www.bollettinoadapt.it, 13 dicembre 2012

Intervista a Marco Valsecchi
Responsabile "Risk & Compliance", NTT DATA Italia

di Claudio Cortesi

NTT DATA è una multinazionale che impiega più di 57000 lavoratori in 36 paesi, ed opera in Africa, Medio Oriente, Europa e Sudamerica. La società nasce in Giappone, dove ha il suo quartier generale, ed oggi è la sesta società di Information Technology al mondo[1]. La controllata italiana ha sede a Milano, ed è lì che incontro il dottor Marco Valsecchi, responsabile del settore Risk and Compliance di NTT DATA per l'area finanziaria.

Qual è il settore di business della sua azienda?

La nostra azienda è controllata al 100% dalla capogruppo giapponese NTT DATA ed impiega 2500 lavoratori in Italia. Il nostro business si concentra soprattutto nelle aree di consulenza, system integration e di outsourcing dei sistemi informatici. Tra i servizi di consulenza che offriamo, mi occupo del settore Risk and Compliance, nell'area financial.

Quali sono i vostri clienti e per quali esigenze svolgono valutazione del rischio?

Nel settore di cui mi occupo i clienti sono principalmente le banche e gli istituti finanziari. Qualora una banca dimostri di saper gestire il rischio in maniera efficace, è soggetta a minori vincoli secondo quanto prescrive l'accordo Basilea 2. Non prevedere i rischi comporta poi maggiori oneri nell'esercizio dell'attività aziendale, che vanno dai risarcimenti per gli infortuni dei lavoratori al risarcimento ad un cliente per l'interruzione di servizio causata da problemi del software; per questo serve fare valutazione del rischio e risk management.

Quale direzione aziendale si occupa del risk management nelle banche italiane?

Noi lavoriamo con molte banche, tra cui i 5 più importanti istituti finanziari in Italia. All'interno delle banche, possiamo distinguere due diverse unità aziendali impegnate sul fronte del risk management. La prima si occupa di Security, intendendo con ciò tutte le misure che garantiscono all'azienda il regolare svolgimento delle sue operazioni di business. Nelle banche ogni giorno vengono scambiati moltissimi dati, sia all'interno, tra le diverse aree aziendali, tra le filiali e la capogruppo, sia all'esterno, con la Banca d'Italia e gli altri istituti per le operazioni di compensazione. Il rischio che questi dati vengano compromessi o violati è costante, e pertanto è necessario predisporre opportune procedure e tecnologie in grado di garantire la sicurezza delle comunicazioni. Queste avvengono principalmente su base informatica, per cui è necessario gestirne i rischi relativi. In ultimo si deve prestare la massima attenzione alle frodi riguardanti le carte di credito ed il bancomat.
Il settore Safety invece si occupa soprattutto dell'applicazione delle leggi in materia di salute e sicurezza sul lavoro, in particolare la 81/2008. È chiaro che nel lavoro quotidiano in azienda le

[1] Gartner, *Market Share Analysis: IT Services, Worldwide*, 2012

funzioni si sovrappongono, ed infatti nelle realtà più piccole spesso una ola direzione si occupa di tutti e due gli aspetti.

Come si svolge la valutazione del rischio?

La valutazione del rischio è un processo molto complesso, in cui si analizzano tutti i fattori di criticità correlati al rischio presenti in un progetto. Nel nostro ambito operativo, quello finanziario, i rischi più rilevanti sono la rapina, i danni agli asset aziendali (si pensi alla distruzione delle filiali durante le manifestazioni) ed il rischio di violazione delle leggi. Individuati i rischi bisogna scegliere le misure di sicurezza più efficaci. Noi ci occupiamo principalmente di progettare gli spazi delle filiali in modo efficiente, e di prevedere gli strumenti informatici utili a garantire la sicurezza, come la videosorveglianza. Quando si individuano gli elementi critici bisogna tener conto anche dell'area di lavoro: a Napoli, ad esempio, spesso i rapinatori giungono in filiale dal sottosouolo, per cui in fase di progettazione della filiale bisogna predisporre opportune contromisure. La security pertanto svolge la valutazione e progetta gli spazi, non si occupa della realizzazione fisica degli stessi. Lo stesso avviene per le tecnologie informatiche, che verranno realizzate dal settore IT.

