Informationssicherhe*IT* für Stadtwerke.

Herausforderungen der Branche

Der aktuelle Technologiewandel sowie neue regulatorische Anforderungen, wie z.B. das IT-Sicherheitsgesetz, stellen Stadtwerke zunehmend vor neue Herausforderungen. Vor allem in den Bereichen des Netzbetriebes und der Netzführung kommen neben den ehemals proprietären Systemen verstärkt Standard-IT-Systeme und Technologien zum Einsatz, wie sie in der Office-IT schon lange genutzt werden.

Der Technologiewandel ist jedoch mit Risiken verbunden. Zunehmende Cyber-Angriffe auf Infrastrukturen der nationalen Grundversorgung, wie z.B. Energie haben den Gesetzgeber zum Handeln veranlasst: Im Rahmen der Digitalen Agenda rücken der Schutz und die Sicherheit von IT-Systemen und Diensten in den Fokus.

Regulatorische Anforderungen

Stadtwerke tragen eine hohe gesellschaftliche Verantwortung, da sie das Rückgrat der Grundversorgung in Deutschland bilden.

Sie müssen sich nun 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.

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

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?

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.

Unsere Expertise für Stadtwerke.

Nachhaltige IT- und Informationssicherheitsstrategie

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. Details zur Konzeption und Implementierung eines ISMS finden Sie unter www.tuv.com/isms.

ISMS Basis-Workshop

Im Rahmen unseres ISMS Basis-Workshops erhalten Ihre 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.

ISMS Gap-Analyse

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

IT-Sicherheitsgesetz, KRITIS, ISO/IEC 27001, ISO/IEC 27002, ISO TR 27019 sind Neuland für Sie? Wir haben den Überblick! Gerne beraten und unterstützen wir Sie beim Aufbau eines passgenauen ISMS. Fragen Sie uns!

TÜV Rheinland i-sec GmbH
Am Grauen Stein, 51105 Köln
Tel. +49 221 806-0
service@i-sec.tuv.com

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.