PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5701 di Venerdì 27 settembre 2024

I sistemi idrici sono a elevato rischio di attacchi informatici

Un recente studio, condotto negli Stati Uniti, ha messo in evidente come i 170.000 sistemi di raccolta e distribuzione di acqua potabile e di gestione di acque di rifiuto rappresentano un'area di elevato rischio, a fronte di attacchi informatici.

Chi scrive ha più volte offerto assistenza a strutture italiane di raccolta e distribuzione di acqua potabile ed a strutture che gestiscono le acque di rifiuto, perché i dirigenti si sono resi conto che possibili attacchi fisici od informatici a queste due strutture potrebbero avere conseguenze devastanti sulla popolazione.

È esattamente la situazione che è stata riscontrata negli Stati Uniti e che ha indotto la EPA -environmental protection agency, a mettere a punto un piano di protezione di queste strutture, sollecitando tutte le aziende coinvolte ad attivare tempestivamente adeguate protezioni.

Un problema non trascurabile di queste strutture riguarda il fatto che la maggioranza degli investimenti viene indirizzata al miglioramento della qualità dell'acqua ed alla diminuzione delle perdite della rete, mentre i fondi destinati alla prevenzione di attacchi informatici sono ancora relativamente modesti.

Ad esempio, un attacco informatico che possa modificare le quantità di sostanze chimiche che vengono disciolte nelle acque, per migliorarne la potabilità, potrebbe portare all'inquinamento di gigantesche quantità di acqua potabile, che non sarebbe così utilizzabile dai cittadini. È ben vero che lungo tutta la rete di distribuzione sono presenti dei sensori, che tengono sotto controllo la qualità dell'acqua e mettono in evidenza la presenza di sostanze inquinanti, ma è anche vero che un problema da affrontare riguarda il punto, in cui potrebbe avvenire l'iniezione di queste sostanze tossiche, alterando i dispositivi informatici che calibrano la quantità di sostanze da immettere nell'acqua. Quanto più lontano è il punto di inquinamento dal punto di distribuzione al pubblico, quanto più facile è individuare tempestivamente il possibile attacco. Se invece il punto di origine dell'inquinamento è relativamente vicino al punto di distribuzione alla utenza, le possibilità di individuare tempestivamente l'anomalia sono purtroppo assai basse.

Un altro problema non trascurabile riguarda il fatto che molte di queste aziende sono operative sul campo da decenni e decenni e quindi molte attrezzature, che normalmente esse utilizzano, possono essere obsolete, almeno alla luce della evoluzione rapida delle tecniche di attacco informatico. Ciò comporta investimenti significativi nella sostituzione di numerose apparecchiature, rallentando gli investimenti su altre voci altrettanto importanti, come appunto menzionato in precedenza.

Il tema, che è stato affrontano gli Stati Uniti, evidentemente è altrettanto valido anche in Italia ed ecco il motivo per cui la nuova agenzia per la sicurezza informatica si sta attivando per sensibilizzare le aziende coinvolte perlomeno sull'avvio di un piano di valutazione dei rischi informatici e la messa punto di un budget, articolato eventualmente su più anni, per mettere sotto controllo la rete da questa tipologia di attacchi.

Ad oggi, almeno in Italia, si sono verificati inquinamento di rete, ma origine perlopiù accidentale, ma la evoluzione del profilo dei criminali fa' sì che non ci debba affatto sorprendere se, a breve termine, il profilo dell'attaccante abbia a cambiare in senso drammaticamente negativo.

Adalberto Biasiotti

---

www.puntosicuro.it