di Antonella Cattaneo

Foto tratte da http://pixabay.com/

La protezione degli asset di automazione

Parliamo di protezione delle reti industriali per bloccare le minacce informatiche e impedire accessi non autorizzati con alcuni esperti del settore

La scena sta cambiando. Rispetto a qualche anno fa si sta assistendo a un'evoluzione delle minacce alla sicurezza informatica che preoccupa molto le aziende. Internet viene sempre più massicciamente utilizzato dentro e fuori l'azienda e questo rende gli utenti sempre più esposti a minacce non conosciute. È anche cambiato il profilo degli 'hacker', le loro motivazioni… Cosa bisogna fare, allora, nel mondo dell'automazione per mettersi al riparo? Sentiamo cosa ne pensano alcuni dei nostri intervistati: Patrich Villa, product manager Watchguard per Fiore (*www.watchguard.com - www.fioresrl.com*), Alberto Griffini, product manager PLC&Advanced Solutions di Mitsubishi Electric, (*it3a.mitsubishielectric.com*), Raffaele Esposito, product manager Safety, I/O & Networking, Phoenix Contact (*www.phoenixcontact.it*), Giancarlo Carlucci, product manager Plant Solutions - PLC, Networks & I/O di Schneider Electric (*www.schneider-electric.it*), Angelo Candian, head of industrial communication di Siemens Italia (*www.siemens.it*).

Automazione Oggi: L'aumento dell'utilizzo di Internet e delle reti di comunicazione in sistemi di automazione ha obbligato le aziende a rivedere il proprio approccio alla sicurezza. Quali metodologie e strumenti possono consentire l'individuazione di problemi e la risoluzione?

Patrich Villa: Sicuramente l'adozione di apparati dedicati alla sicurezza informatica deve trovare sempre più largo uso in tutte le realtà aziendali. Oggi il mondo UTM (apparati che raccolgono molteplici funzionalità per la sicurezza della rete) si è avvicinato molto in termini di rapporto prezzo/funzionalità anche al mercato della piccola e media impresa e questo permette di alzare la soglia di protezione dei dati anche per questa realtà. La crescita di reti wireless infatti, sia in ambito produttivo/logistico sia office, è una falla nella sicurezza della rete. Perciò l'utilizzo di apparati che dispongono di molteplici livelli di sicurezza, come la cifratura dei dati e l'autenticazione degli utenti, diventano strumenti indispensabili, capaci di ridurre drasticamente questa tipologia di rischi.

Raffaele Esposito: La security di una rete di comunicazione in senso lato - e quindi riferibile anche a quelle reti previste a bordo macchina, linea o impianto industriale - è un aspetto che merita un approccio pieno e consapevole, alla stessa stregua di quello che viene tradizionalmente riservato ad altri aspetti progettuali quali ad esempio la safety, la compatibilità elettromagnetica o i rischi di esplosione, laddove tali elementi trovano applicazione. In prima battuta deve esserci la consapevolezza: per non rischiare di sottovalutare o di tralasciare colpevolmente le esigenze di security di una propria rete di comunicazione deve essere maturata una competenza tecnica che consenta di comprendere non solo le opportunità dell'adozione di una tale tecnologia, ma anche i rischi potenziali ad essa associati. Ovviamente questa competenza tecnica deve anche consentire al progettista di individuare agevolmente, valutare e testare soluzioni tecnologiche dedicate alla limitazione degli utilizzi fraudolenti e quindi non previsti della rete di comunicazione/automazione. Elemento imprescindibile è quindi l'adeguata formazione tecnica. A questo andrà poi aggiunto un approccio programmatico tipico della gestione in qualità di un progetto, con definizione delle responsabilità, dei tempi e modi di valutazione e/o di eventuali interventi (progettazione e implementazione di misure di riduzione del rischio).

