Implementazione di contromisure di sicurezza in un sistema DCS/ESD operativo

Nel mondo dell'automazione i rischi dell'uso di tecnologia e soluzioni tipiche del mondo informatico sono sottostimati, a volte sconosciuti. Dopo una presentazione delle tecnologie informatiche utilizzate nell'ambito dell'automazione e dei pericoli a loro associati si presenterà una serie di contromisure atte a ridurli, sottolineando la loro efficacia, i limiti e le problematiche della loro implementazione e gestione.

Andrea Padovani
Paolo Cocco

Keyword

Process IT, IT, Cyber Security, Firewall, Antivirus

GLI AUTORI
A. Padovani, Yara Italia,
P. Cocco, Yokogawa Italia

Nelle realtà produttive pre-esistenti all'informatizzazione dell'automazione l'introduzione di questa tecnologia è avvenuta gradualmente, senza una pianificazione generale di realizzazione.
La spinta a questo passaggio proviene dai vantaggi tipici del mondo IT: facile reperibilità dell'hardware, bassi costi, e soprattutto, facilità di integrazione con altre realtà IT.
Il mondo IT è un mondo diffuso e conosciuto: questo semplifica la realizzazione e diffusione di minacce come virus, worm, e le problematiche che gli utenti dei PC sono abituati ad affrontare.
Un'ulteriore problema dipende dai rapidi tempi di sviluppo del mondo IT, specialmente confrontandoli con quelli dell'automazione dove i tempi di ammortamento dei costi sono di un ordine di grandezza superiore: un sistema sicuro può, in tempi brevi, divenire aperto a minacce esterne.

Le principali minacce informatiche per l'automazione

I dispositivi di automazione propriamente detti sono in genere basati su hardware dedicato e software specificatamente progettato, risultando robusti alle principali minacce IT. Al contrario i principali sistemi di interfaccia uomo macchina, basati su PC standard, sono deboli da questo punto di vista.

Virus

I Virus informatici sono la minaccia che con maggior probabilità può colpire una rete informatica di automazione. Lo stesso efficiente sistema di diffusione che li ha resi principale minaccia IT li rende efficienti anche nella diffusione su sistemi di automazione.
È fondamentale considerare che, sebbene esistano worm informatici espressamente progettati per colpire sistemi di automazione, la minaccia proviene principalmente dall'enorme quantità di virus progettata per i normali sistemi IT ma, ovviamente, capace anche di intaccare i sistemi informatici per l'automazione.

Intrusioni informatiche

Intrusioni non autorizzate in un sistema informatico dedicato all'automazione possono risultare estremamente pericolosi. Il rischio è avere interferenze esterne su un sistema di monitoraggio ad un processo produttivo, generando condizioni di oggettivo pericolo, anche per l'incolumità delle persone.
È opportuno ricordare che si sono già presentati intrusioni pianificate per colpire sistemi informatici di automazione: a scopo terroristico, di estorsione e anche per rivalsa da parte di ex dipendenti.

Connessioni con altri sistemi IT (rete di ufficio)

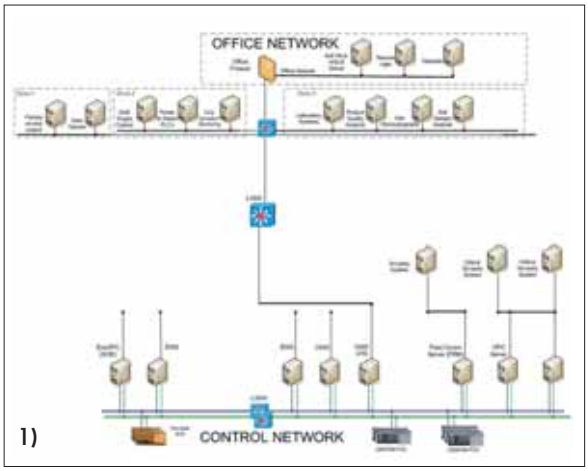
La presenza di una connessione fisica tra un sistema IT generico e uno o più sistemi dedicati all'automazione è un pericolo, potendo rivelarsi un veicolo per diffondere le due precedenti minacce, inoltre presenta un rischio non trascurabile di natura organizzativa.
La responsabilità del sistema IT generico ("rete di ufficio") è affidata a personale differente da quello a cui è affidata la responsabilità del sistema di automazione. Le possibilità che le operazioni eseguite per aumentare la sicurezza dei due sottosistemi e la loro interconnessione siano affette da errore umano aumentano, specialmente per possibili problemi di incomprensione tra i due team.
L'intera progettazione della sicurezza di una delle reti potrebbe basarsi su assunzioni errate riguardo il funzionamento dell'altra, indebolendo le azioni intraprese e consentendo falle di sicurezza.

