La sicurezza in reti e sistemi di controllo

Enzo Maria Tieghi

Questo articolo tratta sicurezza intesa come Cyber Security per applicazioni industriali (sistemi di controllo e automazione, reti e infrastrutture). Si illustrano alcuni concetti relativi a standard quali BS7799 per la gestione di sistemi per la sicurezza delle informazioni e si evidenziano le differenze tra la security in ambiente Information Technology (IT) e la security nelle applicazioni in ambiente produzione. Tali differenze sono trattate da alcuni nascenti standard come ad esempio ISA SP99.

La Norma ISO/IEC 17799 fornisce delle raccomandazioni per l'implementazione di Sistemi per la Gestione della Sicurezza delle Informazioni (Sgsi) utili per chi all'interno dell'organizzazione deve disegnare, implementare e mantenere la sicurezza delle informazioni.
Questa norma dà una base comune per sviluppare regole per la sicurezza delle organizzazioni e per il disegno, l'implementazione, la manutenzione, il possibile miglioramento dei sistemi utilizzati in azienda, compresi quelli per la produzione e la gestione degli impianti.
La ISO/IEC 17799 è un insieme di controlli/contromisure secondo le best practices nella sicurezza dei sistemi informativi, ed è riconosciuta a livello internazionale come standard di riferimento per la sicurezza delle informazioni.
La Norma BS7799:2.2002 è la nuova edizione della BS7799-2:1999 (che risulta quindi obsoleta).
Questa nuova edizione è stata pensata perché si armonizzi con le altre norme sui Sistemi di Gestione, come la EN ISO 9001:2000 e la EN ISO 14001:1996, allo scopo di fornire attuazioni e operazioni dei Sistemi di Gestione che siano coerenti e integrate. La BS7799 introduce anche un modello Pdca (Plan-Do-Check-Act) vale a dire "Pianifica-Realizza-Controlla-Migliora" come parte dell'approccio ai Sistemi di Gestione per sviluppare, attuare e migliorare l'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni dell'organizzazione (Sgsi).
Gli obiettivi del controllo e i controlli/contromisure ai quali fa riferimento la BS7799-2:2002 derivano direttamente dalla ISO/IEC 17799:2000 e a questa sono allineati. La lista degli obiettivi di controllo e dei controlli/contromisure che qui di seguito andremo a elencare non è esauriente e un'organizzazione potrebbe voler prendere in considerazione ulteriori obiettivi di controllo e ulteriori controlli/contromisure, soprattutto in base alla analisi e alla valutazione dei rischi effettuata.
Non tutti i controlli descritti sono rilevanti per ogni situazione, né potranno tenere conto di vincoli locali ambientali, tecnologici ecc.
Occorre notare che gli Utenti, singoli responsabili delle informazioni e dei sistemi da loro gestiti per trattare/elaborare le informazioni, sono i responsabili per la corretta applicazione della BS7799.

E.M. Tieghi, Vision Automation

Cos'è la sicurezza delle informazioni?

Le informazioni sono dei beni e, come ogni altro bene aziendale, hanno un valore: quindi devono essere protette in modo adeguato.
La sicurezza delle informazioni protegge le informazioni da una moltitudine di minacce allo scopo di assicurare la continuità aziendale (quindi anche della produzione), minimizzare i danni aziendali, massimizzare il rendimento del capitale investito, migliorare l'efficienza e l'efficacia.
La Sicurezza delle Informazioni è vista come la preservazione di: *Riservatezza* (Confidentiality) - assicurarsi che le informazioni siano accessibili solo a chi è autorizzato ad averne accesso; *Integrità* (Integrity): salvaguardare l'accuratezza e la completezza delle informazioni e dei beni collegati quando necessario; *Disponibilità* (Availability): assicurarsi che gli utenti autorizzati abbiano accesso alle informazioni e ai beni collegati quando necessario.