Giancarlo Carlucci: L'integrazione tra i sistemi di automazione e le reti di comunicazione digitali, interne o esterne all'azienda, richiede una particolare attenzione fin dalla fase di progettazione. Si devono adottare soluzioni che consentano di proteggere i dati

e l'integrità della rete stessa dal rischio di intromissioni ed errori umani; allo stesso tempo è fondamentale formare il personale affinché sia sensibilizzato alle necessità di sicurezza e ai corretti comportamenti, soprattutto se è data loro la possibilità di interagire con gli asset di automazione attraverso strumenti quali tablet, o PC remoti, cosa che avviene sempre più, ad esempio per le interfacce HMI. Si tratta di integrare il concetto di cybersecurity nell'ambiente industriale, trovando il corretto equilibrio tra la protezione delle reti e il mantenimento delle performance attese dagli asset di automazione; non per tutti gli elementi della rete sarà necessario garantire lo stesso livello di protezione, quindi sulla base di una corretta analisi dei processi, del loro grado di criticità e di rischio nonché del loro livello di apertura verso l'esterno sarà possibile costruire una soluzione di sicurezza adeguata. Gli hardware e software di automazione e controllo hanno oggi caratteristiche che consentono di integrare la sicurezza fisica e logica a bordo di ogni singolo elemento delle macchine o dei processi. Una tendenza che è realtà nei nostri PLC/PAC ad esempio è quella di poter determinare i livelli di accesso, l'attivazione di eventuali servizi http/FTP ecc., garantendo quindi una inviolabilità certificata secondo gli standard Achille L2.

Giancarlo Carlucci, Schneider Electric

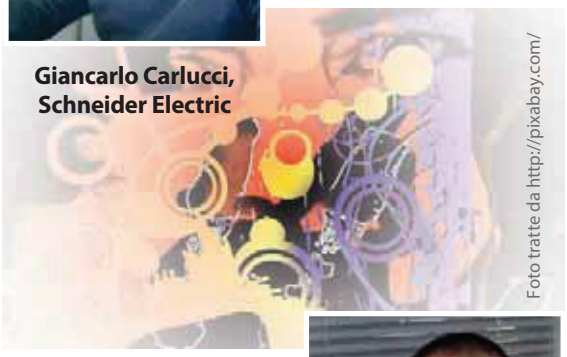

Foto tratte da http://pixabay.com/

Alberto Griffini: L'Industrial Ethernet, inteso come utilizzo di tecnologie Ethernet nell'automazione di fabbrica e nel controllo di processo, ha portato una serie di vantaggi in termini di apertura e flessibilità dei sistemi, ma di contro presta il fianco a possibili problematiche di accessi indesiderati e potenzialmente pericolosi. Per questa ragione la scelta di Mitsubishi Electric di puntare su CC-Link IE, come fieldbus aperto basato su gigabit Ethernet e protocollo realtime, consente di mitigare i rischi di vulnerabilità rispetto a protocolli con stack TCP/IP più comuni nelle reti Enterprise e di conseguenza maggiormente esposti.