Sistema isolato

Le reti che maggiormente necessitano sicurezza sono realizzate senza connessione fisiche ad altre reti o macchine. L'unico modo di scambiare dati con queste reti si basa sull'interfaccia umana. Teoricamente questo determina il massimo livello di sicurezza, impedendo l'esposizione ai rischi precedentemente presentati.
In una realtà industriale mantenere un isolamento totale ed efficace è difficile e si deve evitare ogni "rottura" dell'isolamento per errore o incuria umana, dotando il sistema di un controllo forzato per l'accesso fisico (locale chiuso a chiave, monitoraggio in continuo…). Un isolamento efficace è oneroso economicamente e gestionalmente, e riduce l'usabilità del sistema stesso; isolamenti semplici, basati su procedure di uso, sono aperte a falle di sicurezza, per dolo ed errore umano, e possono generare un falso senso di sicurezza.
Inoltre l'isolamento totale prevede la rinuncia al principale motore dell'informatizzazione dell'automazione: l'integrabilità con altri sistemi IT, come l'interconnessione del sistema DCS con sistemi gestionali o amministrativi.

La componente IT nel sistema DCS/ESD

I principali fornitori di sistemi DCS/ESD propongono una architettura di sistema basata su connessioni ethernet ridondate che permette la comunicazione tra i controllori e le stazioni HMI (realizzate con PC), a cui d'ora in avanti ci riferiremo come "control network".
A fianco della control network è possibile trovare connessioni ethernet con sistemi di terze parti, connessi tramite PC utilizzati come gateway o tramite stazioni HMI.

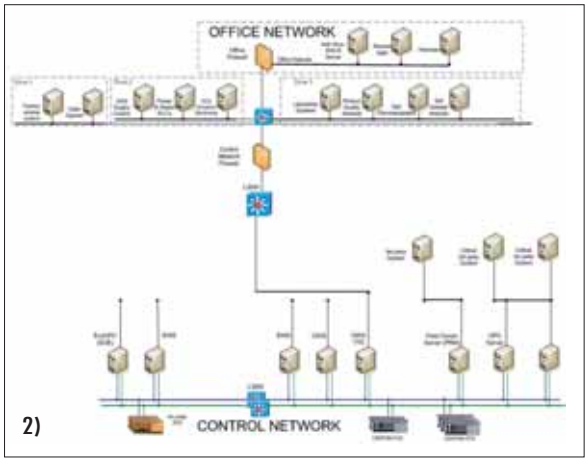


1)

Non da ultimo è possibile avere una interconnessione con la rete IT tradizionale (d'ora in avanti "office network") a scopo di monitoraggio dei dati di processo, reportistica o altro.
L'articolata rete che se ne determina (►**figura 1**) è naturalmente soggetta ai rischi presentati e di conseguenza è opportuno implementare soluzioni di cyber security.

Implementazione di cyber security in un sistema DCS/ESD

Il fondamento di tutta l'implementazione della cyber security consiste in una chiara e definita suddivisione tra la office network (sotto la responsabilità del dipartimento IT) e la control network (sotto la responsabilità del dipartimento automazione come indicato nella ►**figura 2**). A completamento dell'aspetto organizzativo si realizza una modifica dell'architettura, introducendo l'office firewall che crea una separazione tra le due reti, controllando il traffico tra di esse e permettendone la regolamentazione. Il firewall deve essere configurato consentendo il traffico necessario (tipicamente i servizi di Plant Information Management) e bloccando in via precauzionale il restante traffico.