Valutare e gestire i rischi

Tra le fonti per identificare i requisiti della sicurezza per una organizzazione abbiamo l'Analisi e Valutazione del Rischio, intesa come la valutazione delle minacce, dell'impatto, delle vulnerabilità delle informazioni e degli impianti di elaborazione delle informazioni, e la probabilità del loro verificarsi.
La valutazione del rischio è quindi una sistematica considerazione: dei danni aziendali che possono derivare da mancanze nella sicurezza, tenendo conto delle potenziali conseguen-

ze della perdita di riservatezza, integrità o disponibilità delle informazioni o altri beni; la realistica possibilità che si verifichi una tale mancanza alla luce di minacce e vulnerabilità, con i controlli/contromisure presi.
I risultati della valutazione porteranno alla gestione del rischio, inteso come il processo per identificare, controllare, minimizzare o eliminare i rischi inerenti alla sicurezza che possono incidere sui sistemi di informazione, a un costo accettabile.

La sicurezza delle informazioni non è un prodotto: è un processo

Un sistema non è possibile che sia sicuro al 100%, e di solito, un sistema "vive" in quanto soggetto a cambiamenti, che possono anche solo riguardare il contesto in cui è installato e le persone che lo utilizzano.
Inoltre la sicurezza è un processo, e in quanto tale deve essere tenuto alimentato dal momento in cui viene ipotizzato l'utilizzo del sistema e fino al momento successivo a quello in cui il sistema viene dismesso: bisogna quindi essere pronti a condurre altre analisi del rischio anche in momenti successivi alla implementazione del sistema stesso, quando possano variare non solo il sistema ma anche le condizioni a contorno.
La sicurezza delle informazioni non è un prodotto, un'appendice che si possa "attaccare" in modo posticcio al sistema che si sta valutando.
La sicurezza è un processo che nasce ancora prima del sistema: la sicurezza deve essere "pensata" insieme a tutti gli altri requisiti del sistema, e su questo punto la norma BS7799 non transige.
Ma non solo. La sicurezza non "finisce" mai: siamo noi che dobbiamo continuamente pensare alla sicurezza, per fare in modo che la sicurezza del nostro sistema di informazione rimanga attuale, e non conceda varchi a vulnerabilità e minacce che non abbiamo neanche ipotizzato al momento della sua nascita e che oggi o domani potranno divenire vulnerabilità o minacce reali.
Proprio nell'ottica del processo Plan-Do-Check-Act, "Pianifica-Realizza-Controlla-Migliora".

La norma BS7799 e i sistemi Scada

Come molti altri sistemi che gestiscono informazioni all'interno dell'organizzazione dell'azienda, anche i sistemi Scada utilizzati in produzione fanno parte di processi spesso critici per l'azienda.
La continuità della produzione, l'affidabilità dei propri impianti permettono all'azienda di mantenere e migliorare le proprie quote di mercato e la propria reputazione.
Il fatto di poter conoscere in dettaglio come si sta comportando il nostro impianto, cosa stiamo producendo, come lo stiamo producendo, le rese, gli scarti e ogni altra informazione relativa alla produzione e ai prodotti che escono dalla linea e vengono instradati nella supply chain, molto spesso è anche un preciso requisito per poter continuare a rimanere sul mercato.
Pensiamo alla produzione in ambienti regolamentati (quali i farmaci o i prodotti per la cura personale) oppure ancora bevande e alimenti: in questi ambienti esistono precise norme cogenti quali quelle imposte dalla FDA (Food & Drug Administration - USA), dal Ministero della Salute, oppure da regolamenti della Comunità Europea, come ad esempio il Regolamento (CE) n.178/2002 del Parlamento Europeo e del Consiglio del 28 gennaio 2002, che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare.
Negli ultimi anni, con l'insorgere dell'emergenza terrorismo, ci si è resi conto che anche molti sistemi che gestiscono le cosiddette infrastrutture, come ad esempio gli impianti degli acquedotti, delle centrali elettriche (nucleari e non), le reti di distribuzione energia, acqua, gas, telecomunicazioni ecc. possono essere obiettivi "critici" e in quanto tali devono essere protetti. Proprio in questa direzione sono state lanciate iniziative specifiche, come ad esempio quella avviata direttamente dalla Casa Bianca con l'edizione del manuale "21 Steps to Improve Cyber Security of Scada Networks".

