Industria 4.0 e interconnessione. Dai modelli di processo "pacchettizzati" al Risk Management-based model

Date : 27 settembre 2017

La consulenza in ambito ICT offre **scenari operativi incredibilmente stimolanti**, in particolare oggi che Industria 4.0 e Open Innovation stanno pian piano riducendo le storiche differenze tra PMI e Grandi Aziende.

Il vero discrimine nel modo di affrontare le sfide portate dall'innovazione tecnologica è infatti la qualità delle tecnologie da implementare all'interno di un'infrastruttura IT, non tanto il livello occupazionale o la complessità organizzativa della struttura aziendale.

L'effort di risorse temporali, economiche, logistiche dedicato all'IT è cresciuto esponenzialmente, dettato - secondo gli analisti - da esigenze operative imprescindibili e dall'evoluzione tecnologica, non più (solo) da normative perentorie da soddisfare in tempi prestabiliti (a meno delle consuete, molto italiche, proroghe).

Vecchi modelli di processo

L'inesorabile tramonto dei tempi della stesura del c.d. D.P.S. (documento programmatico sulla sicurezza) - spesso vissuto come un inutile orpello burocratico - è stato formalmente sancito dal Decreto Legge n. 5 del 9 febbraio 2012, convertito dalla legge n. 35 del 4 aprile 2012. L'aspetto interessante, qui oggetto di riflessione, è il fatto che sia stato il trend tecnologico a decretarne ancora prima la morte.

Non vi sono dubbi che già molti anni fa esistesse un (limitato) numero di aziende decise ad affrontare seriamente la tematica della sicurezza IT in modo lungimirante, trovando all'interno dei ruoli aziendali o in out-sourcing figure professionali in grado di avere una **visione olistica a 360°** delle varie criticità. Tuttavia, la natura stessa delle regole di stesura originariamente pensate per il D.P.S. portava inevitabilmente molte aziende a ricercare soluzioni pacchettizzate grossomodo compilabili o, peggio, ad effettuare rocamboleschi "copia e incolla" da fonti eterogenee e di dubbio spessore. Il risultato: un burocratico orpello "100% compliant" (si fa per dire).

Talvolta, in occasione di seminari o convegni, ci piace raccontare un aneddoto risalente nel

tempo, quando ci trovammo coinvolti nella stesura di un D.P.S. per un'azienda di medie dimensioni e nella formazione di quello che doveva essere il "Responsabile della Sicurezza" (ruolo chiave, in tale contesto). Ci era stato richiesto dal CEO dell'azienda di svolgere, su una specifica figura professionale interna all'azienda, un'attività di formazione molto intensa e puntuale, oltre che onerosa; e così facemmo. Peccato che a incarico svolto, ratificato il Documento ed apposte le firme di rito per l'archiviazione, due giorni dopo venimmo a sapere che tale figura professionale, accuratamente formata, venne "lasciata a casa" per scadenza di contratto, senza nemmeno un passaggio di consegne. Naturalmente il Consiglio Direttivo era a conoscenza del fatto che tale collaborazione sarebbe terminata in breve tempo, ma evidentemente non era stata percepita l'importanza di avere nell'organigramma una figura professionale "stabile" in grado di interfacciarsi con i consulenti esterni per gestire eventuali criticità e gestire in modo opportuno le tematiche di sicurezza & privacy, anche al fine di poter intervenire in modo adeguato in caso di incidenti (c.d. "data breach").

Ipotizzare un approccio di questo tipo oggi, qualunque sia il limite occupazionale e finanziario del contesto aziendale in esame, è oggettivamente inattuabile se si vogliono mantenere obiettivi concreti in grado di portare vantaggi tangibili alla realtà produttiva. Senza dimenticare il nuovo obbligo di notifica all'Autorità di controllo di cui all'art. 33 del Regolamento UE 2016/679, di prossima "applicazione" (v. *infra*).

Definitivamente tramontato il vecchio approccio per modelli di processo "pacchettizzati", la c.d. **Quarta Rivoluzione Industriale** trova la sua perfetta collocazione all'interno di questo nuovo e virtuoso scenario.

