PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4125 di Lunedì 20 novembre 2017

Qual è il livello di sicurezza informatica dei BMS?

Durante la recente mostra Sicurezza a Milano, numerosi espositori proponevano sistemi integrati di gestione di edifici, a livello di impianti tecnologici e di sicurezza anticrimine. Qual è il livello di sicurezza informatica di questi applicativi?

Nessuno può negare che i sistemi integrati di gestione degli edifici, dell'energia e di altre apparecchiature possano offrire una elevata efficienza energetica, un migliore comfort per gli abitanti e in alcuni casi anche una sicurezza fisica accresciuta. Questi sistemi permettono di controllare in modo integrato i numerosissimi impianti presenti in un edificio moderno e i dati generati da questi applicativi consentono di migliorare la gestione dell'edificio.

D'altro canto, l'attenzione alla efficienza sempre più elevata può talvolta far dimenticare di prestare altrettanta attenzione alla protezione di questi applicativi da possibili attacchi dall'esterno.

Mi permetto di tracciare un parallelo tra le nuove automobili super intelligenti e il fatto che degli hackers, nemmeno dotati di attrezzature assai sofisticate, sono più volte riusciti a prendere il controllo di queste autovetture, con conseguenze facilmente immaginabili.

Per quanto riguarda l'esperienza diretta di chi scrive, i progettisti, installatori e gestori di questi applicativi integrati non sempre hanno una specifica sensibilità e cultura nei confronti della sicurezza informatica, premiando sempre le prestazioni dei sistemi, sulla loro gestione sicura.

Per dare una conferma oggettiva a questa situazione mi permetto di ricordare alcuni eventi che dovrebbero costituire un significativo monito.

Uno dei primi casi di sabotaggio di sistemi di gestione risale al 1982, quando i servizi segreti americani furono in grado di produrre un'esplosione in una tubazione di gas, che proveniva dalla Siberia.

Tutti i giornali del mondo hanno dato notizia dell'ormai famoso virus stuxnet che ha distrutto il 20% delle centrifughe nucleari iraniane, disabilitando il controllo di velocità delle turbine e facendo quindi esplodere le centrifughe.

Nel 2014 degli hacker furono in grado di danneggiare in modo grave una acciaieria tedesca, motivando le loro azioni con ragioni di tutela dell'ambiente.

Un hacker a Shenzhen, in Cina, prese il pieno controllo di tutti le funzioni primarie di un albergo di lusso, utilizzando soltanto un applicativo che aveva caricato sul suo iPad.

Uno dei più diffusi applicativi integrati di gestione di edifici è stato colpito da hacker, che hanno preso il controllo dei sistemi di controllo accesso, degli ascensori e degli impianti di videosorveglianza in numerosi insediamenti, che usavano questo specifico applicativo.

Spesso questi attacchi sono conseguenza indiretta di altri attacchi, come è accaduto nel novembre 2013 quando 40 milioni di utenti di una catena di vendita on-line hanno visto sottratti i dettagli delle loro carte di credito. La vulnerabilità non era presente nel sistema primario della catena di vendita on-line, ma nel sistema di gestione dei parametri ambientali, affidato ad una ditta in subappalto.

Le ragioni per questi attacchi sono le più varie, come ad esempio quelle avanzate da gruppi di attivisti che avanzano pretese ambientalistiche, terroristi che desiderano creare disservizi a livello nazionale in nazioni nemiche, aziende che desiderano sabotare dei concorrenti, dipendenti licenziati che vogliono così vendicarsi del datore di lavoro e via dicendo.

Non mi addentro nelle varie attività che possono essere danneggiate, ma basti ricordare che una compromissione di questi sistemi può disabilitare o far assumere ad un hacker il controllo di impianti di illuminazione, controllo accessi, condizionamento, videosorveglianza, ascensori, fatturazioni alberghiere, rivelazioni di principi di incendio e via dicendo.

Il problema di fondo di molti di questi applicativi nasce dal fatto che essi hanno cominciato ad essere sviluppati in tempi nei quali l'efficienza premiava certamente sulla sicurezza informatica. Se andiamo a vedere i nomi delle aziende che propongono questi sistemi, troviamo aziende che sono sul mercato da 100 anni e che hanno cominciato a sviluppare questi sistemi 40 anni fa. Inoltre la gran parte degli installatori di questi sistemi provengono dal mondo dell'impiantistica elettrica ed industriale, che non brilla certamente per la sua sensibilità e competenza nel settore della sicurezza informatica.

Ecco perché una recente indagine di mercato ha offerto un elenco delle aree nelle quali è indispensabile intervenire in maniera significativa, per migliorare la resistenza di questi applicativi ad attacchi dall'interno ed all'esterno. Ad esempio:

- miglioramento della sicurezza di rete,
- l'utilizzo di protocolli di comunicazione più sicuri,
- l'utilizzo di sistemi ridondanti,
- l'addestramento del personale e pubblicazione di specifiche regole di comportamento,
- il miglioramento dei log di sistema,
- l'effettuazione periodica di audit di sicurezza informatica.

Mi sembrano raccomandazioni per le quali venditori ed installatori dovrebbero essere grati e che possono costituire una guida nell'elaborazione di capitolati per la fornitura e installazione di questi applicativi, tanto utili se ben controllati, quanto pericolosi se non vigilati a sufficienza.

Adalberto Biasiotti
