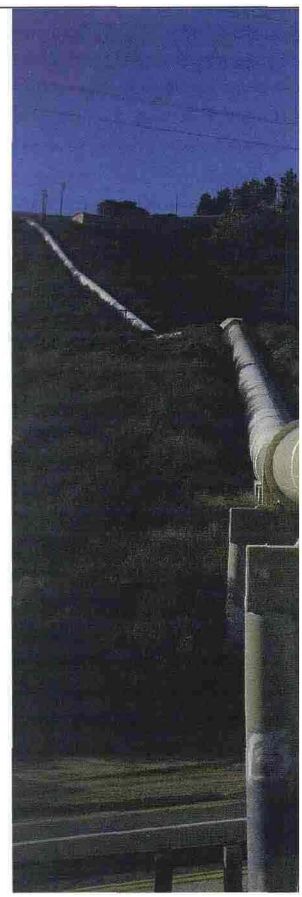
AUTOMAZIONE Industriale
Mensile
Data 01-2011
Pagina 56/57
Foglio 1 / 2

Chi violerebbe un acquedotto?



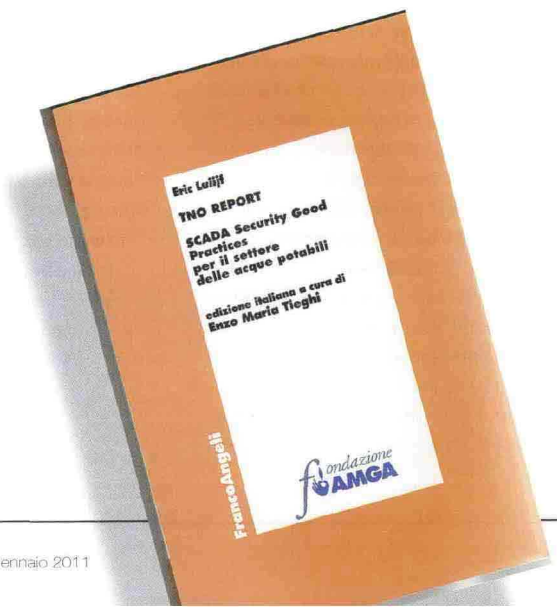
La cronaca dimostra come i sistemi Scada, utilizzati per gestire le reti idriche, siano uno dei possibili obiettivi di attacchi informatici

di Adolfo Violante

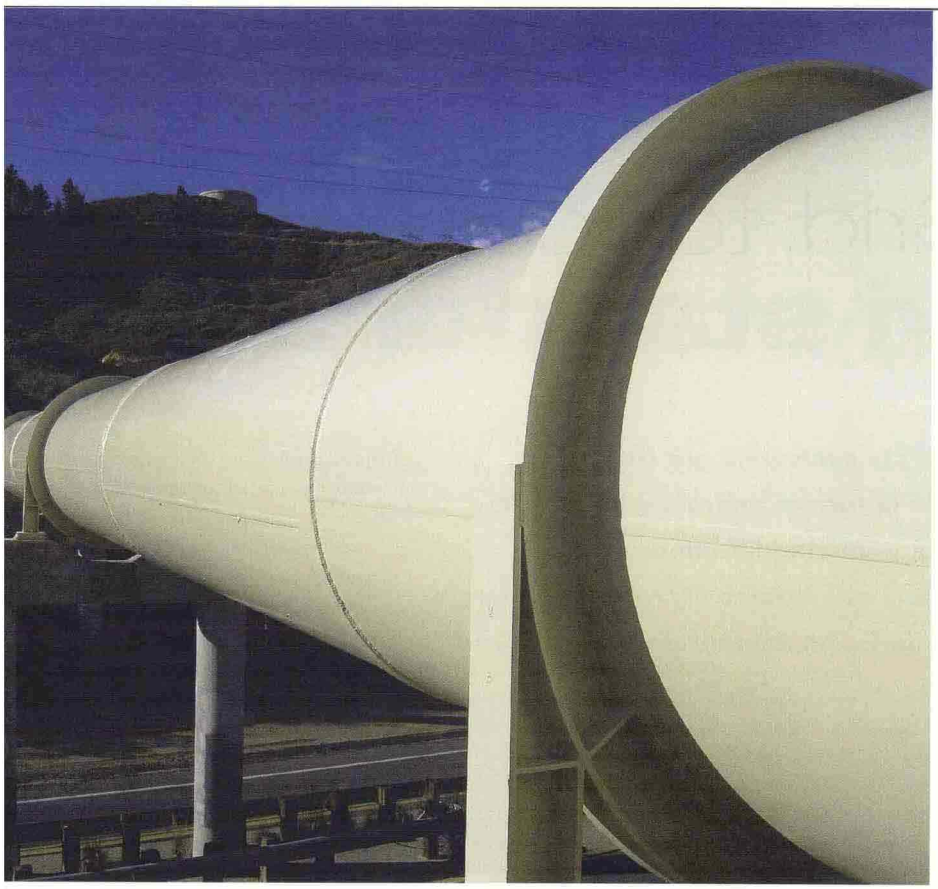
Chi potrebbe essere interessato a violare lo Scada di un impianto di distribuzione dell'acqua potabile? I dati disponibili, infatti, non servirebbero all'hacker in questione e non avrebbero nemmeno valore economico sul mercato. A chi potrebbe interessare per quante ore ha funzionato una pompa o di quanto è variato il livello di un invaso?
Forti di queste 'convinzioni' per anni i sistemi Scada utilizzati dalle aziende di distribuzione e depurazione dell'acqua non sono stati oggetto di particolari attenzioni dal punto di vista della sicurezza. Il tutto nell'errata convinzione che nessuno potesse essere interessato a penetrarli con scopi ostili.
Eppure, come dimostra il volume 'Tno report - Scada Security Good Practices per il settore delle acque potabili', edito da Franco Angeli e curato, nella versione italiana, da Enzo Maria Tieghi, la realtà è molto diversa.
Benché nessuno dia volentieri evidenza degli incidenti verificatisi sui propri impianti, la letteratura non manca di riportare casi eclatanti. Ha fatto scuola, in questo ambito, la vicenda di Vitek Boden che, tra il gennaio e l'aprile del 2000, per ben 46 volte aveva manipolato il sistema Scada di Hunter Watertech, un gestore olandese, disperdendo nell'ambiente quasi un milione di litri di acque reflue.
Più recentemente, nel gennaio del 2007, problemi di comunicazione con i sistemi Scada per la distribuzione dell'acqua a Fort Worth, negli Usa, provocarono otto ore di fermata nella fornitura di acqua potabile.