Angelo Candian: Non esiste una soluzione standard che può sempre essere applicata perché ogni sistema possiede le proprie condizioni di contorno, diversi rischi e diversi obiettivi di protezione. Ma ci sono procedure collaudate e un numero ragionevole di misure possibili che devono essere prese in considerazione per un concetto di sicurezza efficiente. Le misure di sicurezza individuali hanno sempre lacune e sono quindi insufficienti. Un provvedimento individuale è più facile da by-passare rispetto a diversi in successione. È anche vero che minacce multi-sfaccettate devono essere contrastate con innumerevoli misure. Ad esempio, i virus non possono essere efficacemente contrastati con i firewall, e gli accessi non autorizzati non possono essere neutralizzati con i programmi antivirus. Misure tecniche di protezione non possono coprire tutti gli obiettivi di protezione, il che significa che le misure organizzative sono indispensabili. Così, un solo concetto può ridurre al minimo tutti i rischi e fornire una protezione efficace. Di conseguenza, il concetto Siemens di sicurezza industriale corrisponde a una difesa multistrato, la cosiddetta 'difesa in profondità'. Questo concetto fornisce protezione all'automazione di sistema a tutto tondo e in profondità. Da un lato, questo significa che vari e reciprocamente complementari meccanismi protettivi sono in atto per essere in grado di soddisfare le diverse minacce (protezione a tutto tondo) e, dall'altro, che ci sono diverse barriere che devono essere superate da un potenziale aggressore. Il concetto contiene componenti importanti di sicurezza del sistema, della rete e integrità del sistema.
Con un approccio di 'difesa in profondità' in cui le misure di sicurezza necessarie sono perfettamente intrecciate, è possibile ottenere una completa e affidabile protezione di un sistema automatizzato. Solo l'operatore può in definitiva garantire che il sistema funzioni correttamente, ma il costruttore, ad esempio Siemens, può aiutare fornendo prodotti con funzioni di sicurezza, in modo che i concetti di sicurezza possano essere effettivamente implementati.

Patrich Villa, Watchguard per Fiore

A.O.: Nel mondo dell'automazione si è cercato di adeguare le metodologie tipiche del mondo safety al mondo security con scarso successo. Come è possibile fare una stima del livello di rischio?

Villa: La stima del livello di rischio deve essere fatta analizzando la rete nel suo insieme e individuando i potenziali punti di accesso delle minacce: connettività Internet, servizi pubblicati, punti di accesso wireless e wired, terminali a disposizione degli utenti, metodologie di autenticazione e via dicendo. Si tratta di un processo che richiede competenze informatiche e di networking specifiche oltre che una metodologia che esula da quanto fatto fino ad oggi in termini di safety. È sempre maggiore il numero di società che si sta specializzando in analisi dei rischi e di sicurezza informatica.

Esposito: In linea generale un processo di analisi del rischio prevede fasi successive che possono essere riassunte in modo estremamente sintetico nell'individuazione dei rischi, nella stima degli stessi e in un successivo raffronto di questi rischi stimati con un livello di rischio ritenuto accettabile. Qualora il rischio stimato sia superiore al rischio accettabile, sarà necessario mettere in opera misure di riduzione del rischio. Calando questo processo generale nel mondo della security andrebbero quindi individuate le potenziali vie per un accesso fraudolento alla propria installazione/rete e andrebbero valutate le potenziali conseguenze di un tale accesso

(in senso lato, comprensivo quindi di tutte le componenti quali ad esempio costi di mancata produzione, danni all'installazione, rischi per gli operatori, perdita di dati sensibili e quindi di know-how, danni di immagine…). Se tali conseguenze sono superiori a quelle ritenute accettabili sarà necessario predisporre misure tecniche per evitare accessi indesiderati, scegliendo soluzioni tecnologiche tanto più affidabili quanto maggiore è il range tra rischio potenziale e rischio accettabile.

Angelo Candian, Siemens Italia

Griffini: Benché safety e security riguardino entrambe la sicurezza, si tratta di fattori di rischio e metodi di contenimento differenti (ricordando che un sistema sicuro al 100% non è in genere possibile). L'approccio è quindi in entrambi i casi basato su stime di carattere statistico e le metodologie di calcolo del rischio usate nel campo safety potrebbero in teoria essere adottate anche nel mondo security. In questo senso lo sforzo necessario potrebbe essere quello di identificare e quantificare fattori e probabilità di rischio nella security, ancora invece poco codificati.

