A proposito di Cyber Security

La sicurezza dei sistemi di controllo e automazione industriale diventa sempre più critica in quanto reti diverse sono spesso collegate tra di loro e i sistemi sono integrati in un ambiente di produzione condiviso. Le misure di sicurezza mirano a tutelare la riservatezza, l'integrità e la disponibilità di un sistema informatico dall'essere compromesso a causa di attacchi intenzionali o accidentali. Così come avviene per il processo e la sicurezza fisica, il miglioramento della sicurezza informatica deve essere continuativo. A causa della grande varietà di elementi che devono essere trattati per migliorare la sicurezza del sistema, molte aziende si sforzano per definire la migliore strategia di approccio a questi problemi.

Advertorial

Via Luciano Lama, 33
20099 Sesto S. Giovanni (MI)
www.abb.it

Un elemento chiave nella definizione della migliore strategia per affrontare la sicurezza del sistema è quello di definire diverse aree nel sistema o nell'organizzazione potrebbero essere vulnerabili per violazioni della sicurezza informatica.
ABB ha sviluppato una metodologia rapida e pragmatica per identificare queste aree pericolose, aiutando le aziende a concentrare la loro strategia di cyber-security sulle aree che hanno bisogno di più attenzione. Il Cyber Security Fingerprint di ABB è un approccio standardizzato che raccoglie preziose informazioni sia da diversi attori dell'organizzazione del cliente, sia dalla configurazione e dalle impostazioni dei computer critici.
Sulla base di queste informazioni, il report risultante fornisce raccomandazioni dettagliate per ridurre le vulnerabilità di cyber security e aiuta a sviluppare una strategia di sicurezza mirata e sostenibile per i sistemi di controllo. Questo report descrive i risultati di Cyber Security Fingeprint e fornisce una descrizione dettagliata delle raccomandazioni che miglioreranno complessivamente le misure di cyber security in tutta l'organizzazione e nel sistema di controllo. Mentre la relazione è solamente un indicatore dello stato della sicurezza in un preciso momento, le raccomandazioni in esso contenute non garantiscono comunque un sistema di controllo completamente sicuro. Qualsiasi sistema, indipendentemente dal numero di precauzioni, può essere compromesso.

Cyber Security - Fornire e gestire la sicurezza informatica per sistemi di controllo e automazione industriale è complicato in quanto ci sono sempre continui cambiamenti tecnici, organizzativi e politici. È una sfida complessa che richiede sia misure procedurali sia tecniche. La frequenza degli incidenti di sicurezza è aumentata notevolmente negli ultimi anni. Gli incidenti includono tentativi di intrusione diretti e dannosi, attacchi di virus, worm e altri codici dannosi, e violazioni della sicurezza non intenzionali. Oltre alle minacce di virus e hacker, vi è una crescente preoccupazione per la possibilità di attacchi criminali o terroristici contro le infrastrutture e i processi critici. In passato, le persone con accesso legittimo al sistema sono state la principale causa segnalata degli incidenti di sicurezza. In generale, tali attacchi sono i più difficili da prevenire in quanto gli addetti ai lavori (o ex dipendenti) sono le persone che hanno accesso alle password, ai codici, e ai sistemi così come hanno una conoscenza dettagliata della natura del sistema e delle sue potenziali vulnerabilità. Tuttavia, negli ultimi dieci anni, la quota di incidenti di origine esterna è aumentata drasticamente, in particolare sottoforma di infezioni da virus e worm. In molti casi, collegare un computer portatile o un dispositivo di memorizzazione che è stato precedentemente collegato a un ambiente infetto può provocare infezioni. Gli eventi recenti hanno inoltre dimostrato chiaramente la possibilità di attacchi complessi con obiettivo i sistemi di controllo, realizzati da organizzazioni specializzate e piene di risorse.

