Vulnerabilità e sicurezza informatica dei sistemi di telecontrollo connessi alla rete internet: il caso dell'Acquedotto Montescuro Ovest

Questa esperienza è stata presentata al Forum del Telecontrollo che si tenuto a Milano il 29 e 30 settembre 2015. Nel progetto di telecontrollo realizzato è stato enfatizzato l'aspetto relativo alla sicurezza informatica dei dati aziendali, sempre più importante in un contesto di incrememto del rischi da cyber attack.

Il notevole incremento in termini di complessità e dimensioni dei sistemi idrici gestiti a livello di ambito ottimale, ha obbligato le utilites a migliorare il livello di conoscenza di tali sistemi, adottando e/o potenziando piattaforme software (GIS, Supervisory Control And Data Acquisition System SCADA, Sistemi di Supporto alle Decisioni DSS) in grado di gestire le informazioni raccolte, e di renderle fruibili alle diverse strutture operative aziendali.
L'interconnessione di tali sistemi informatici e la loro accessibilità web, ha di contro aumentato la vulnerabilità complessiva del sistema, attirando le attenzioni di possibili pirati informatici, con possibili gravi conseguenze sul corretto funzionamento complessivo del sistema fisico gestito e sugli utenti serviti. Occorre quindi porre particolare attenzione all'aspetto concernente la sicurezza informatica al fine di prevenire, intervenire e/o ripristinare i sistemi informatici da eventuali cyber attacchi.

In quest'ottica Proxima S.r.l., società che opera dal 1996 nel settore della progettazione e realizzazione di sistemi di telecontrollo, ha progettato e sta realizzando per conto di Siciliacque S.p.A. il "Sistema di Telecontrollo dell'Acquedotto Montescuro Ovest", un sistema che gestisce circa 90 impianti - serbatoi, centrali di pompaggio, partitori, camere di manovra e punti di misura, centraline di protezione catodica - distribuiti su un territorio esteso e orograficamente variegato della Sicilia occidentale.

Per la criticità della funzione del sistema in esame si è posta particolare attenzione agli aspetti legati alla sicurezza (Fig. 1 - NdR: per visionare la fig. 1 e seguenti: vedere il file pdf in download o la galleria immagini del presente redazionale), riducendo al minimo le probabilità che tale sistema sia soggetto ad un attacco informatico che permetta l'accesso ai dati e soprattutto impedisca l'accesso agli organi idraulici presenti in campo, in modo che non causino disagi, limitazioni o danni al sistema idrico e agli utenti serviti.

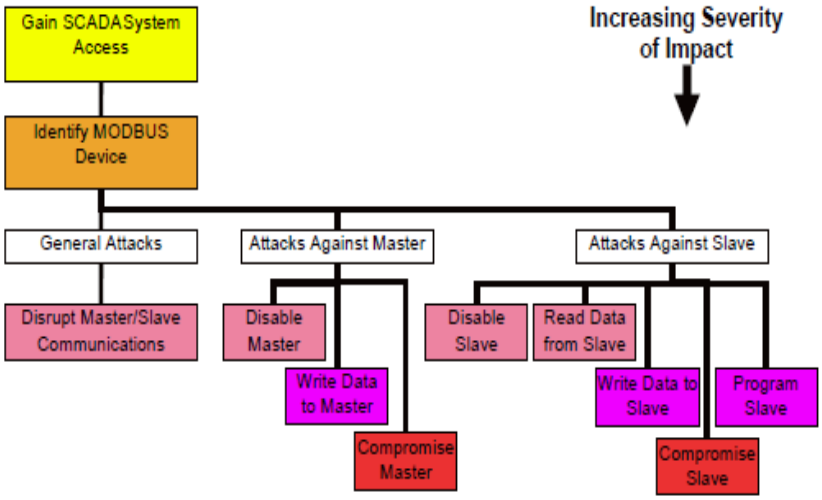

Fig.1 Livelli Profondità di attacco informatico

Gli attacchi informatici ai danni di un sistema SCADA possono: interferire con le operazioni, effettuare modifiche non autorizzate alle logiche dei programmi, cancellare o modificare dati, trasmettere false informazioni, cambiare le soglie di allarme, comandare organi di manovra, agire sugli organi dosatori per alterare la quantità di sostanze immesse dell'acqua, ecc. … con conseguenze facilmente immaginabili.