Un nuovo approccio alla valutazione dei rischi

La famiglia di certificazioni ISO/IEC 27001 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) ha costituito, e costituisce, un ottimo preambolo operativo in tema di qualità di standard internazionale a tutto ciò che porta alle attività della Smart Factory 4.0.

Introdotta nel 2005 (la versione italiana UNI è del 2006), questa Norma offre la possibilità di realizzare un **sistema completo di gestione delle informazioni digitali** con un effort di risorse e una profondità analitica decisamente superiore a qualunque altro approccio utilizzato negli anni precedenti. Si tratta senza dubbio del primo e reale *process modeling* in grado di portare gli attuatori a seguire un approccio di *Risk Management* dotato della rigorosità matematica necessaria e degli strumenti analitici adeguati per raggiungere gli obiettivi preposti.

Le 4 attività fondamentali già stabilite nelle linee guida per la ISO/IEC 27001 ed ereditate dai Sistemi per la Gestione della Qualità ISO 9000 (Pianificazione e Progettazione, Implementazione e Sviluppo, Monitoraggio, Mantenimento e Miglioramento) ben si applicano ai contesti in cui l'azienda si sta muovendo con decisione verso Industria 4.0, ove è indubbio che Imprese già certificate o in fase di certificazione posseggano già un *mindset* fondamentale per affrontare le sfide dell'Open Innovation.

L'approccio dettato dal Risk Management risulta particolarmente interessante qualora vi sia la

necessità di soddisfare e realizzare i requisiti di **interconnessione** informatica all'interno dell'infrastruttura ICT dell'azienda, attività fondamentale nel contesto italiano Industria 4.0 poiché la giovane normativa prescrive che la Smart Factory debba poter contare su una **gestione informativa globale solida, capillare e sicura**. Se dal punto di vista degli obiettivi macroscopici essa è in grado di garantire l'accesso a una cospicua serie di agevolazioni in termini di credito di imposta, per quanto riguarda il QoS (Quality of Service) reale percepito da parte degli addetti ai lavori si ha come side-effect (ancorchè sia riduttivo definirlo così) un incremento notevole delle performances attese da tutto ciò che rientra nella gestione del flusso informativo aziendale. Tipicamente, infatti, il posizionamento su rete locale interna era attività riservata a dispositivi pc-like, macrofamiglia in cui far ricadere allo stesso modo pc, laptop, smartphones o altre tecnologie dotate di un sistema operativo a interfaccia utente grafica e con alti canoni di usabilità.

Gli aspetti sistemistici inerenti la sicurezza, su tali dispositivi, possono contare su figure professionali dedicate e su uno storico di casi d'uso estremamente ampio maturato negli anni dell'informatica moderna, ma allo stesso modo in continua evoluzione. I recenti gravi danni causati da softwares malevoli quali i famigerati **ransomware** hanno posto l'accento sul fatto che la gestione della sicurezza non possa essere racchiusa in attività pacchettizzate nella quali l'obiettivo finale risulti un punto di arrivo definitivo e stabile, a causa dell'adattamento alle "condizioni ambientali" di tale tipologia di sistemi di hackeraggio e alla loro continua evoluzione. La "**sicurezza by design**", tematica che negli ultimi anni sta richiedendo la formazione di figure professionali *ad hoc*, permette ancora una volta di applicare in tale contesto i concetti math-based del Risk Management, per cui all'annullamento del rischio si antepone la minimizzazione dei danni subìti e la capacità di reagire in modo proattivo.