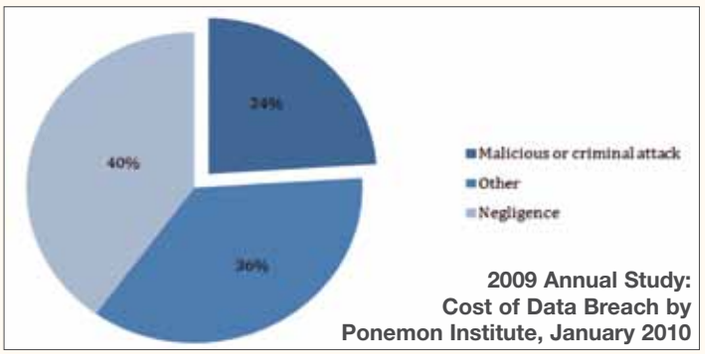
La sicurezza per i sistemi di automazione e controllo industriali è simile a quella applicata per la parte IT, ma permangono un certo numero di significative differenze. I sistemi di automazione e controllo hanno maggiori requisiti di integrità, disponibilità, e prestazioni, nonché la necessità di avere un accesso immediato.
Inoltre, il potenziale impatto di un attacco su sistemi di automazione e di controllo può includere non solo le perdite finanziarie e la perdita di fiducia del pubblico, ma anche la violazione dei requisiti normativi, danni alle strutture e all'ambiente, così come la messa in pericolo della sicurezza pubblica e dei dipendenti.
La sicurezza al 100% non è possibile da ottenere. Un sistema che implementa misure di sicurezza e procedure innovative potrebbe essere ancora vulnerabile a causa delle connessioni alle reti dei fornitori, contractors o partner.
Anche un sistema che è percepito come totalmente isolato dal mondo esterno è vulnerabile a falle di sicurezza da fonti come il collegamento di computer portatili o dispositivi di memoria, l'installazione non autorizzata di software o attacchi deliberati. Recenti studi dimostrano che solo il 24% di tutti gli incidenti di sicurezza informatica è malizioso o di matrice criminale. Il restante 76% è causato da negligenza o dovuto a difetti del sistema. Tale studio ha anche mostrato come il costo di attacchi maliziosi o di matrice criminale risulti più costoso rispetto agli altri.

Cyber Security Fingerprint

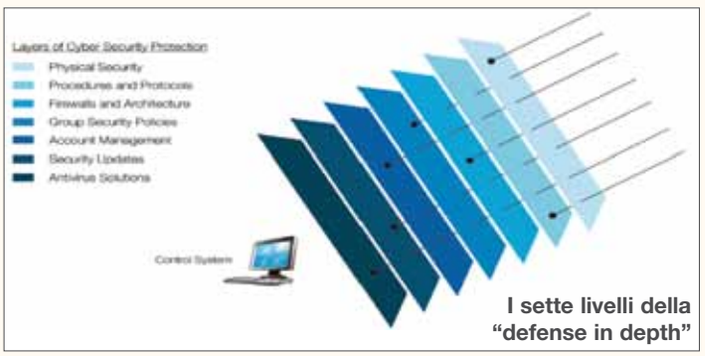
Defense in Depth - Il principio della "Defense in Depth" significa creare più livelli di prevenzione indipendenti e ridondanti. Le misure di sicurezza devono essere stratificate in più punti e diversificate. Questo riduce il rischio che il sistema venga compromesso se una singola misura di sicurezza dovesse essere elusa. La tabella relativa alle aree controllate mostra la corrispondenza tra gli elementi controllati dal Fingerprint e i sette strati di protezione per la sicurezza informatica.

Principio del "Minor privilegio" - Il principio del "minor privilegio" (noto anche come il principio della "minor autorità") richiede che ogni programma, processo o utente (a seconda del soggetto) abbia solo il permesso di accedere alle informazioni e risorse dell'ambiente di elaborazione che sono necessarie per il suo ruolo, scopo o responsabilità. In sostanza, questo significa che sarà necessario fornire un account di accesso con i privilegi che sono essenziali per il lavoro di un utente specifico.

