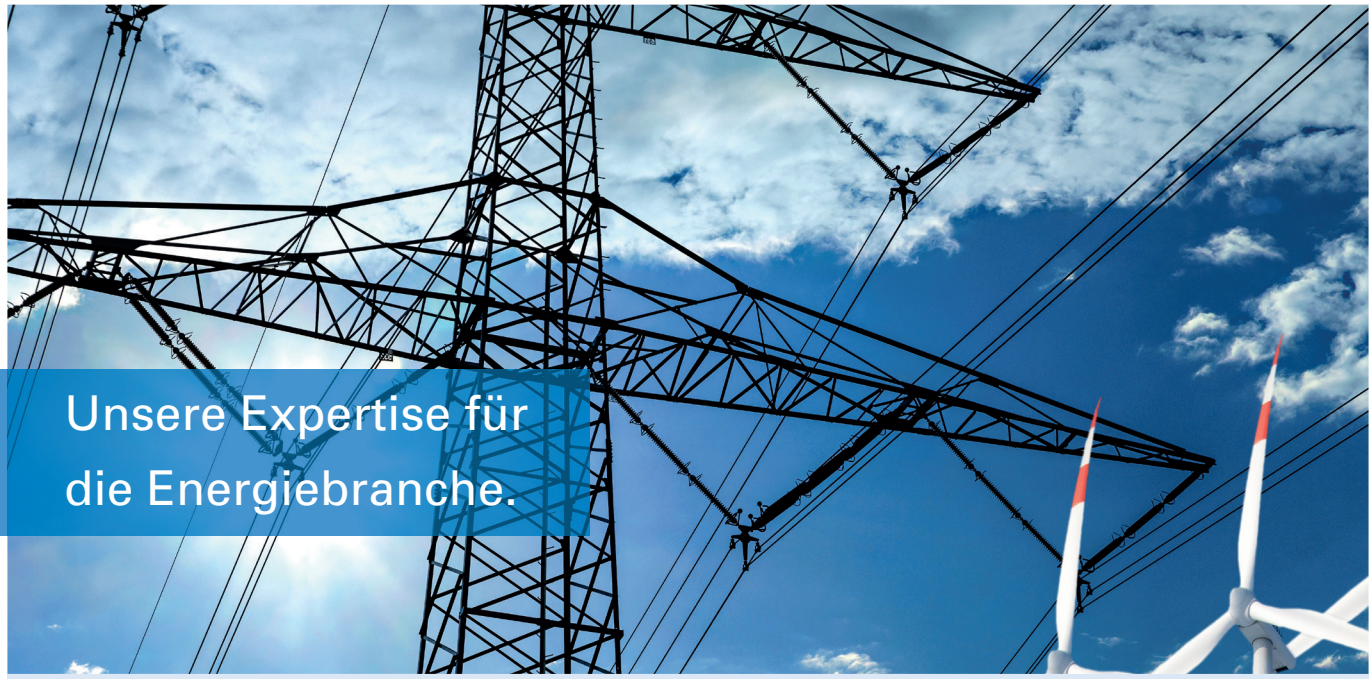
Ganzheitlicher Schutz gegenüber Cyber-Angriffen wird erst möglich, wenn die technische IT und die Office-IT näher aneinander rücken und Synergien aus den beiden Welten genutzt werden. Zum nachhaltigen Gelingen eines ganzheitlichen Schutzes sind hierbei vor allem die unterschiedlichen Anforderungen der einzelnen Bereiche zu berücksichtigen.

Potenzielle Einfallstore für Hacker

- Websites
- Kommunikations-schnittstellen
- Mail-Infrastruktur
- Scada-Systeme
- Unzureichendes Rollen- und Berechtigungsmanagement
- Mangelnde IT-Sicherheits-Updates
- Fehlende Dokumentation der IT-Architektur

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.



Unsere Expertise für die Energiebranche.

Vorteile eines professionellen ISMS

- Wirksame Kontrolle von IT-Risiken durch systematisches Risiko-Management
- Schwachstellen aufdecken und Zusatzrisiken minimieren
- Versorgungssicherheit als hohes gesellschaftliches und schützenswertes Gut gewährleisten
- Identifikation angemessener und wirtschaftlicher Maßnahmen zur Risikoreduktion
- Nachweislicher Betrieb eines ISMS gegenüber Dritten, wie z.B. Aufsichtsbehörden, Prüfern, Kunden und Partnern

TÜV Rheinland unterstützt Unternehmen der Energiebranche bei der systematischen Erhöhung der Informations- und IT-Sicherheit auf allen Ebenen. Hierbei reichen die Aktivitäten von der Evaluierung des aktuellen Informationssicherheitsniveaus über die Unterstützung bei der Entwicklung und Implementierung von Sicherheitslösungen und Managementsystemen bis hin zu deren kontinuierlichem Betrieb.

Unsere Services und Lösungen

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

Kriterienkatalog zur Sicherheit von EVUs

TÜV Rheinland hat gemeinsam mit Partnern einen Kriterienkatalog für Energieversorgungsunternehmen entwickelt. Fragen Sie uns!

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806-4050
Fax +49 221 806-2295
service@i-sec.tuv.com

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.