2)

Poiché il ruolo dell'office firewall è proteggere una rete dalle minacce presenti nell'altra rete è difficile assegnare la responsabilità della sua gestione tra i due gruppi coinvolti (IT e automazione), inoltre la disciplina esclusa rimane priva di ogni strumento di protezione, e può solo contare sul lavoro dell'altro gruppo.
Per questo si prevede l'installazione di un secondo firewall (control network firewall): l'office firewall può essere sotto completa responsabilità del dipartimento IT, garantendo la protezione della office network, mentre il control network firewall può essere sotto responsabilità del dipartimento di automazione, garantendo la protezione della control network.
La presenza dei due firewall diminuisce la possibilità di errori umani in quanto le loro configurazioni devono essere armonizzate per consentire comunicazioni lecite tra le due reti: la maggior parte di errori di configurazione si rileva all'atto della messa in servizio dei due dispositivi.
Queste modifiche architetturali identificano con precisione le due reti, ne assegnano chiaramente la responsabilità e instaurano un primo baluardo di difesa della control network dalle minacce esterne.
Un secondo passo fondamentale si basa sul cosiddetto "hardening" dei dispositivi, che consiste nella modifica della configurazione di base di ogni dispositivo (ad esempio password di default) e nella rimozione di ogni servizio non necessario per il funzionamento del sistema di controllo (ad esempio l'inibizione delle porte USB, la disattivazione di servizi del sistema operativo non necessari, …).

Protezione contro i virus

Il firewall non è sufficiente a garantire la protezione da infezioni di virus informatici. Questo dipende sia dalla possibilità che nuovi virus possano passare attraverso traffico apparentemente lecito, sia dal fatto che i virus si possano diffondere tramite i media rimovibili. Negli anni '80 il principale mezzo di diffusione dei virus informatici era il floppy disk: oggi non è da trascurare il ruolo degli USB drive.
Il mezzo più efficace per proteggersi dai virus è l'installazione di un software antivirus, approvato dal fornitore del DCS – compresi i suoi settaggi per non interferire con il sistema – e mantenerlo aggiornato.
La diffusione dei virus è facilitata da ogni

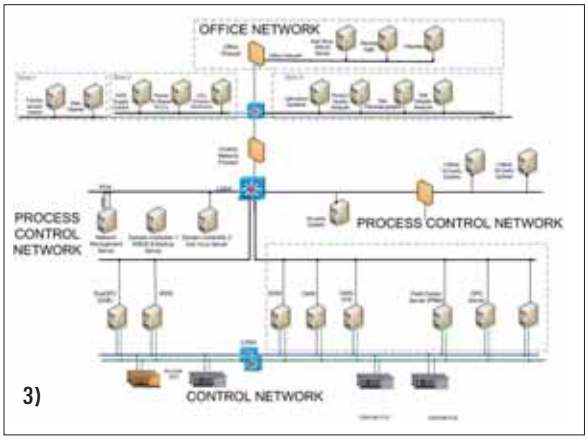
falla di sicurezza del sistema operativo: è determinante garantirne costanti aggiornamenti, sempre previo consenso del fornitore del DCS.
Questa soluzione si scontra con una mentalità diffusa nel mondo dell'automazione: quella di "lasciar il sistema in esecuzione", che prevede una assenza di azione. L'approccio verso la cyber security richiede di spostare la mentalità verso un approccio di "mantenere il sistema in esecuzione", che richiede una azione attiva sul sistema, con tutti i rischi ad essa connessi.
È necessario prevedere un test prima di eseguire ogni aggiornamento, anche se autorizzati dal fornitore del sistema DCS, su macchine esplicitamente identificate la cui mancata funzionalità non crea danni significativi. In caso non esistano queste condizioni è necessario installare appositamente una o più macchine aggiuntive da utilizzare come ambiente di test, mantenendo così il livello di rischio sotto una soglia tollerabile.

