ACQUA SICURA 4.0: la CYBER SECURITY nei sistemi SCADA (Controllo e Telecontrollo)

RELATORI: FRANCESCO TIEGHI (RESP. DIGITAL MARKETING di ServiTecno), **ANTONIO ALLOCCA** (CEO di ATI)

ABSTRACT: scopo dell'intervento è quello di ***sensibilizzare System Integrator*** ed ***End Users*** riguardo le ***nuove sfaccettature e frontiere della Cyber Security*** negli ambienti di ***processo***.
la CYBER SECURITY ICT (intesa come protezione da rischi informatici) e quella relativa ai SISTEMI DI PROCESSO, hanno principi simili ma priorità differenti. Come interpretare al meglio il problema in un'epoca tecnologica in cui le architetture dei sistemi ed il numero di connessioni sta aumentando con ritmo esponenziale, anche in considerazione di Smart Grid, IOT (Internet Of Things) e Cloud Computing.
Due i principi chiave:
1) I tre principi base su cui si fonda la Cyber Security sono: RISERVATEZZA,INTEGRITA' e DISPONIBILITA' del dato (RID). In inglese CIA (CONFIDENTIALITY, INTEGRITY & AVAILABILITY).
Per chi lavora nell'IT l'ordine in cui sono scritti rispecchia le priorità: per chi ha a che fare con il processo e reti di impianto invece questo ordine è esattamente invertito.
Infatti la DISPONIBILITA' è il primo aspetto da preservare in un sistema di supervisione in ambito UTILITY, in reti che rendono possibile la distribuzione di flussi e servizi primari: sistemi ridondati, alta disponibilità e fault tolerance non sono un lusso.
L'1% di fermo del sistema, calcolato su una base annuale ANNUALE di 365 giorni, equivale a oltre 3 giorni e mezzo di disservizio: QUANTO VALE IN TERMINI DI SAFETY, SECURITY e COSTI DI MANCATA EROGAZIONE DEL SERVIZIO? (senza considerare il danno alla "reputation")
2) IOT è dietro l'angolo: ogni dispositivo parlante è una potenziale porta di ingresso e di problemi.
Durante le vacanze di NATALE 2014 la catena di supermercati TARGET negli USA ha perso il controllo dei suoi POS, permettendo la clonazione di più di 40 MILIONI di CARTE DI CREDITO. Gli hacker hanno agito per oltre due settimane ed il danno provocato è stato superiore ai 60 MILIONI di dollari (esclusa la causa in corso tra le banche e TARGET stessa): la PORTA DI INGRESSO è stata una linea lasciata aperta per la visualizzazione di parametri relativi alla MANUTENZIONE delle CELLE FRIGORIFERE che veniva gestita remotamente (da Chicago per tutti i 1.797 punti vendita negli USA). Gli intrusi sono entrati dai frigoriferi…COME SI SAREBBE POTUTO EVITARLO?

L'evoluzione delle architetture dei sistemi e l'estrema diversificazione delle tecnologie rendono disponibili soluzioni di telecontrollo ed automazione articolate e specializzate.
Il centro di controllo, elemento baricentrico dei sistemi SCADA, consente di concentrare tutte le informazioni di carattere tecnico e gestionale presenti sui singoli impianti, tramite la trasmissione di dati in tempo reale. Nello specifico ambito dei sistemi di telecontrollo per reti idriche, l'obiettivo dell'intervento in oggetto è quello di analizzare una problematica di crescente interesse e grande attualità: la sicurezza informatica.
In senso assoluto, il concetto di sicurezza è difficilmente traducibile nella vita reale, anche se l'applicazione di alcune linee guida rende più difficile il verificarsi di eventi dannosi e di incidenti: è del 2010 la pubblicazione in Italia del volume "SCADA Security Good Practices per il settore delle acque potabili". Per quanto riguarda i sistemi SCADA, lo scopo è quello di aumentare la disponibilità e di impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia dovuta ad eventi accidentali.
Quindi gli obiettivi chiave - riservatezza, integrità e disponibilità –, oltre a preservare la "Security", consentono di ridurre i costi di esercizio degli impianti e di ottimizzarne le prestazioni. Verranno analizzati le principali minacce e le relative azioni preventive, mirate ad impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia dovuta ad eventi accidentali.
L'originalità dell'intervento vuole essere nell'approccio semplice e concreto ad una tematica altrimenti troppo indefinita, spesso relegata nella sfera delle disquisizioni teoriche e non pratiche. Affrontare concretamente questi argomenti prevede un mix-and-match di competenze trasversali, che devono vedere

una specifica collaborazione tra venditori di tecnologie, System Integrator ed Utilizzatori dei sistemi di telecontrollo.