

NIS2-Konformität wirtschaftlich umsetzen

[20.10.2026] Im Rahmen der NIS2-Richtlinie sind auch kleinere Stadtwerke dazu verpflichtet, verbindliche Anforderungen an die Cyber-Sicherheit, das Risikomanagement und die Meldeprozesse umzusetzen. Aufgrund fehlender Security-Experten und begrenzter IT-Budgets ist das jedoch eine große Herausforderung.

Mit der nationalen Umsetzung von NIS2 im Dezember 2025 wurde der Kreis der betroffenen Unternehmen und Einrichtungen deutlich erweitert. Neben den klassischen KRITIS-Betreibern zählen nun auch zahlreiche kleinere Energieversorger, Netzbetreiber, Wasserbetriebe und kommunale Dienstleister mit mindestens 50 Beschäftigten oder einem Jahresumsatz von zehn Millionen Euro dazu. Gleichzeitig werden die Anforderungen an die Cyber-Resilienz dieser Einrichtungen wesentlich strenger und die Sanktionen verschärft.

NIS2 verlangt unter anderem dokumentierte Konzepte für Risikoanalysen und Informationssicherheit, eine durchgängige Netzwerk- und Systemüberwachung, funktionierende Maßnahmen zur Bewältigung und Meldung von Ereignissen sowie abgesicherte Zugriffs- und Berechtigungskonzepte. In der Praxis verfügen allerdings gerade kleinere und mittlere Stadtwerke oft über historisch gewachsene IT- und OT-Umgebungen mit unzureichenden Sicherheitsstandards und unterschiedlichen Insellösungen. Zudem fehlen häufig geeignete Möglichkeiten zur zentralen Überwachung, Korrelation und Analyse sicherheitsrelevanter Daten aus unterschiedlichen Systemen.

Nur Minderheit ist NIS2-Ready

Das stellt viele kommunale Versorgungsbetriebe vor die anspruchsvolle Aufgabe, komplexe Anforderungen zeitnah zu erfüllen, ohne den laufenden Betrieb zu überlasten. Zwar haben einige Betriebe bereits erste NIS2-Vorgaben umgesetzt, doch Schätzungen und Umfragen aus der Branche gehen davon aus, dass derzeit nur eine Minderheit der kleineren und mittleren Einrichtungen tatsächlich NIS2-Ready ist.

Die Einhaltung der Richtlinie wird durch ein strukturelles Problem erschwert: Der Fachkräftemangel betrifft kleinere und mittlere Stadtwerke in besonderem Maße. Tiefgreifende Security-Expertise, rund um die Uhr verfügbare Spezialisten oder gar ein eigenes Security Operations Center (SOC) sind für sie wirtschaftlich und personell kaum realisierbar. Damit stecken viele kommunale Unternehmen in einem Dilemma, denn selbst wenn die notwendigen Maßnahmen bekannt sind, lassen sie sich mit den vorhandenen Ressourcen nur schwer umsetzen.

Um der Richtlinie umfassend gerecht zu werden, reicht es nicht aus, nur einzelne Aspekte zu betrachten und bestimmte Komponenten nachzurüsten. Stadtwerke benötigen eine zentrale Sicherheitsüberwachung, die sämtliche Ereignisse aus unterschiedlichen Systemen konsolidiert, automatisiert bewertet und gezielte Eskalationsprozesse anstößt. Wichtige Bestandteile sind ein zuverlässiges Log-Management, um Bedrohungen schneller und zuverlässiger zu erkennen, sowie ein intelligentes Alarmierungs- und Monitoring-System, über das die Informationen automatisch und ohne Zeitverlust an die richtigen Stellen gelangen.

Dabei darf die OT-Sicherheit nicht vernachlässigt werden, denn OT- und IT-Umgebungen sind in vielen Versorgungsbetrieben eng miteinander verzahnt. Angriffe auf die Office-IT können somit direkte Konsequenzen für Netzleitstellen, Steuerungssysteme oder technische Anlagen haben und die Versorgungssicherheit unmittelbar beeinträchtigen. Aus diesem Grund berücksichtigt die NIS2-Richtlinie ausdrücklich auch Risiken in OT-Umgebungen und fordert angemessene Schutzmaßnahmen. Oft stellt die strukturierte Umsetzung der erforderlichen Maßnahmen Stadtwerke vor die größten Herausforderungen. Ein einfacher Handlungsfahrplan kann dabei helfen, diese zu bewältigen und zu beschleunigen.

Status quo bewerten

Zu Beginn sollte eine ehrliche Bestandsaufnahme der Ist-Situation stehen. Welche Anforderungen erfüllen die IT- und OT-Umgebung bereits, wo bestehen Schwachstellen? Welche Prozesse und Maßnahmen fehlen vollständig? Wer auf Nummer sicher gehen möchte, beauftragt einen externen Dienstleister mit einer Reifegradanalyse, die die Sicherheitslage genau untersucht.

Gerade bei kleineren Versorgern sind finanzielle und personelle IT-Ressourcen knapp und spezialisiertes Know-how ist nicht ausreichend vorhanden. Umso entscheidender ist es deshalb, zunächst die kritischen Systeme und Prozesse zu identifizieren und Mindestmaßnahmen zu definieren, die die Cyber-Sicherheit mit verhältnismäßig geringem Aufwand erheblich erhöhen. Dazu gehören neben Log-Management und Monitoring unter anderem automatisiertes Zertifikatsmanagement, Multi-Faktor-Authentifizierung sowie professionelles Patch- und Schwachstellenmanagement. Wichtig ist: Auch die NIS2-Richtlinie schreibt keine lückenlose Absicherung vor, sondern verlangt praktikable und verhältnismäßige Maßnahmen.

Zusammenarbeit mit externen Partnern

Gerade für kleinere Versorger ist der Aufbau eines eigenen Security-Teams oft weder personell noch wirtschaftlich machbar. Durch die Zusammenarbeit mit einem externen Partner können sie anspruchsvolle Aufgaben gezielt in erfahrene Hände geben und profitieren so von umfassender Expertise, einem 24/7-Schutz und einem professionellen SOC, ohne eigene Ressourcen zu binden. Cybersecurity ist jedoch kein rein technisches Thema. Um Schwachstellen bei der täglichen IT-Nutzung durch Mitarbeitende zu vermeiden, spielt auch Security Awareness eine wichtige Rolle. Mit klaren Sicherheitsrichtlinien, Sensibilisierung und gezielten Schulungen können Betriebe Risiken nachhaltig reduzieren.

Die Zeit drängt. Wer jetzt noch zögert, die NIS2-Anforderungen mit Nachdruck voranzutreiben, riskiert nicht nur erhebliche Sanktionen, sondern setzt auch Geschäftsführer und Vorstände der persönlichen Haftung aus. Mit praktikablen und wirtschaftlich tragfähigen Lösungen sowie der gezielten Unterstützung externer Security-Spezialisten sind jedoch auch kleine und mittlere Versorger in der Lage, die erforderlichen Maßnahmen in überschaubaren Projektphasen und trotz eingeschränkter Ressourcen umzusetzen. Damit legen sie zugleich den Grundstein für eine resiliente und effiziente Sicherheitsstruktur, die nachhaltig gegen Cyber-Risiken schützt.

()

• www.iqsol.biz

Dieser Beitrag ist im Schwerpunkt Cyber-Sicherheit der Ausgabe September/Oktober 2026 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, Cyber-Sicherheit, iQSol, NIS2