Protezione contro intrusioni informatiche

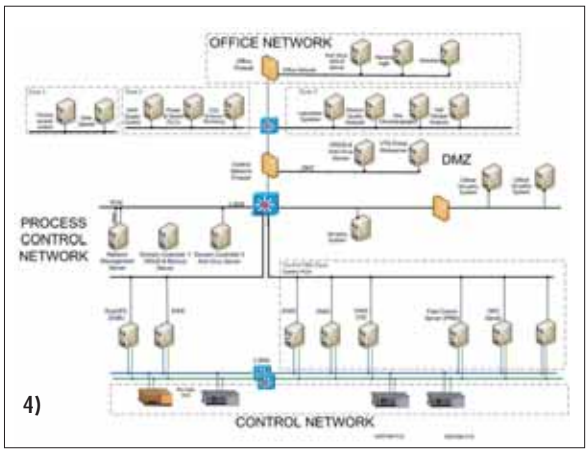
La modifica dell'architettura del sistema, introducendo due firewall, fornisce già un margine di sicurezza contro eventuali intrusioni informatiche; ciò non è sufficiente: non può prevenire una intrusione (dolosa o dovuta ad errore umano) che nasce all'interno della stessa control network.
Il sistema più semplice per proteggersi contro queste minacce è dotarsi di un Network Management Server, PC dedicato all'esecuzione di software NMS (Network Management System). Progettando opportunamente l'architettura della rete, e utilizzando managed switch (switch programmabili e configurabili) è possibile sia mantenere controllo sul traffico esistente sulla rete, sia gestire la configurazione degli switch di rete, disattivando tutte le porte inutilizzate annullando la possibilità di intrusione da errore umano, e rendendo più difficoltosa l'intrusione dolosa.

Impatto della cyber security nell'architettura di un sistema DCS/ESD

Le soluzioni presentate sono efficienti, ma è chiaro che la loro gestione può essere gravosa, in funzione della dimensione del sistema da mantenere, e in funzione degli intervalli di aggiornamento decisi. Già per sistemi di medie dimensioni il carico di lavoro può risultare non ragionevole.
La soluzione ricalca quella implementata già da diversi anni nei sistemi IT: l'implementazione di un sistema di gestione centralizzato tramite la funzionalità Active Directory (AD) di Microsoft Windows (Domain Controller) affiancato da un sistema centralizzato di aggiornamento anti virus (Anti Virus Server) ed a un servizio WSUS (Windows Service Update Services, servizio di aggiornamento del sistema operativo). Per introdurre questi aggiuntivi PC si deve prevedere una modifica dell'architettura, introducendo una rete ad essa dedicata, d'ora in poi chiamata *process control network* (►**figura 3**).