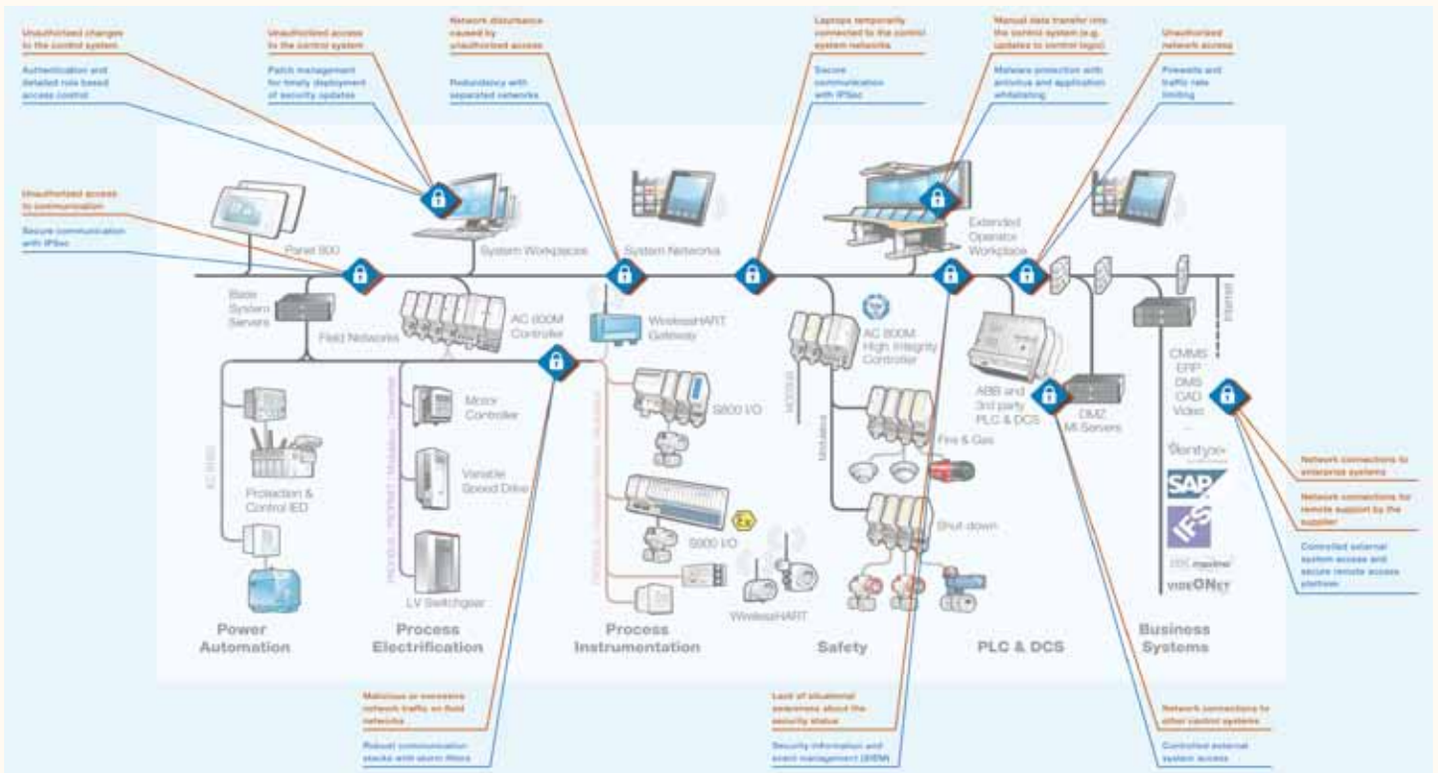
Principio della "Minor funzione" - Simile al principio del "minor privilegio" il principio della "minima funzione" è incentrato sulle funzioni del sistema di controllo. Per esempio non dovrebbe essere installato software non necessario sui computer. Il sistema dovrebbe infatti avere solo ciò che serve per far funzionare un sistema di controllo.



2009 Annual Study: Cost of Data Breach by Ponemon Institute, January 2010



I sette livelli della "defense in depth"



Tutti i sistemi di controllo sono esposti a delle minacce. Il sistema 800XA garantisce un'affidabile protezione sul campo

Advertorial

ABB sviluppa una metodologia rapida e sicura per la sicurezza dei sistemi di controllo e automazione industriale, mediante un approccio standardizzato, aiutando le aziende a concentrare la loro strategia di cyber security sulle aree che hanno più bisogno di attenzione.

Lo scorso giugno 2013, ABB mette a punto un sistema di Cyber Security Security Pacth Update e Antivirus Solution per conto della **Icap Sira** di Parabiago (MI), presso lo Stabilimento di Barberino del Mugello (FI) nella foto.