ISA S99: Manufacturing and Control System Security

Il comitato ISA SP99 per la sicurezza nei sistemi di controllo e automazione ha iniziato la sua attività già da qualche anno e durante il 2004 ha iniziato a rilasciare per la pubblicazione i primi due Technical Report dai titoli: SP99-TR1 Technical Report 1 - Security Technologies for Manufacturing and Control Systems; SP99-TR2 Technical Report 2 - Integrating Electronic Security into the Manufacturing and Control Systems Environment.
A fronte di questi documenti sono già previsti e in elaborazione i diversi capitoli del nascente standard denominato ISA-99 che affronteranno i seguenti argomenti: ISA-99.00.01 - Manufacturing and Control System Security Part 1: Models and Terminology; ISA-99.00.02 - Establishing a Manufacturing and Control System Security Program; ISA-99.00.03 - Operating a Manufacturing and Control System Security Program; ISA-99.00.04 - Specific Security Requirements for Manufacturing and Control Systems.

La sicurezza dei sistemi di controllo e automazione

La security in ambiente Information Technology (IT) è da diversi anni un tema all'attenzione dei responsabili di sistemi, reti e infrastrutture informatiche. Solo negli ultimi tempi, con il proliferare delle tecnologie IT anche in ambiente di fabbrica si è iniziato a guardare con più interesse e cognizio-

ne al tema security anche in ambienti industriali finora assolutamente considerati immuni da problemi relativi a incidenti tipici del mondo IT, quali intrusioni, perdita di dati e caduta di sistemi e reti dovuti a software malevoli.
Si è allora iniziato a studiare il problema e presto si è giunti alla conclusione che non tutti i metodi di protezione utilizzati nei settori IT tradizionali sono applicabili al mondo dell'"IT di fabbrica": in particolare sono stati evidenziati 11 motivi per i quali la Sicurezza di sistemi di controllo in produzione (DCS, PLC, Scada/HMI, reti di fabbrica ecc.) è differente da quella dell'IT.
A supporto di ciò riportiamo quanto viene menzionato nel documento ISA-TR99.00.02 "Integrating Electronic Security into the Manufacturing and Control System Environment", all' Art. 6.5: "Special Considerations for Manufacturing and Control Systems… Manufacturing and Control System electronic security plans and programs are *consistent with*, and build on, *existing IT security* experience, programs, and practices. *However*, there are critical operational differences between IT and Manufacturing and Control Systems that influence how *specific measures* should be applied. (…)".

La gerarchia funzionale dei sistemi

Nella figura 1, vengono evidenziati i livelli definiti nello standard ANSI/ISA95 relativi ai diversi livelli di gerarchia funzionale dei sistemi in ambiente industriale: tale struttura è richiamata anche nel nascente standard ISA99. ISA S99 si occupa della security dal livello zero al livello tre compresi.

Le "Doti dell'informazione": Disponibilità, Integrità e Riservatezza

Il diagramma che segue evidenzia le differenze negli obiettivi della security IT (richiamati a destra) rispetto a quelli del-