Risulta evidente che nella gestione del rischio, ai tempi dell'Industria 4.0, lo scenario operativo da analizzare abbia aumentato la dimensione fino ad includere tecnologie differenti dal classico dispositivo pc-like. L'interconnessione apre le porte dell'infrastruttura di rete locale ai macchinari industriali, perlopiù del settore manifatturiero, apparati dotati di un aspetto hardware (elettronico e meccanico) preponderante, e che ora si trovano a dover affrontare un aspetto software che fino a pochi anni fa non era richiesto. Il tipico display di controllo, a corredo del 99% dei macchinari industriali risalenti a meno di 20 anni fa, dotato di software embedded con interfaccia grafica evoluta o di un semplice schermo a linee, non è più il solo aspetto di interesse, in quanto le attività di controllo e di monitoraggio dell'apparato produttivo ora potrebbero essere delegate ad entità terze, quali il sistema informativo aziendale, un layer software middleware o altri dispositivi informatici che rendono quasi superfluo il display embedded se non per l'operatore addetto all'utilizzo del macchinario stesso.

In altri termini, il bacino di utenza dell'apparato industriale si amplia e si sposta significativamente **dall'operaio specializzato a una moltitudine di altre entità uomo-macchina** che vanno dall'ingegnere informatico progettista dello strato middleware, in grado di interfacciarsi con il software del macchinario industriale, al responsabile tecnico addetto alla manutenzione, al solution provider in out sourcing che si occupa dell'integrazione con un sistema MES. Allo stesso modo, la quantità di informazioni che il sistema gestionale aziendale si trova a dover manipolare viene ampliata dalle informazioni provenienti da e dirette verso i macchinari industriali interconnessi, la cui natura è anch'essa eterogenea: si va dalle istruzioni

macchina impartite da remoto (controllo remoto), alla gestione di informazioni di monitoraggio produttivo o sullo stato di servizio dell'apparato. Tale mole di dati viene immessa all'interno dell'infrastruttura aziendale, gestita da strati software *ad hoc* e protetta da policies di cybersecurity (via hardware e software) che, premessa la natura fortemente caratterizzante di tali informazioni, devono essere adattate alla presenza di **nuovi contesti informativi da proteggere**. Ipotizzando un caso d'uso reale, si provi a immaginare quali danni possa causare un attaccante impadronitosi della tecnica di immissione di istruzioni macchina in un qualsiasi macchinario industriale a causa di una *failure* del sistema di sicurezza dell'infrastruttura di rete a cui il macchinario stesso è ora interconnesso.

Verso il nuovo Regolamento UE 2016/679

Scenari come quelli appena descritti sono, non a caso, oggetto di attenzione anche da parte del Nuovo Regolamento UE 2016/679 in materia di protezione dei dati personali (che sarà pienamente applicabile a partire dal 25 maggio 2018), in cui è esplicitamente prescritto un approccio basato sul rischio e su efficaci misure di *accountability* (responsabilizzazione). La prescrizione di un atteggiamento proattivo da parte dei titolari pone l'azienda di fronte ad attività di Ricerca e Sviluppo su **metodologie ottimali di tutela del flusso informativo**, e che spinge *de facto* verso l'adozione di modelli di processo basati sulla valutazione dei rischi (noti o evidenziabili) e delle misure tecniche e organizzative (anche in ambito sicurezza) che il titolare decide in autonomia debbano essere applicate.

Ciò ancorché oggetto del Nuovo Regolamento UE sia il trattamento dei rischi derivanti da attacchi sui dati personali degli utenti, e non delle informazioni aziendali in generale o delle informazioni da-verso macchine.

Così come avvenuto nel caso del passaggio, graduale o spesso parallelo, dai Sistemi per la Gestione della Qualità ai Sistemi 27001, ci si trova oggi di fronte a uno strumento normativo – il Nuovo Regolamento UE – pienamente integrato con le regole già dettate dall'Industria 4.0 e dall'Open Innovation, di cui può costituire un interessante corollario operativo.

Una sfida e una rivoluzione, il cui ambito di azione per gli addetti ai lavori include tematiche ingegneristiche, gestionali e giuridiche, tutte richiedenti una capacità di autoadattamento e di flessibilità professionale concreta, di spessore e mai generica, divenuta – oseremmo dire, finalmente – imprescindibile.

A cura di: **Ing. Igor Serraino** ed **Avv. Andrea Maggipinto**