A.N.I.P.L.A.
ASSOCIAZIONE NAZIONALE
ITALIANA PER L'AUTOMAZIONE

mcT Petrolchimico

Quale futuro per la Cyber security ?

Giovedi 24 novembre 2016
Crowne Plaza Hotel – San Donato Milanese
Sala Visconti –ore 9:00

Obiettivi

I sistemi di automazione e di controllo industriale sono diventati molto più vulnerabili agli incidenti di sicurezza a causa delle seguenti tendenze che si sono verificate nel corso degli ultimi 10 o 15 anni:

• l'uso sempre più diffuso di prodotti COTS – (Commercial) Off-the Shelf Component, l'integrazione di tecnologie come MS Windows, SQL ed Ethernet significa che i sistemi di controllo di processo sono oggi vulnerabili agli stessi virus, worm e trojan che pregiudicano i sistemi IT classici;
• l'integrazione aziendale (utilizzando reti di impianto, aziendali ed addirittura reti pubbliche) significa che i sistemi di controllo di processo (anche quelli in attività anche da molti anni) vengono ora sottoposti a sollecitazioni per le quali non erano stati progettati;
• la domanda di accesso remoto – i servizi di assistenza 24/7 per attività di ingegneria o di supporto tecnico rendono possibili dei collegamenti non autorizzati al sistema di controllo;
• Informazione pubblica – La pubblica disponibilità di manuali su come utilizzare i sistemi di controllo non discrimina sul tipo di uso che della relativa conoscenza si potrebbe fare;
• la regolamentazione sui minimi livelli di sicurezza richiesti per i sistemi di controllo, è molto rara.

Con riferimento al Rapporto Clusit 2015 si osserva che :

• Nonostante ci siano importanti sforzi da parte delle Forze dell'Ordine di tutto il mondo, si sono ottenuti risultati poco significativi nel contrasto al cyber crime ed al cyber espionage: è mancata una strategia ampia di contrasto al fenomeno e ciò nonostante l'aumento dei rischi e delle minacce.
• Se da un lato sono aumentati in percentuale rilevante gli investimenti in sicurezza informatica (saliti dell'8% nel 2014 a livello globale, nonostante il perdurare della crisi economica), il numero e la gravità degli attacchi (percepiti, visto che 2/3 degli attacchi si stima che non vengano neanche rilevati) continuano ad aumentare.

Sempre in riferimento al succitato rapporto, si prevede che la crescita inarrestabile del Cybercrime porterà alla ulteriore diffusione di quelle logiche estorsive che hanno dato origine a ransomware di grande successo quali Cryptolocker, i quali continueranno a diffondersi, colpendo non solo gli utenti finali e le aziende, ma anche la Pubblica Amministrazione ed i sistemi industriali, incluse le Infrastrutture Critiche. Questi attacchi saranno compiuti sia per ragioni economiche che politiche, consolidando un trend di crescente collaborazione tra gruppi cyber criminali e gruppi terroristici o paramilitari. Sarà di estrema importanza prevenire nei modi più opportuni queste minacce e gestirle al meglio, qualora si dovessero concretizzare.
È in questo contesto, non proprio confortante, che si inserisce la III Edizione della Giornata di Studio ANIPLA sulla Cyber Security per i sistemi ICS (Industrial Control System), in programma nel contesto della mostra convegno mcT Tecnologie per il Petrolchimico
In primo luogo si vuole *focalizzare la consapevolezza dell'uditorio sull'importanza della Cyber Security per i sistemi di controllo industriali,* dando esempi concreti di eventi legati alla cyber security e fornendo una sintesi delle tendenze attuali e del prossimo futuro e *in secondo luogo fare formazione*, affrontando sinteticamente i temi riguardanti la gestione del rischio e della Cyber Security per un sistema di controllo industriale, chiarendo le fasi e definendo i diversi ruoli coinvolti, con le rispettive competenze e dando una panoramica delle normative / certificazioni di riferimento.

Coordinatori

• Michele Monaco, SAIPEM: michele.monaco@saipem.com
• Maria Regina Meloni, SAIPEM: regina.meloni@saipem.com

Programma

9:00 Registrazione dei partecipanti

9:50 Introduzione alla Giornata ANIPLA
Regina Meloni - Saipem

10:00 Industrial Cyber Security e Industrie4.0: OT dalla fabbrica cablata ai sistemi in Cloud
Mario Testino - ISA

10:20 Minaccia Cyber nel contesto industriale: i nuovi scenari di rischio per il know how nazionale
Daniele Ali - FINCANTIERI

10:40 Studiare la cyber security attraverso i processi organizzativi: indicazioni dal campo
Alberto Zanutto – Università di Lancaster (UK)

11:00 Coffee-break offerto dagli sponsor

11:30 L'attività di Vulnerability Assessment in accordo agli standard IEC 62443
Mauro Gennaccaro – DNV GL

11:50 Resilienza dei sistemi di controllo industriali
Francesco Faenzi - LUTECH

12:10 Industrial Cyber Security: facile implementazione di adeguate strategie di difesa
Emanuele Temi – Phoenix Contact

12:30 Cyber security: evoluzione delle metodologie negli ultimi anni
Raul Chiesa - Lloyd's

12:50 Industrial Security: proteggere il sistema produttivo nell'era di Industry 4.0
Cristian Sartori - Siemens

13:10 SCADA (in)security rises
Alberto Volpatto – Secure Network

13:30 Conclusioni

A seguire buffet offerto dagli sponsor

Il riconoscimento di **3 (tre) CFP** al presente evento (codice 1002-16) è stato autorizzato dall'Ordine Ingegneri di Milano, che ne ha valutato anticipatamente i contenuti formativi professionali e le modalità di attuazione. Richiesti crediti formativi per i periti industriali

La partecipazione è libera.

Le iscrizioni sono aperte al link:

http://www.eiomfiere.it/mctpetrolchimico_milano/preregistrazione.asp?custom=anipla1