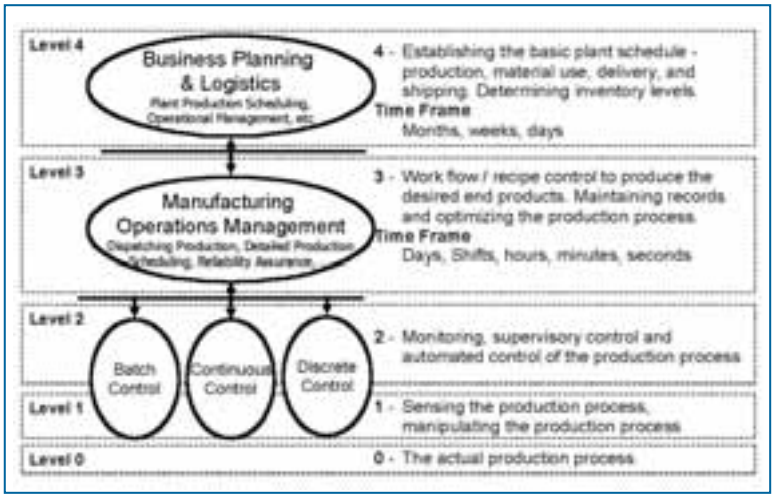

Figura 1 - I livelli gerarchici dello standard Ansi/ISA95

Figura 2 - Confronto tra gli obiettivi ISA-99.00.01

la security in ambiente di produzione e sistemi di controllo (a sinistra). Abbiamo infatti già evidenziato precedentemente che per la BS7799 i capisaldi della Security risiedono nel garantire Riservatezza, Integrità e Disponibilità dell'informazione (in questo ordine). Nei sistemi di controllo le qualità più preziose per l'informazione sono Disponibilità e Integrità, mentre spesso Riservatezza assume un'importanza molto inferiore.

Perché la Sicurezza IT è diversa da quella "industriale"?

I rischi sono diversi!
Sistemi IT: la perdita di dati e informazioni, file e documenti, provocano ritardi di transazioni e incidono sul business (risorse, tempo, soldi)…
Sistemi di controllo: oltre a quanto previsto per i Sistemi IT, la non sicurezza dei sistemi può incidere sull' integrità fisica di persone (salute, incidenti sul lavoro, rischio ambientale e territoriale) e sulla conservazione di impianti di produzione e cose (risorse, tempo, soldi, macchinari…).

L'architettura di rete è diversa!
Sistemi IT: architettura client-server, con gestione di rete con particolari punti critici (solo i server?).
Sistemi di controllo: gli stessi "client" sono dei "server" di dati critici e real-time distribuiti sulla rete (Controllori/DCS, PLC, Scada/HMI, CNC, DNC ecc.).

I requisiti di disponibilità sono diversi!
Sistemi IT: attività nel normale orario di ufficio e possibilità di gestire fermate e/o "re-boot" per eventuali manutenzioni.
Sistemi di controllo: in molti casi sempre attivi 24/24h, 7/7gg in impianti a produzione continua o secondo turni e lotti di produzione. Fermare i sistemi non è possibile senza fermare la produzione!

Conseguenze a volte difficilmente prevedibili
Sistemi IT: in IT la conseguenza è la perdita di dati.
Sistemi di controllo: le conseguenze dipendono dal processo controllato.
Tutte le funzioni devono essere verificate affinché non aggiungano vulnerabilità al sistema e al processo.

Tempi critici per le interazioni
Sistemi IT: in situazioni di emergenza ci sono procedure per la salvaguardia dei dati, la chiusura delle applicazioni, lo shutdown dei sistemi…
Sistemi di controllo: le reazioni in situazioni di emergenza devono essere rapide ed efficaci. Le informazioni critiche devono essere aggiornate sotto gli occhi degli operatori; a volte non c'è tempo per richiedere password per autenticazioni o autorizzazioni.

I tempi di risposta richiesti e il traffico di rete sono diversi
Sistemi IT: il throughput e le prestazioni della rete sono prevedibili e spesso non sono critiche.
Sistemi di controllo: non sono accettabili ritardi negli azionamenti, nella rilevazione dei dati da sensori e controllori. I "telegrammi" di dati sono brevi e frequenti. Spesso non è necessario un alto "throughput" della rete, ma è necessario garantire le prestazioni.