Chi si occupa della valutazione del rischio nelle banche italiane?

Nelle grandi banche italiane, le prime 5 a livello nazionale, vi sono tre livelli operativi. Nella capogruppo vi è la direzione Corporate Security che definisce il livello di rischio e le policy da seguire. Vi è poi un livello intermedio che individua, per ogni filiale, quali soluzioni adottare in base ai criteri definiti dalla capogruppo. Infine i settori Real Estate e IT realizzano il progetto. Ciò vale nelle grandi banche. Nelle banche intermedie, quelle che hanno fra le 500 e le 1000 filiali, di solito non vi è il settore intermedio. Nelle piccole banche locali, spesso il settore Security ed il settore Safety sono uniti.

All'interno del processo aziendale, quando si svolge la valutazione del rischio?

Le aziende assumono decisioni coerenti con la loro strategia commerciale. Il management decide se aprire o no una nuova filiale in virtù dei profitti attesi nell'area, anche se vi è un elevato rischio rapina. Noi arriviamo dopo, a decisione avvenuta, e ci occupiamo di garantire la massima sicurezza possibile. La valutazione del rischio era un servizio importante che noi offrivamo alle banche fino a qualche anno fa. Nel mercato di oggi invece la valutazione non viene più venduta come servizio, ma è una commodity che noi offriamo gratuitamente. A seguito della valutazione, noi siamo in grado di individuare le soluzioni tecniche più efficaci e di realizzarle direttamente, ed è questo il nostro business.

La sicurezza dei lavoratori dipende molto dalla formazione che ricevono. Come operate per la formazione dei dipendenti?

Nella formazione dei dipendenti negli ultimi anni si è fatto molto ricorso alla metodologia e-learning. Tale approccio si è però rivelato inefficace, poiché generalmente il lavoratore viene esposto, ad esempio, a 50 corsi di 2 ore ciascuno; lui assiste ai video didattici passivamente, senza interazione, ed il corso ha scarsa efficacia. Nella nostra esperienza si è rivelato più utile prevedere corsi dal vivo. Il problema è che i corsi dal vivo costano molto, per cui non è possibile fornirli a tutti i dipendenti. Occorre scegliere quindi il target su cui la formazione è più efficace; ad esempio si possono coinvolgere i direttori, che poi trasferiranno le nozioni ai propri dipendenti. Oppure ci si può rivolgere a chi svolge le mansioni più esposte, come gli addetti alla clientela. In ogni caso le scelte relative alla formazione sono prese di concerto con la direzione Risorse Umane.

Quali sono le figure professionali che operano nel vostro settore?

Il nostro settore svolge analisi di rischio, volto ad individuare i fattori di pericolo per l'azienda ed i lavoratori. Definisce le policy aziendali, con i comportamenti e le procedure che i dipendenti devono osservare. Infine stabilisce le politiche di sicurezza che l'azienda deve adottare, quali sistemi di videosorveglianza o la gestione delle combinazioni delle casseforti. Noi agiamo soprattutto nella logica di system integrator coordinando l'intero processo. Se, ad esempio una banca deve aprire una nuova filiale e ci chiede di garantire la sicurezza dei propri dipendenti, noi valutiamo il rischio, definiamo le policy da adottare, adeguandole alle esigenze individuate ed alla normativa in materia. Acquistiamo gli strumenti necessari, accordandoci con fornitori ed installatori, ed implementiamo la soluzione sul luogo di lavoro. Abbiamo quindi bisogno di professionisti preparati nelle tecnologie informatiche e nel management del rischio. Se dovessi stimare le competenze nella mia unità aziendale, le posso dire che abbiamo il 75% di ingegneri ed il 25% economisti, in percentuale minore gli esperti di area giuridica.

Claudio Cortesi
Scuola internazionale di Dottorato in Formazione della persona e mercato del lavoro
ADAPT-CQIA, Università degli Studi di Bergamo