Foto tratte da http://pixabay.com/

Alberto Griffini, Mitsubishi Electric

Raffaele Esposito, Phoenix Contact

Candian: Una misura organizzativa è quella di stabilire un processo di gestione della sicurezza. Al fine di prendere decisioni fondate sulle quali le misure abbiano senso, si deve prima analizzare quali rischi concreti non possono essere tollerati. Sia la probabilità di un rischio che si verifichi sia l'eventuale entità dei danni giocano un ruolo decisivo. Se l'operatore omette di effettuare un'analisi dei rischi o non determina gli obiettivi di protezione, vi è un notevole rischio che vengano prese misure inadatte, troppo costose o inefficaci e molti punti deboli non verranno rilevati o sanati.
Gli obiettivi di protezione derivano dall'analisi dei rischi e servono come base per misure tecniche concrete. Le misure devono essere controllate dopo l'implementazione. Il rischio deve essere valutato di volta in volta, e se ci sono stati cambiamenti, perché la situazione 'minaccia' può essere cambiata. A quel punto il processo ricomincia dall'inizio.

A.O.: Ci sono strategie per ridurre l'impatto di tecnologie non sicure in sistemi di automazione? Quale livello di sicurezza devono garantire?

Villa: L'adozione di algoritmi di cifratura certificati e riconosciuti e l'adozione di tecnologie di autenticazione sicure possono già garantire un notevole incremento del livello di sicurezza. Purtroppo ancora oggi queste tecnologie sono viste come accessorie e di difficile implementazione.

Esposito: La proposta di componentistica o di soluzioni attinenti la security aziendale è sufficientemente vasta e in grado di raggiungere livelli di efficacia atti a coprire anche eventuali situazioni di rischio elevato. Una prima soluzione 'entry level' è costituita da accessori meccanici che permettono di impedire l'accesso all'infrastruttura di rete andando, in modo fisico, a impedire la connessione di cavi su porte di connessione disponibili e non utilizzate nell'infrastruttura di rete. Passando a un livello di protezione decisamente superiore, è possibile ricorrere all'uso di managed switch che possono essere configurati in modo da garantire una politica di security multilivello. È infatti di volta in volta possibile agire a livello di accessi qualificati (User Account) permettendo l'accesso a zone nevralgiche solo a personale esperto qualificato (che per poter accedere dovrà ricevere opportuna password). Con i medesimi dispositivi, è inoltre possibile configurare delle Virtual Local Area Network (Vlan), piuttosto che attingere a tutta una serie di protocolli di derivazione IT quali ad esempio Https, Snmp V3 con crittografia, Web/Telnet interface … I managed switch consentono infine anche di definire una politica di accesso dall'esterno alla singola porta mediante la creazione di una 'white list' contenente gli indirizzi MAC dei soli dispositivi che possono dialogare su quella specifica porta. Volendo ulteriormente innalzare il livello di protezione in caso di collegamento da remoto è possibile ricorrere anche a dispositivi diversi, vale a dire i router/firewall industriali. Questi ultimi dispositivi consentono un accesso da remoto estremamente sicuro grazie alla loro gestione di tunnel VPN (Virtual Private Network) permettendo in tal modo una comunicazione crittografata, e quindi sicura, attraverso una rete esterna 'insicura' (ad esempio Intenet). Il firewall integrato consente inoltre la definizione di una politica di comunicazione, permettendo, tramite opportuna configurazione, di consentire o limitare lo scambio dati da/verso l'impianto su determinate porte o in comunicazione con soli ben specifici dispositivi (specifica dell'indirizzo IP).

Carlucci: Ci sono da considerare sia un elemento culturale, sia un elemento operativo. L'elemento culturale riguarda la necessaria azione per rendere consapevoli tutti coloro che operano in ambienti industriali connessi alla rete dei comportamenti corretti e