I software di sistema sono diversi
Sistemi IT: software di sistema e sistemi operativi noti e collaudati per attività di gestione informatica.
Sistemi di controllo: i SO possono essere diversi, oppure sono gli stessi dei sistemi IT, ma usati in modo diverso: le regole abituali nel mondo IT spesso non sono praticabili.
Che sistema operativo o che scheda di rete hanno un PLC o un DCS? Lo skill delle persone è diverso da personale IT.

Limitazioni delle risorse hardware e software
Sistemi IT: IT definisce i requisiti hardware e software dei sistemi e gestisce manutenzione e aggiornamento, secondo regole e procedure di sicurezza informatica.
Sistemi di controllo: Spesso hardware e software sono "speciali" e forniti insieme a tutto il sistema.
Non si può aggiornare l'uno o l'altro secondo le richieste della sicurezza IT.

Integrità di dati e informazioni
Sistemi IT: i dati sono sui server e difendibili con le "regole del RID" (Riservatezza, Integrità, Disponibilità).
Sistemi di controllo: i dati e le informazioni arrivano direttamente da sensori, controllori e sottosistemi: la loro integrità è essenziale e spesso non controllabile.
Necessitano precauzioni specifiche per eliminare eventuali fonti di corruzione dei dati e intrusioni.

Le comunicazioni sono diverse
Sistemi IT: i protocolli e i mezzi di comunicazione sono di solito noti e legati a standard (TCP/IP ecc.)
Sistemi di controllo: i protocolli e i mezzi di comunicazione sono diversi, spesso proprietari o specifici per l'applicazione: reti tra PLC, DCS, CNC/DNC, comunicazioni seriali asincrone con RTU ecc.

Aggiornamenti Software
Sistemi IT: IT aggiorna costantemente all'ultima release del software di sistema o applicativo per garantire la manutenibilità, le performance e la sicurezza.
Sistemi di controllo: difficilmente si possono installare patch di software di sistema o applicativo: prima è necessario un test accurato di ogni componente per verificare impatti con gli altri componenti e moduli del sistema, verificare che non si infrangano regole di validazione.

Alcuni riferimenti e standard per la security industriale

Di seguito evidenziamo alcuni standard e riferimenti dai quali possiamo trarre indicazioni in tema di security nelle applicazioni industriali.

Riferimenti

[1] BS7799-2:2002, Information security management systems - Specification with guidance for use.
[2] ISO/IEC 17799:2000, Information Technology - Code of practice for information security management.
[3] ISA SP99 TR1, Security for Manufacturing and Control Systems (ISA-TR99.00.21-2004)
[4] ISA SP99 TR2, Integrating Electronic Security into Manufacturing and Control Systems Environment (ISA TR99.00.02-2004).
[5] ISO/IEC 15408, Common Criteria.
[6] Nist, System Protection Profile for Industrial Control Systems (SPP-ICS).
[7] Cidx Chemical Industry Data Exchange - Cibersecurity Vulnerability Assessment Methodology (VAM) Guidance.
[8] Gamp 4, Good Automated Manufacturing Practices - App. O Guideline for Automated System Security.
[9] *21 Steps to improve Cyber Security of Scada Networks*, Ufficio di Presidenza degli USA.
[10] *Common vulnerabilities in critical infrastructure control systems*, U.S. Dept. Of Energy's National Nuclear Security Administration.
[11] *Securing Process Control Systems* - IT Security (Europarlamento).
[12] National Strategy to Secure Cyberspace: www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
13] ISA SP99, Ansi/ISA SP95.00.01 (IEC/ISO 6226401) , Ansi/ISA SP95.00.02 (IEC/ISO 6226402 draft), Instrument Society of America: www.isa.org
[14] Critical Infrastructure Protection: Cybersecurity of Industrial Control Systems: www.mel.nist.gov/proj/cip.htm
[15] Process Control Security Requirements Forum (Pcsrf): www.isd.mel.nist.gov/projects/processcontrol/