

NIS2: Gebäudeautomation bei Versorgern besser absichern

Artikel vom **13. Oktober 2026**

Gebäude- + Grundstücksmanagement

Kommunale Versorger müssen im Zuge von NIS2 und KRITIS-Dachgesetz auch die Gebäudeautomation stärker schützen. Iconag zeigt, warum vernetzte Steuerungen, Gateways und Zähler eine kritische Schnittstelle zwischen IT und OT bilden können.



Christian Wild verweist auf die Bedeutung abgesicherter Gebäudeleittechnik für kommunale Versorgungsbetriebe. (Bild: ICONAG)

Die Versorgungssicherheit mit Strom, Wärme und Wasser hat in Deutschland einen hohen Stellenwert. Während Umspannwerke und Leitstände häufig aufwendig geschützt werden, bleibt die Gebäudeautomation in Verwaltungs- und Betriebsgebäuden von Energieversorgern nach Einschätzung von ICONAG-Leittechnik GmbH oft weniger stark im Fokus. Mit der NIS2-Richtlinie und dem KRITIS-Dachgesetz rücken diese Schnittstellen nun stärker in die Regulierung. »In modernen Versorgungsbetrieben

wachsen IT und Operational Technology (OT) immer stärker zusammen. Wenn Systeme der Gebäudeautomation ungesichert an IP-Netze oder Cloud-Dienste angebunden sind, entsteht eine kritische Flanke«, erläutert Christian Wild, Experte für Gebäudeleittechnik und Geschäftsführer. »Über kompromittierte Gebäudeleitsysteme können sich Angreifer im schlimmsten Fall Zugang zu sensiblen Unternehmensnetzen verschaffen.«

Bestandsaufnahme als Grundlage Für die Umsetzung der geforderten Schutzmaßnahmen empfiehlt Wild kommunalen Versorgungsbetrieben ein strukturiertes Vorgehen. Am Anfang steht eine vollständige Bestandsaufnahme aller vernetzten Steuerungen, Gateways und Zähler auf der Gebäudeebene. Erst auf dieser Basis lassen sich Risiken bewerten und geeignete technische sowie organisatorische Maßnahmen ableiten. Besonders wichtig sind die Netzübergänge zwischen Gebäudeleittechnik und Unternehmens-IT. Sie sollten über definierte Übergangszonen und strenge Zugriffskontrollen abgesichert werden. So lässt sich begrenzen, welche Systeme miteinander kommunizieren dürfen und welche Nutzer oder Dienste Zugriff erhalten.

Prozesse für Updates, Backups und Rollenrechte Da Komponenten in der operativen Gebäudetechnik oft über viele Jahre betrieben werden, braucht ein tragfähiges Sicherheitskonzept feste Prozesse. Dazu zählen regelmäßige Firmware- und Software-Updates, Notfall-Backups sowie eine klare Verwaltung von Rollenrechten. Diese Maßnahmen sollen dazu beitragen, die Gebäudeautomation dauerhaft in die Sicherheitsarchitektur kommunaler Betriebe einzubinden. »Ein modernes Stadtwerk ist nur so stark wie das schwächste Glied in seinen Steuerungssystemen«, betont Wild. »Wer die OT-Sicherheit frühzeitig in die Betriebsabläufe integriert, erfüllt nicht nur die NIS2-Auflagen, sondern sichert die eigene Resilienz nachhaltig ab.« Das Unternehmen aus Idar-Oberstein entwickelt seit 1996 herstellernerneutrale Software für Gebäudeleittechnik und Energiemanagement. Die modulare »B-CON Software-Suite« integriert heterogene Systemlandschaften mit BACnet, Modbus, KNX, M-Bus, OPC und offenen Schnittstellen. Auch die Zusammenarbeit mit CAFM-, ERP- und Drittsystemen wird unterstützt.

Hersteller aus dieser Kategorie