delle necessarie precauzioni al fine di non causare danni, stabilendo anche correttamente le policy di accesso ai dati e ai sistemi. È un fatto che il principale veicolo di diffusione dei virus nei settori industriali sono i PC e i supporti esterni usati per lo sviluppo e la manutenzione dei sistemi. E la gran parte degli incidenti è di natura non intenzionale. C'è poi l'approccio pratico descritto da documenti e best practice applicate agli hardware e software di sistema. La logica che noi adottiamo nelle nostre architetture, PlantStruxure, è l'approccio DiD (Defence in Depth) basato su sei principi cardine che guidano nella definizione delle difese da incidenti generati da elementi esterni all'infrastruttura del sistema. Si tratta in primo luogo di creare un 'security plan' che individua tutte le vulnerabilità, le procedure e politiche da seguire in caso di incidente, questo fin dalla fase di progettazione di un sistema. Questo è un elemento essenziale per dare risposta rapida e certa in caso di attacchi. Dal punto di vista delle reti, è opportuno stabilire una corretta network separation separando l'automazione di processo e il controllo di sistema da altre reti interne o esterne, creando meccanismi che consentano di far transitare nei due sensi solo il traffico autorizzato: utilizzando VPN, firewall, router; alla protezione deve affiancarsi la segmentazione della rete. Un quarto elemento è la protezione perimetrale attraverso firewall di terza generazione (stateful inspection) che salvaguardi i punti nevralgici dell'infrastruttura di rete. Si può rafforzare ulteriormente la sicurezza utilizzando dispositivi intelligenti che implementino e distribuiscano servizi o controlli direttamente sul campo (device hardening); ultimo ma essenziale punto, l'adozione di un sistema di monitoraggio e di aggiornamento costante dell'infrastruttura di rete.


Foto tratte da http://pixabay.com/

Griffini: Anche per i sistemi di automazione i rischi legati alla sicurezza possono provenire da agenti interni, quali operatori, errori, accessi 'fisici', o esterni come gli attacchi via Internet e i virus. L'approccio a livello aziendale prevede misure di sicurezza, più o meno elevate secondo il potenziale rischio, di tipo tradizionali come VPN, firewall, password ed altre tecnologie più integrate nel prodotto. In particolare nel caso dei nuovi controllori Melsec iQ-R di Mitsubishi Electric sono disponibili 'protection key' di tipo elettronico e filtro indirizzo IP per proteggere il programma CPU e bloccare accessi non autorizzati.

Candian: In primo luogo è importante aumentare la comprensione generale del fatto che le misure di prevenzione devono esistere in modo sistematico, universale e sostenibile anche durante il processo di sviluppo e che devono essere costantemente controllate. Coloro che sono coinvolti attivamente nella strutturazione di questo processo, sia i fornitori sia i reparti di sviluppo, devono porre le basi per certificazioni di sicurezza, ad esempio in conformità con ISA Secure (International Society of Automation) o Nerc-CIP (North American Electric Reliability Corporation - Protezione delle Infrastrutture Critiche). Gli esperti poi esaminano i processi di sviluppo e l'organizzazione interna che vengono valutati sulla base degli aspetti di sicurezza.
L'obiettivo è quello di trovare misure di miglioramento nei processi rilevanti e, se richiesto o ritenuto utile, a introdurre anche nuovi ruoli e responsabilità all'interno dell'organizzazione. I seguenti miglioramenti di processo sono stati introdotti da Siemens nel contesto di tali valutazioni e sono stati raggiunti risultati di miglioramento. Creazione di un nuovo ruolo nel processo di Product Lifecycle Management: esperti di sicurezza dei prodotti controllano il processo PLM e sono responsabili per la sicurezza dei dati di prodotto; creazione di linee guida di programmazione; istituzione di linee guida per la programmazione della sicurezza al fine di evitare punti deboli tramite analisi statistiche nel codice sorgente; istituzione della gestione del rischio per la sicurezza del prodotto; ampliamento del processo PLM Siemens che valuta il rischio per la sicurezza in specifici step PLM e dai quali derivano contromisure. Ottimizzazioni del processo di sviluppo: adattamenti del processo di sviluppo, al fine di aumentare proattivamente la sicurezza contro lo sviluppo di punti deboli; creazione di una sensibilizzazione alla sicurezza in fase di sviluppo; creazione di una consapevolezza tra gli sviluppatori al fine di stabilire la sicurezza industriale come elemento centrale; ampliamento della strategia di prodotto con meccanismi di sicurezza; introduzione dell'integrità dei dati, della riservatezza dei dati e della disponibilità dei dati nei prodotti come elementi fondamentali.