Per lungo tempo i sistemi SCADA sono rimasti nascosti all'interno della rete aziendale, dando ai gestori una sensazione di «sicurezza» ed «inaccessibilità». Viceversa gli SCADA attuali si sono evoluti verso soluzioni standardizzate a basso costo e di facile manutenzione ed accessibilità, con una conseguente diffusione di conoscenza che li ha resi vulnerabili attirando l'interesse di malintenzionati ed hacker.
I principali fattori che hanno contribuito ad un aumento della vulnerabilità dei sistemi di telecontrollo sono:

- L'interconnessione delle reti di telecomunicazioni
- Le modalità di accesso remoto ai sistemi
- La standardizzazione delle tecnologie
- La disponibilità di reperire informazioni tecniche

Un aspetto fondamentale della sicurezza in tali sistemi è rappresentato dai protocolli di comunicazione in quanto costituiscono il mezzo con cui le informazioni vengono recuperate dalle apparecchiature in campo e vengono inviati i comandi.
I protocolli utilizzati sono stati per lungo tempo «proprietari», adottando l'approccio "Security By Oscurity", oggi la tendenza attuale è orientata ad adoperare protocolli «Aperti» e «Standard». Il rovescio della medaglia è dato dall'ampia documentazione disponibile che ne aumenta la vulnerabilità agli attacchi informatici. Il protocollo di comunicazione che nello specifico si è scelto di adottare è il «DNP3 Secure Authentication» basato sullo standard IEC62351: uno dei pochi standard aperti disponibile per le comunicazioni SCADA, che soddisfi i principali requisiti di sicurezza. Tra i vari obiettivi di sicurezza che lo standard ricerca, troviamo:

- L'autenticazione del processo di trasferimento di dati tramite firma digitale
- La garanzia di accessi esclusivamente dopo autenticazione
- La garanzia della confidenzialità dei dati trasmessi tramite la prevenzione dell'eavesdropping, ossia la possibilità che le comunicazioni vengano intercettate
- La prevenzione di attacchi di spoofing (intromissione nella rete sostituendo una degli elementi della rete)
- Criptaggio dei dati (al fine di nascondere il contenuto dei messaggi a chi dovesse intercettare le comunicazioni senza avere la chiave di cifratura)

Nel futuro prossimo, per sopperire alle possibili carenze tecniche dei clienti si tenderà a realizzare sistemi di telecontrollo allocando le risorse necessarie su Cloud, al fine di demandare gli aspetti legati alla sicurezza del centro di controllo alle aziende fornitrici di tali piattaforme che adottano tecniche di sicurezza e di Disaster Recovery più evolute di quelle adottabili da un gestore di servizi di piccole-medie dimensioni. In tal modo si eliminano anche le componenti di rischio di attacco dall'interno che risultano le più pericolose, in quanto il malintenzionato dispone di un punto di accesso fisico al sistema.

Alle misure sopra citate, vanno comunque affiancati i metodi classici di protezione di una rete di telecomunicazioni (firewall, antivirus, policy, etc etc) che tuttavia da soli non sono sufficienti a garantire adeguata protezione.

Nel sistema di Montescuro Ovest, la scelta proposta da Proxima S.r.l. del supporto di trasmissione nel sistema da utilizzare ha tenuto conto di vincoli tecnici, geografici ed economici. Si è adottato in via prioritaria un sistema di comunicazione basato su Radio Digitale, operante su frequenze licenziate, avente sistemi di criptazione dei dati a 256 bit ed altre funzionalità per la gestione tramite accesso remoto sicuro. Si è evitato così di adoperare soluzioni quali il GPRS o il GSM, che se pur economiche espongono le periferiche di controllo ad una maggiore esposizione di rischio (Fig. 2).

