Memoria per Telecontrollo 2015

Autore della memoria
Raffaele Esposito
Product Manager Safety, I/O & Networking
Phoenix Contact Spa

Titolo della memoria
La Cyber Security quale elemento strategico dell'approccio Industry 4.0

Testo della memoria
Le necessità di flessibilità ed efficienza produttiva sono soddisfatte dal mondo dell'industria attraverso l'uso sempre più ampio e consapevole di tecnologie digitali in senso lato.
Tali tecnologie hanno modificato radicalmente approcci, strumenti e modalità operative del mondo industriale con un impatto che può essere assimilato a quelle delle passate Rivoluzioni Industriali.
Si tratterebbe della quarta (dopo quelle caratterizzate dall'uso a fini produttivi del vapore, dell'elettricità e dell'energia nucleare), da qui il termine ''Industry 4.0'' utilizzato per la prima volta a livello ministeriale tedesco.
Industry 4.0 si basa sui cosiddetti ''sistemi virtuali-reali'' (Cyber Physical Systems), vale a dire sistemi ad alta complessità costituiti da componentistica intelligente basata su varie tecnologie quali ad esempio la meccanica, l'elettronica, l'informatica e che, in genere, sono posti tra loro in comunicazione attraverso una rete, spesso costituita da Internet.
Varie le definizioni utilizzate per identificare soluzioni o concetti tecnologici che costituiscono le colonne portanti di Industry 4.0: si pensi ad esempio ai concetti di Internet of Thing, Smart Factory, Smart Grid, Cloud, …
Gli obiettivi della cosiddetta "Smart Factory" sono rappresentati in modo estremamente sintetico dalla massimizzazione dell'efficienza energetica, dell'ergonomicità, della flessibilità produttiva e dell'ottimizzazione dei flussi di materiale, in modo da perseguire, allo stesso tempo, anche una riduzione degli impatti ambientali dell'attività produttiva.
A questo fine, le tecnologie digitali sono degli alleati estremamente preziosi, soprattutto nel caso in cui si attinge a tecnologie Web-oriented con la predisposizione di opportuna infrastruttura di rete.
Svariati i vantaggi ottenibili, tra i quali, si possono evidenziare, tra gli altri, gli aspetti di:

- integrazione delle unità produttive in sistemi di gestione dati governati da sistemi ERP e/o MES;
- accesso da remoto (teleassistenza e telecontrollo);

- utilizzo di tecnologie wireless;
- possibili analisi predittive e organizzazione di manutenzione programmata.

Di contro, uno degli aspetti da prendere in conto per qualsiasi infrastruttura di rete, e non necessariamente solo per quelle con accesso al Web, è sicuramente quello della Security, intesa come accesso non autorizzato alla rete.

La consapevolezza dell'importanza di un adeguato livello di security è in continua crescita anche a livello operativo, laddove si diffonde quella consapevolezza già ben nota a massimi livelli gestionali.

All'interno dei documenti elaborati al World Economic Forum 2014 è infatti chiaramente evidente il fatto che i "***Cyber Attacks*** *sono considerati uno dei* ***rischi più elevati*** *per l'economia in termini di IMPATTO e PROBABILITA'".*

I rischi legati ad accessi non voluti alla propria infrastruttura di rete, anche se tecnicamente ben noti, sono spesso sottovalutati nel loro possibile impatto economico.

I costi di un cyber attack vanno infatti valutati in modo estensivo.

Quanto può costare ricostruire i dati persi? (sempre ammesso che questi dati siano ricostruibili)

Quanto può valere economicamente la perdita di know-how?

Quanto può essere il costo di una mancata produzione?

Quanto possono costare eventuali azioni di spionaggio/hackeraggio di terze parti lanciate attraverso la vostra infrastruttura di rete?

Ma, soprattutto, quanto può costare un cyber attack che possa danneggiare la reputazione di un'azienda?

Nella valutazione dei rischi legati alla Security di una rete è necessario considerare i possibili accessi fraudolenti non solo da remoto ma anche on site (uso ad esempio di memory stick infette), la dismissione dei sistemi operativi utilizzati, la pratica impossibilità di utilizzo di programmi anti virus standard in PC industriali, il tempo di connessione al Web della rete, l'utilizzo di connessioni sicure (VPN, firewall), gli accessi multipli della rete (macchine in serie, ognuna delle quali con accesso al Web), lo stoccaggio sicuro delle credenziali di accesso alla rete, ….

Le soluzioni tecnologiche maggiormente standardizzatesi sul mercato prevedono l'utilizzo di safety router che consentono una connessione al Web attraverso tunnel VPN con opportuna crittografatura dei dati e con l'utilizzo di adeguate soluzioni di firewall.

Sta inoltre prendendo piede l'utilizzo di un approccio su base cloud anche per le connessioni sicure da remoto a macchine o installazioni industriali.

Spesso utili a favorire un adeguato livello di security sono anche altre tipologie di soluzioni tecnologiche quali l'utilizzo di VLAN, la definizione di partizioni di rete dedicate (aree DMZ) piuttosto che di tecniche di verifica dell'integrità di sistema attraverso hardware esterno indipendente dal sistema operativo utilizzato.