Poiché la funzionalità del domain controller e dell'antivirus server è fornire servizi e gestire i PC in maniera centralizzata ognuna delle macchine presenti nella control network deve avere una connessione alla process control network, tramite la quale le macchine possono ricevere aggiornamenti per il sistema operativo e per l'antivirus, ed essere in generale gestite remotamente dal domain controller. Le principali azioni di sicurezza finora descritte sono realizzabili e gestibili centralmente, con una maggiore efficienza ed un ridotto carico di lavoro.
L'introduzione della process control network permette di collegare ai PC della control network sia le macchine di terze parti sia le macchine di servizio del DCS stesso, in maniera razionale ed organizzata, potendo raggiungere i servizi forniti dal DCS senza ricorrere a connessioni punto-punto. Sfruttando la presenza del domain controller e del server antivirus è possibile utilizzare una soluzione unica per tutte le macchine incluse nella stessa process control network, a prescindere dal loro fornitore. A seconda delle dimensioni della rete può risultare vantaggioso per ottimizzare l'occupazione della banda organizzarla in più sottoreti, collegate tra loro tramite uno switch di livello 3 (router) secondo le normali buone norme di progettazione di una rete ethernet.
Una naturale evoluzione di questa architettura è introdurre la possibilità di aggiornare il WSUS e il server antivirus in maniera automatica; per ottenere una maggiore efficienza e sicurezza si introduce un'ulteriore ramo nell'architettura: la DeMilitarized Zone o DMZ (►**figura 4**).
Una macchina all'interno di questa rete può essere raggiunta dall'esterno, ma non può iniziare comunicazioni all'esterno della propria rete. In caso che i PC all'interno della DMZ vengano violati questi non possono intaccare macchine all'esterno della DMZ, garantendo un elevato grado di sicurezza alla process control network. All'interno della DMZ si installano un anti virus server e un WSUS di appoggio, che ricevono gli aggiornamenti dall'esterno. A loro volta verranno interrogati dal WSUS e antivirus server all'interno della process control network che possono aggiornarsi, senza connessione diretta con la rete esterna riducendo i pericoli associati a questa operazione.
Un ultimo sviluppo all'architettura si ottiene introducendo eventuali reti di terze



parti, che non necessitano contatto diretto con la control network, inserendola tra i firewall office e il control network evitando di appesantire la process control network. Con una opportuna configurazione del control network firewall anche queste reti possono essere gestite tramite i servizi di Network management, AD, WSUS, Antivirus Server.

Principali problematiche nella implementazione della cyber security

L'implementazione della cyber security può essere realizzata in maniera modulare, per fasi successive, distribuendo i costi e le tempistiche di configurazione. Anche un sistema DCS in uso può essere sottoposto alla realizzazione della cyber security con poche attenzioni aggiuntive: lavorando principalmente sulla componente HMI i rischi sono contenuti e, con una buona pianificazione, sostanzialmente eliminati.
Le azioni più determinanti a contenere i rischi hanno un costo di realizzazione minimo. Considerando che la probabilità di una infezione da parte di un virus informatico è svariati ordini di grandezza maggiore della probabilità di subire un tentativo di intrusione va da sé che uno degli aspetti fondamentali della cyber security è avere un sistema antivirus aggiornato. Le più semplici implementazioni richiedono una licenza software per ogni macchina, con costo dell'ordine di decine di euro.
La problematica risiede nelle competenze professionali tipicamente diffuse nel mondo dell'automazione, sensibilmente diverse dalle competenze professionali IT. Una mancata o parziale conoscenza dell'argomento può rendere vano un sistema teoricamente ben progettato. Una mancata fase del processo di hardening, dimenticanza tra le più comuni in caso di carenza di conoscenza, può aprire falle di sicurezza notevoli.
Purtroppo anche nel mondo dei professionisti IT mancano la sensibilità e la conoscenza delle tipiche richieste nel mondo dell'automazione, rendendo arduo trovare figure professionali adeguate all'implementazione della cyber security in una rete di automazioni.
La sfida nella cyber security in un sistema DCS si fonda sulla necessità di avere figure professionali competenti sia nel mondo dell'automazione, sia nel mondo IT, rispettando le richieste di affidabilità e robustezza tipiche dell'automazione, con la mentalità proattiva necessaria – tipica del mondo IT – per agire sui sistemi esistenti mantenendoli sicuri.

Bibliografia

[1] ANSI/ISA-99.00.01-2007 - *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models.*
[2] https://www.tofinosecurity.com/blog/scada-air-gaps-%E2%80%93-technology-or-philosophy.
[3] Jeffrey Hahn, Donna Post Guillen, Thomas Anderson, *Process Control Systems in the Chemical Industry: Safety vs. Security*, Idaho National Laboratory, Control Systems Security and Test Center. Idaho Falls, Idaho (http://www.inl.gov/technicalpublications/Documents/3169874.pdf).
[4] YARA Generic IT Security Design Project - IT Security Design Specification Rev 0.2 Yokogawa Italia.