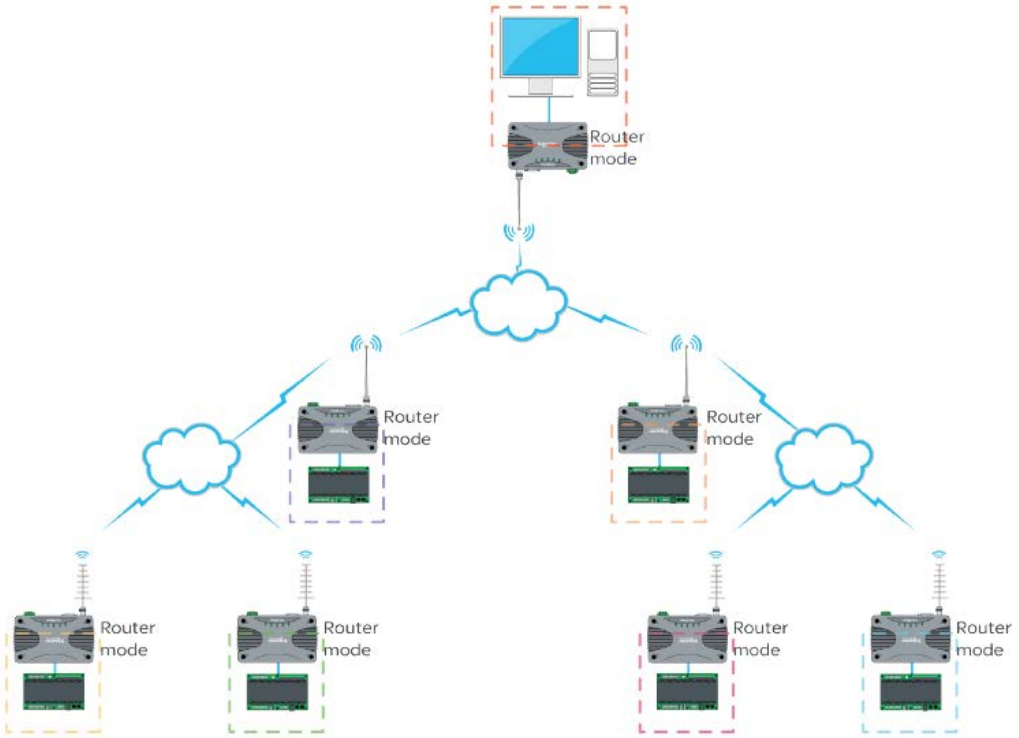

Fig. 2 Architettura Radio Digitale Trio

Operando su frequenze licenziate, si elimina la possibilità di disservizi legati ad interferenze e si possono adottare protocolli di comunicazione proprietari, garantendo capacità di affidabilità enormemente superiori rispetto ai sistemi in banda libera o collettiva.

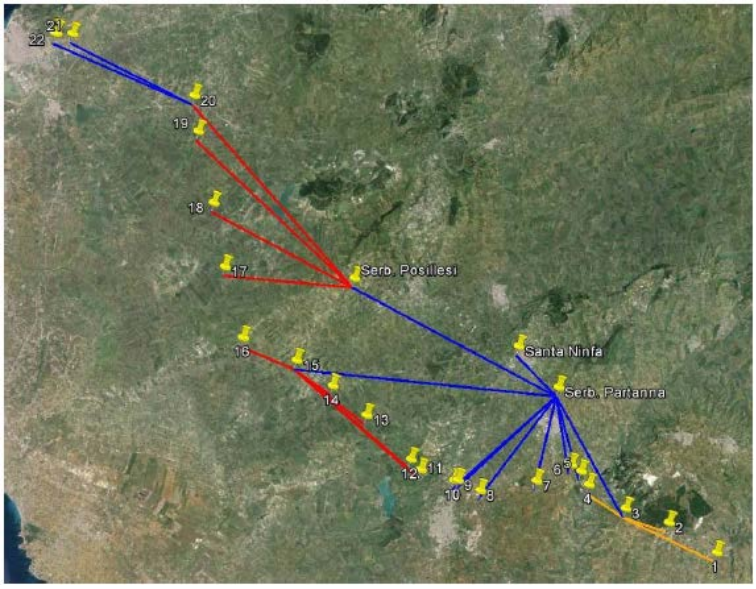

Fig. 3 Network Radio Montescuro Ovest – Ramo Basso

Il sistema realizzato dimostra come siano state adottate diverse politiche per garantire al sistema robustezza nella ricezione del dato e sicurezza globale di non accesso alle informazioni o ai comandi da parte di persone non autorizzate, il tutto senza limitare le funzionalità richieste oggi da un sistema di telecontrollo all'avanguardia.

Per approfondimenti e informazioni: www.e-proxima.eu