PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6105 di Lunedì 22 giugno 2026

# Reti idriche e cybersecurity: infrastrutture critiche a rischio

***La crescente digitalizzazione delle reti idriche espone acquedotti e sistemi fognari a nuovi rischi informatici. Serve un approccio strutturato alla sicurezza per prevenire attacchi e garantire continuità del servizio.***

Le reti idriche si dividono in due grandi categorie, rispettivamente le reti idriche di acqua potabile e le reti idriche di acqua di rifiuto. Entrambe meritano un'estrema attenzione, per metterle in grado di fronteggiare possibili attacchi informatici, che diventano sempre più potenzialmente gravi, quanto più l'informatica entra nella gestione di queste reti.

Recentemente gli specialisti di sicurezza informatica hanno messo in evidenza come la crescente informatizzazione delle reti idriche apra un varco per possibili attacchi informatici. Questi attacchi possono portare ad una indisponibilità delle reti idriche di acque potabili, con conseguenze facilmente immaginabili, come pure la indisponibilità di reti idriche di acque di rifiuto, con conseguenze potenzialmente altrettanto gravi.

Gli esperti hanno messo in evidenza come questi attacchi possano essere portati sia da hackers, sia da organizzazioni criminali, che chiedono un riscatto per poter ripristinare la funzionalità delle reti informatiche.

Al proposito, chi scrive in passato ha più volte offerto assistenza a gestori di rete idriche, in Italia, quando questi gestori si sono resi conto che ormai le reti informatiche controllano le valvole, le pompe, gli accessi ad aree riservate, gli erogatori di sostanze chimiche, che possono essere utilizzate per la bonifica dell'acqua potabile o per la parziale neutralizzazione degli aspetti negativi delle acque di rifiuto.

Nella grande maggioranza, queste reti sono gestite da aziende, che sono sul campo da decine di anni e che non sempre si sono preoccupate di aggiornare le conoscenze del personale addetto alla gestione delle reti, sottolineando i rischi specifici legati all'informatica, usata in maniera sempre più allargata.



Ad esempio, nel 2024 gli ispettori del General accounting Office, negli Stati Uniti, hanno potuto verificare che la Environmental Protection Agency non aveva fatto alcuna analisi di rischio informatico, riferito alla gestione delle reti.

La raccomandazione di chi scrive è che tutti i gestori di reti di acque chiare ed acque scure sviluppino, od eventualmente aggiornino, un'analisi di rischio informatico, che metta in evidenza le varie tipologie di attacchi e, cosa ancora più importante, le

possibili conseguenze degli attacchi sul servizio reso alla popolazione.

Oggi ancora ci si preoccupa più del fatto che una frana possa interrompere un acquedotto di acqua potabile, piuttosto che un attacco informatico possa bloccare le pompe, che alimentano le torri piezometriche, che permettono di offrire alla cittadinanza serbatoi di acqua potabile in pressione.

È ben vero che le normative sulle reti di acqua potabile in Italia sono state aggiornate con il D.Lgs. 102/2025, che introduce controlli più rigorosi e nuovi limiti per i PFAS e il TFA. Il decreto tuttavia si concentra più su aspetti di qualità delle acque, piuttosto che sulla prevenzione di attacchi informatici.

DECRETO LEGISLATIVO 19 giugno 2025, n. 102 Disposizioni integrative e correttive del decreto legislativo 23 febbraio 2023, n. 18, di attuazione della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio, del 16 dicembre 2020, concernente la qualita' delle acque destinate al consumo umano.

**Adalberto Biasiotti**



**www.puntosicuro.it**