Convegno Isaca (Capitolo di Roma)
(3 giugno 2004)

La sicurezza informatica in ambiente industriale: problematiche ed una proposta di ricerca

(Glauco Bertocchi)

L’automazione industriale

Caratteristiche

- Consente di eseguire compiti (produrre) con velocità, qualità elevata e costante
- Riduce i costi ed i compiti gravosi o pericolosi
- Consente di monitorare eventi complessi che avvengono in tempi molto brevi
- Solamente con l’uso di apparati di automazione e controllo è possibile lo svolgimento in sicurezza di alcuni tipi di processi complessi

L’automazione industriale

Problematiche

- La sicurezza negli impianti industriali dipende, in larga misura, dagli apparati di automazione e controllo
- Il crescente uso di tecnologie IT (desktop, server, lan, wan, protocolli, sistemi operativi, ecc.) per monitoraggio e controllo

Domande….

- Che tipo di sicurezza si deve adottare nei riguardi degli strumenti IT utilizzati per monitorare e controllare un impianto industriale ad alto rischio (stabilimento chimico,produzione e distribuzione di energia elettrica, distribuzione di gas, ecc.)?????
- Come si modifica l'analisi del rischio degli impianti con l'introduzione di nuovi componenti, gli apparati IT, le cui debolezze sono ben note????

Lo stato attuale (ambito industriale)

- La sicurezza (safety) degli impianti industriali è materia ben nota ed oggetto di continui studi, così come l'automazione industriale. La novità è rappresentata dalla massiccia introduzione delle tecnologie IT (specialmente con l'uso delle reti di vario tipo) e dalla "scoperta" della loro vulnerabilità.
- Sta crescendo la consapevolezza che la sicurezza informatica (cyber security) è un aspetto di fondamentale importanza in organizzazioni in cui il monitoraggio e controllo di impianti critici è affidato ad apparati IT; i rischi derivanti non sono quelli noti in ambito IT (ad esempio: perdita, alterazione o diffusione non autorizzata di informazioni,ecc.) ma piuttosto quelli ben più gravi , noti in ambito industriale : danni alla salute della popolazione, decessi, danni ambientali, perdite economiche.

Lo stato attuale (ambito industriale)

- Sta aumentando la consapevolezza in ambito industriale (alcuni esempi):
  - proposte di standard per i profili di sicurezza dei centri di controllo distribuito (DCS),
  - gruppi di lavoro in materia di sicurezza dei sistemi di controllo istituiti da diverse associazioni industriali di categoria.
  - proposte di standard per la crittografia dei sistemi SCADA (Supervisory control and data acquisition),
- Esistono alcune compagnie , di origine IT o industriale, che stanno offrendo i loro servizi, proponendo l'analisi del livello di cyber security e le conseguenti misure .

Lo stato attuale (ambito IT)

- Nel “mondo” IT la sicurezza informatica è materia ben nota, oggetto di continui studi. Esistono metodologie standard che, con approcci diversi, esaminano e valutano le interazioni delle tecnologie IT con le attività e gli obiettivi delle società in cui sono utilizzate.
- La necessità di affrontare e trovare sempre nuove soluzioni all’inventiva dei cyber criminali è questione di sopravvivenza per le compagnie IT (e non solo per loro..)

Ulteriori quesiti……

- Basterebbe “trasferire” la sicurezza informatica (metodologie e tecniche) del mondo IT per soddisfare le esigenze di protezione dei sistemi informatici di monitoraggio e controllo degli impianti industriali ….. ?
- “Il trasferimento”dovrebbe limitarsi ai mezzi tecnici (firewall, antivirus, crittografia, autenticazione, ecc.) o dovrebbe anche interessare le metodologie ….?
- Come si deve modificare l’analisi dei rischi in ambito industriale in conseguenza di quelli derivanti dall’uso di tecnologie IT …? Come si valutano questi ultimi..? Con metodi IT..o diversi..?

Si potrebbe proporre….

- Esaminare le principali metodologie standard per l'analisi del rischio dei sistemi informativi e valutare la loro applicabilità ai sistemi informatici di monitoraggio e controllo.
- Formulare quindi una proposta di metodologia per l'analisi del rischio dei sistemi informatici di monitoraggio e controllo e per la classificazione dei relativi criteri di sicurezza informatica.

Una ricerca

Sulla base delle considerazioni precedenti è stata accettata (ISPELS) una proposta biennale di ricerca avente come oggetto:

Specificazione di una metodologia per l'analisi del rischio dei sistemi informatici utilizzati per monitoraggio e controllo di impianti industriali(SIMC) e per la classificazione dei relativi criteri di sicurezza informatica.