Le regole della sicurezza

A fronte di questi e decine di altri 'incidenti' più o meno gravi, verificatisi nel settore delle acque potabili, ma anche in qualunque altro ambito di distribuzione e produzione controllato da software, è necessario prevedere adeguate politiche di protezione, per salvaguardare l'azienda stessa, l'ambiente e gli utenti. Il tutto anche in considerazione del fatto che, complice il rischio di nuove forme di attacco terroristico, non è più sufficiente limitarsi a proteggere fisicamente gli impianti cosiddetti sensibili. Non a caso, una delle prime iniziative del neo-presidente degli Stati Uniti Barak Obama è stata quella di varare nuove misure per garantire maggior sicurezza nel cyberspazio. Poiché da un attacco virtuale possono crearsi situazioni di pericolo reale.
Da qui l'idea di raccogliere, nella pubblicazione, una serie di Good Practices per quanti si occupino di sistemi Scada. Si tratta di consigli pratici "che, pur non rappresentando un'imposizione normativa, poiché la legge in questo ambito è ancora decisamente carente", rappresentano un utile punto di riferimento nel settore specifico delle acque ma, più in generale, in qualunque ambiente produttivo gestito da un software.



AUTOMAZIONE Industriale
Mensile
Data 01-2011
Pagina 56/57
Foglio 2 / 2



Dalla politica...

In particolare la pubblicazione ricorda come " la corretta implementazione di sicurezza informatica per reti e sistemi Scada richieda un ambiente in cui il management ponga una grande attenzione alla security. Questo coinvolge procedure di security inserite nei processi operativi in conformità a relative analisi del rischio di un processo di risk management che si applichi all'intera azienda".
Un'attenzione specifica, in particolare, viene riservata alla necessità di possedere, in azienda, una specifica consapevolezza della sicurezza: "Uno dei principali fattori di rischio che richiede controllo all'interno è l'elemento umano. Anche questo forma un fattore di rischio primario nell'ambiente Scada. La conoscenza consapevole della security aiuta il management e i dipendenti a restare focalizzati nelle loro attitudini verso la security e inoltre a migliorare il livello di sicurezza dell'organizzazione". Un atteggiamento aziendale che deve essere imposto anche ai fornitori esterni: "La politica prioritaria di sicurezza per i sistemi e reti Scada vale anche per i dipendenti di terze parti. Il primo punto da stipulare è l'accesso ristretto ai sistemi scada. Come minimo, le terze parti forniscono garanzia che i loro dipendenti sono degni di fiducia. Sono state concordate e messe per iscritto le condizioni cui sottostanno le apparecchiature e software di terze parti (inclusi i laptop per tecnici di manutenzione, modem) che possono essere collegati ai sistemi e reti Scada. Tutte le attività svolte da terze parti su componenti di reti e sistemi in ambiente Scada vanno tenuti sotto controllo. Questo previene guasti seri che possono mettere a rischio la garanzia di erogazione di acqua potabile".

La letteratura è ricca di attacchi informatici ai danni delle reti di controllo delle acque

...alle pratiche di sicurezza

Accanto ai principi di organizzazione generale, è ovviamente fondamentale predisporre adeguate tecnologie di protezione: "L'accessibilità di reti e sistemi Scada da reti pubbliche e da reti aziendale è schermata e resa sicura nella misura in cui superare una misura di security non consente un accesso incontrollato a reti e sistemi Scada. In aggiunta a Firewall, collegamenti di rete easy-to check e sistemi call-back, misure di sicurezza quali autenticazione con password individuale, cambiata regolarmente, rilevamento di intrusioni, misure antivirus e politiche di patch possono essere usate per erigere barriere in grado di respingere attacchi ostili".
L'impiego di moderni sistemi di protezione rappresenta solo il primo passo nella direzione di un'autentica politica di protezione delle reti Scada. A questo si aggiunge la necessità di "rimuovere qualunque collegamento non essenziale tra la rete scada e le altre reti".
Rimane comunque fondamentale separare, rigorosamente, l'ambiente Scada da quello di Office Automation. Questo soprattutto in considerazione del fatto che "i sistemi e i software Scada sono fortemente sensibili agli inattesi pacchetti distribuiti da worm e ai sovraccarichi di rete".

Il valore delle informazioni

Nel volume viene ricordato un importante assunto: "Le informazioni sono dei beni e, come ogni altro bene aziendale, hanno un valore: quindi devono essere protette in modo adeguato. La sicurezza delle informazioni protegge le stesse da una moltitudine di minacce allo scopo di assicurare la continuità aziendale, minimizzare i danni aziendali, massimizzare il rendimento del capitale investito, migliorare l'efficienza e l'efficacia". ■