Il Sistema ABB 800xA 5.0 con CPU Symphony DCI System SIX composto da:

2 Aspect Server; 2 Batch Server; 2 Connectivity Server per DCI; 1 Information Manager; 13 Client.

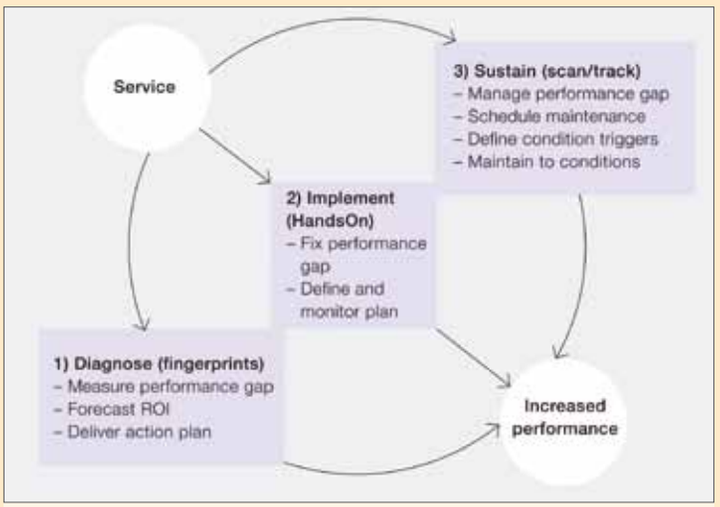
Il servizio prevede:

1) "Security Pacth Update": aggiornamento annuale (effettuato da tecnici ABB) delle Patch di sicurezza rilasciate da Microsoft e certificate da ABB su tutti i Server\Client sopra elencati , utilizzando un sistema automatico di distribuzione degli aggiornamenti Microsoft denominato WSUS.

2) "Antivirus Solution" aggiornamento quadrimestrale (effettuato da tecnici ABB) della definizione degli antivirus rilasciate da McAfee e certificate da ABB su tutti i Server\Client sopra elencati, effettuata da remoto, utilizzando il sistema di accesso remoto di ABB denominato RAP (Remote Access Platform) e il sistema di distribuzione automatica EPO di McAfee.

3) Prima e dopo ogni aggiornamento viene rilasciato al cliente un documento di Benchmark che garantisce il mantenimento delle performance del sistema.

Stabilimento di Barberino del Mugello (FI)



Cyber Security Fingerprint di ABB segue la metodologia dei "3 passi" nei servizi avanzati

Layer multipli riducono drasticamente il rishio di attacchi

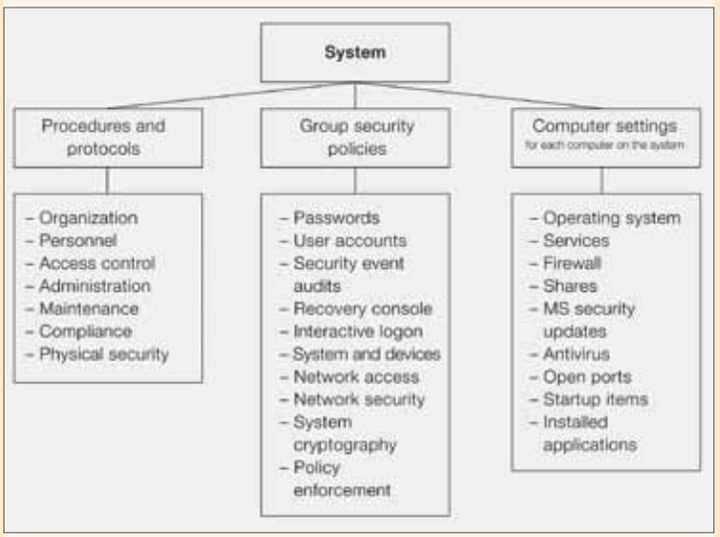


ABB analizza 3 componenti chiave del sistema di controllo dell'impianto per determinare i principali KPI

Affidabilità e semplicità anche nelle applicazioni più complesse?

Sicuramente.

Trasmettitore di pressione 266.
Ancora più semplice e intuitivo nella gestione, con la possibilità dell'innovativa tecnologia TTG (Through The Glass), che permette di programmare il trasmettitore in un gesto, evitando l'utilizzo di costosi configuratori esterni, il nuovo trasmettitore di pressione 266 presenta elettronica e housing innovativi.
Continuità ed esperienza tecnologica sono alla base del 266 che fa dell'efficienza, della sicurezza e dell'usabilità i suoi punti di forza. **www.abb.it/measurement**

ABB SpA
Measurement Products
Field Instruments and Devices, Flow Measurement
Telefono: 0344 58111
Fax: 0344 56278
strumentazione.processo@it.abb.com

Power and productivity
for a better world™

ABB