A.O.: Sicurezza nel campo dell'automazione e sicurezza informatica: tra le due c'è un abisso? È colmabile?

Villa: La sicurezza nel campo dell'automazione sarà sempre più legata alla sicurezza informatica, perciò ritengo che la cultura della sicurezza informatica dovrà rientrare gradualmente negli skill del progettista di automazione.

Esposito: Che esista o meno un abisso tra safety e security è una questione di punti di vista. Se ci si riferisce alla conoscenza e alla gestione delle due problematiche da parte dei tecnici progettisti di automazione industriale di sicuro le distanze sono oggettivamente importanti ed è ben naturale che lo siano vista la 'cultura' in ambito safety che da decenni si è sviluppata soprattutto per ragioni di rispondenza a imposizioni di tipo normativo/legislativo, a tutt'oggi ancora non presenti per l'ambito security industriale.
Senza contare che lo sviluppo di soluzioni di automazione con integrazioni di aspetti derivati dall'area dell'Information Technology è cronologicamente molto più recente e non ha quindi ancora avuto modo di sedimentare esperienze tecnologiche/applicative così come è invece ormai largamente accaduto in ambito safety. Se invece ci si riferisce alla disponibilità di soluzioni sia in termini qualitativi sia in termini quantitativi e al supporto da parte dei

fornitori delle stesse, le distanze si riducono enormemente sino a quasi annullarsi. Anche la possibilità di acquisire una buona competenza tecnica è poco diversa: imponente è stato infatti lo sforzo di diffusione dei concetti della security industriale svolto negli ultimi anni da parte di aziende fornitrici, di consorzi, enti e associazioni con innumerevoli interventi in convegni, seminari e workshop che andavano a rispondere alla 'sete di conoscenza' presente sul mercato. Da questo punto di vista, forse, negli ultimi anni, anche a livello di riviste tecniche si è probabilmente disquisito più di security che di safety.

Carlucci: La sicurezza per l'automazione e la cybersecurity non sono affatto separate da un abisso: sono sempre più due elementi che si integrano a vicenda anche se ognuna di esse conserva caratteristiche specifiche. In un contesto in cui sempre più elementi dei processi industriali - uno per tutti, il PLC - comunicano con lo standard IP scambiando dati con una rete industriale o con la rete aziendale, è necessario affrontare in modo olistico la sicurezza fisica e logica.

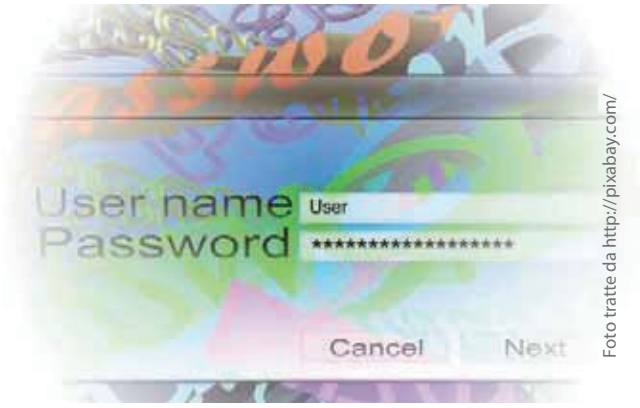

Foto tratte da http://pixabay.com/

Candian: Nello stabilire i concetti di sicurezza, la situazione nell'ambiente di automazione sembra molto diversa da quella in ufficio. Le reti di protezione nell'automazione presentano un'enorme sfida, perché si entra in conflitto con altri requisiti importanti come la capacità di performance, la disponibilità e facilità d'impiego. Inoltre, garantire una rete o sistema sicuro richiede una costante attenzione ai dettagli e possibili adattamenti, il lavoro non termina con una semplice installazione, come nel caso di un normale sistema di automazione. Anche dopo il collaudo, le minacce devono essere valutate e le risposte fornite con adattamenti e aggiornamenti, se necessario, per garantire che il sistema rimanga sicuro.

