

Sicherheit für die Trinkwasserversorgung

Eine Störung oder gar der Ausfall der Trinkwasserversorgung über ein größeres Gebiet bzw. über einen längeren Zeitraum führt zu massiven Auswirkungen auf die Bevölkerung. Daher zählt die Trinkwasserversorgung zu den Kritischen Infrastrukturen (KRITIS).



IPS VideoManager vereint Videomanagement und Videoanalyse aus einem Guss und unterstützt die Leitstelle im Alarm- und Ereignisfall. Foto: Securiton Deutschland/ Gorodenkoff-stock.adobe.com

In Deutschland gibt es über 5.000 Wasserversorgungsunternehmen, sowohl größere Betreiber als auch überwiegend kleinere Eigenbetriebe seitens Kommunen. Die Qualitätsstandards sind sehr hoch, für Verantwortliche stellt sich daneben auch die Frage: Ist die Trinkwasserversorgung ausreichend vor möglichen kriminellen Angriffen geschützt?

Die fortschreitende Digitalisierung macht auch die Steuerung von Trinkwasser-Infrastrukturkomponenten über die Ferne möglich. Aber nicht nur Betreiber selbst, auch ein unberechtig-

ter Personenkreis mit entsprechenden Fähigkeiten kann dadurch auf die Systeme einwirken und sie im schlimmsten Fall sabotieren. Die letzten Jahre haben gezeigt, dass solche Risiken bestehen und das Thema IT-Sicherheit im Bereich der Kritischen Infrastrukturen in den Fokus rücken muss. Entsprechende Gesetze und Verordnungen, sowohl das IT-Sicherheitsgesetz (IT-SiG 2.0) als auch die BSI-Kritisverordnung (BSI-KritisV), wurden verabschiedet und sind seit dem 1. Mai 2023 bindend. Das KRITIS-Dachgesetz wurde im Jahr 2022 verabschiedet, der Refe-

rentenentwurf 2023 in die einzelnen Resorts verteilt. Mit einem rechtsgültigen Gesetz wird noch in der Wahlperiode gerechnet.

Trinkwassersicherheit als primäres Ziel

Zu den möglichen Gefahren zählen beispielsweise das Einbringen von schädlichen Substanzen in den Wasserkreislauf oder die Sabotage der für den Betrieb erforderlichen Komponenten. Das Verhindern solcher Absichten und ande-

rer Anschläge auf das Trinkwasserversorgungsnetz haben daher höchste Priorität. Falls dennoch ein unberechtigter Zutritt erfolgt, müssen dies Frühwarnsysteme anzeigen, sodass unmittelbar Interventionsmaßnahmen eingeleitet werden können. Nicht zuletzt entstehen auch für die Wiederinbetriebnahme von sabotierten oder beschädigten Komponenten oft sehr hohe Kosten, welche durch ein schlüssiges Sicherheitskonzept verringert oder gar vermieden werden können.

Passgenaue Sicherungsmaßnahmen

Hochfunktionale Videosicherheitssysteme und Gefahrenmeldeanlagen werden eng miteinander verzahnt und gewährleisten eine reibungslose Detektion sowie eine zuverlässige Alarmierung im Ereignisfall. Basierend auf den einschlägigen Normen und Richtlinien für Gefahrenmeldeanlagen wird der Sicherungsumfang für die Überwachung von Infrastrukturelementen und Gebäuden festgelegt. Unter Berücksichtigung der örtlichen Gegebenheiten, der Betriebsabläufe und der zu überwachenden Objekte selbst wird anhand des Gefährdungspotenzials und der Risikoanalyse gemeinsam mit dem Betreiber ein individuelles Sicherheitskonzept erarbeitet. Aufgrund der unterschiedlichen Anforderungen an die Schutzziele kommen teils auch spezielle Detektionstechniken zum Einsatz. Nur so kann ein reibungsloser und störungsfreier Betrieb gewährleistet werden.

Sicherheitskonzepte sehen eine automatisierte Erfassung von Unregelmäßigkeiten bereits an den Grundstücksgrenzen vor. Mittels intelligenter Videoanalyse erfolgt bei unerlaubtem Eindringen eine automatische Alarmauslösung, welche an eine betreiberinterne und ständig besetzte Stelle oder auch an eine externe übergeordnete Notruf- und Serviceleitstelle (NSL) weitergeleitet wird. Der Alarmauslösegrund ist in jedem Fall seitens des kamerabasierten Systems für das Betriebspersonal sofort ersichtlich. Durch eine gezielte Täteransprache besteht gleichzeitig die Möglichkeit, die Eindringlinge anzusprechen und möglicherweise vom weiteren Vorhaben abzuhalten. Ist dies nicht der Fall, können zusätzliche Kameras eine systemseitige Täterverfolgung auf dem Gelände übernehmen. Diese Beobachtung und Verfolgung dient auch der Rekonstruktion der Geschehnisse und der Beweissicherung.

Mit Hilfe von elektronischen Sicherheitskomponenten, beispielsweise Überwachungskameras, können seitens des zuständigen Betriebspersonals die erforderlichen Interventionsmaßnahmen und gleichzeitig die Objektsicherungsmaßnahmen eingeleitet werden. Im Einzelnen kann es sich dabei um interne Maßnahmen handeln, wie die Abschottung von Versorgungsleitungen. Oder es können externe Maßnahmen wie Strafverfolgungen eingeleitet werden. Zusätzlich zur Alarmierung werden die Videobilddaten automatisch gesichert und kryptographisch verschlüsselt (Beweissicherung). Die Dauer der Aufzeichnung und Speicherung der Videobilddaten erfolgen kundenspezifisch und werden im Vorfeld festgelegt.

Damit das Sicherheitspersonal bzw. die Leitebene eine komplette Übersicht der überwachten Bereiche hat, werden alle gesicherten Objekte eines Trinkwasserbetreibers miteinander vernetzt und zentral auf einem Bedienarbeitsplatz aufgeschaltet. Von hier aus kann dann bequem und übersichtlich

der Zustand des Gesamtsystems und auch eine Alarmbearbeitung erfolgen.

Sicherheitskonzept für ein Gesamtsystem

Neben den benannten Systemlösungen sollten je nach spezifischen Anforderungen und Gegebenheiten für eine Rundumabsicherung weitere Technologien aus den Bereichen Zutrittskontrolle, Brandmeldung, universelles Alarmmanagement sowie mobiler Objektschutz und in der heutigen Zeit auch Drohnensicherheit mit in Betracht gezogen werden. Die Möglichkeiten sind vielfältig und verfolgen immer das Ziel, integrative Systemtechnologien in einem umfassenden Gesamtsystem zu vereinen. Nur ein spezifisches und durchdachtes Sicherheitskonzept, abgestimmt auf die jeweils vorherrschenden Gegebenheiten der Organisationen, erfüllt die Sicherheitsanforderungen für solche Hochsicherheitsbereiche.

www.securiton.de