A.O.: Analizzando i dati relativi a incidenti su reti e sistemi di fabbrica si è notato che i due terzi degli incidenti viene generato dall'esterno. A tal proposito gli americani avevano pubblicato un documento '21 step to improve cyber security of Scada networks'. Cosa ne pensate?

Villa: Lo ritengo un documento interessante, più che per i contenuti tecnici, a mio avviso pochi, per la volontà di sensibilizzare il mondo dell'automazione sul tema suggerendo le domande alle quali bisogna trovare risposta per realizzare un sistema sicuro.

Esposito: Il fatto che i due terzi degli incidenti sia dovuto ad accessi da esterno/remoto non sorprende se si pensa alla quantità di persone che può potenzialmente accedere a una rete da una porta locale non adeguatamente protetta (i soli operatori che hanno accesso fisico al luogo) e alla quantità di persone che possono invece potenzialmente accedere alla rete da remoto per magari un collegamento a Internet non adeguatamente protetto. Il documento citato si riferisce in particolare a reti che includono dispositivi Scada (le cosiddette 'Scada Network') utilizzate nell'ambito della gestione delle infrastrutture di servizi essenziali (distribuzione energetica, distribuzione e depurazione delle acque, automazione di mezzi di trasporto….) e ha quindi una visione precisa e che non sempre collima con le specificità di una soluzione di automazione industriale più puramente produttiva. Nonostante questo aspetto, l'approccio suddiviso in aspetti tecnici legati specificatamente al prodotto (in questo caso lo Scada) e in aspetti gestionali/organizzativi maggiormente incentrati su una politica globale di management della security può costituire una valida guida per applicazioni più generali.

A.O.: In poche parole quindi qual è l'elemento che ogni azienda deve considerare al fine di non essere 'vulnerabile' e quale la stima del rischio?

Esposito: L'aspetto chiave è quello di non fornire punti di accesso al network non adeguatamente protetti in funzione delle modalità di strutturazione e configurazione di rete. Quando esiste solo un possibile accesso da locale bisognerebbe prestare attenzione a porte libere in quanto magari in esubero rispetto alle necessità specifiche dell'applicazione su componentistica utilizzata. Anche la settorializzazione delle zone di accesso con un'adeguata politica di User Account può limitare gli accessi indesiderati alle aree a maggior rischio. Negli accessi da remoto (teleassistenza, telecontrollo, cloud) è fondamentale definire adeguate politiche di accesso e proteggere i dati scambiati qualora gli stessi debbano attraversare delle reti esterne delle quali non si ha certezza circa un adeguato livello di security. Qualora infine siano presenti infrastrutture di rete anche per comunicazioni di tipo wireless, si dovranno prendere opportune precauzioni al fine di impedire accoppiamenti di dispositivi esterni alla rete o di acquisizione fraudolenta dei dati scambiati.

A.O.: Quale la competenza che deve essere fornita per far fronte ad attacchi?

Esposito: Fondamentale la conoscenza dettagliata delle potenzialità tecniche dei dispositivi, dei protocolli e delle soluzioni utilizzate al fine di poter valutare appieno le modalità di scambio dati e di accesso ai dispositivi o alla rete nella propria interezza. Solo in questo modo è possibile identificare eventuali falle nel sistema attraverso le quali vi è il pericolo di subire accessi fraudolenti potenzialmente rischiosi o dannosi per la propria applicazione. Altrettando fondamentale è ovviamente la competenza necessaria per utilizzare quelle soluzioni tecnologiche disponibili sul mercato che consentono di rispondere in modo adeguato ai rischi presenti.