SCiNTLEX
Diritto e Società dell'Informazione

SICUREZZA AZIENDALE E RISK MANAGEMENT. NUOVE STRATEGIE PER EVITARE IL CYBERCRIME

Sicurezza aziendale e risk management. Nuove strategie per evitare il cybercrime

A cura di Annalisa Spedicato - Studio Legale Lisi

Il cybercrime si evolve ad una velocità talmente elevata, che la legge non riesce a tenere il suo passo, dichiarava McNiven, consulente del governo americano per il cybercrime, durante un convegno sulla sicurezza informatica nel settore bancario tenuto a Riyadh, Arabia Saudita nel 2005.

Ed effettivamente è proprio attorno ai crimini informatici che ruotano oggi i maggiori fatturati delle organizzazioni criminali, non solo, gli strumenti informatici e telematici sono diventati un mezzo di concorrenza sleale tra le aziende, talmente potente, da costringere il Consiglio di Europa ad intervenire normativamente nel 2001.

In quell'occasione a Budapest il legislatore europeo, preoccupato dell'incidenza negativa degli strumenti informatici su alcune tipologie di reati, decise di mettere a punto una convenzione apposita per la lotta contro la criminalità informatica, convenzione poi entrata in vigore il 1o luglio 2004.

L'Italia, oggi, si appresta a ratificare la suddetta convenzione. Infatti, il Senato della Repubblica (dopo la Camera dei Deputati), lo scorso 27 febbraio 2008, ha approvato, in via definitiva, il disegno di legge di Ratifica ed esecuzione della Convenzione del Consiglio d' Europa sulla criminalità informatica, che ora attende la firma del PdR, prima di approdare nell'ambito della Legge n. 231/2001, estendendo di fatto e, anche per i reati informatici (art. 7), la responsabilità amministrativa degli enti.

I reati informatici oggetto della presente ratifica sono i seguenti:

falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.);accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.); detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.); diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.); intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.); installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies c.p.); danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.); danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.); danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.); danneggiamento di sistemi informatici o

telematici di pubblica utilità (art. 635-quinquies c.p.); frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.).

Al di là di alcune novità, sicuramente recate dalla presente ratifica, non bisogna, dimenticare, in ogni caso, che il nostro Paese è stato uno dei primi in Europa ad introdurre una legge organica in materia. La legge 23 dicembre 1993, n. 547, in tema di delitti informatici, assieme alla legge 18 agosto 2000, n. 248 sulla pirateria informatica, la quale ha modificato le disposizioni in materia della legge 22 aprile 1941, n. 633, introdotte dal decreto legislativo 29 dicembre 1992, n. 518, e la legge 6 febbraio 2006, n. 38, già costituivano il chiaro quadro normativo sul cybercrime, portavoce dell'orientamento adottato dal legislatore italiano. Pertanto, pare che la portata dell'adeguamento normativo da realizzare, per l'esecuzione della Convenzione, nel settore del diritto penale sostanziale, sia assai modesta, essendo in vigore una disciplina che, già di per se, risulta essere esaustiva.

In ogni caso, l'introduzione dell'articolo 25-septies (24-bis nel testo approvato dal Senato, NdR) del decreto legislativo 8 giugno 2001, n. 231, risponde all'esigenza di introdurre forme di responsabilità penale per le persone giuridiche, anche con riferimento ai reati informatici più gravi(cfr. relazione di accompagnamento al testo presentato alla Camera dei Deputati).

La Convenzione detta una disciplina molto dettagliata sulle modalità di gestione del cosiddetto risk management, ovvero del complesso di strategie organizzative di cui un'azienda deve dotarsi per evitare di incorrere nelle sanzioni penali.

In effetti, la legge 231/2001, sancendo la responsabilità amministrativa degli enti, una responsabilità che, di fatto, presenta profili squisitamente penalistici, pare abbia imposto il superamento del vecchio brocardo latino secondo cui societas delinquere non potest.

E' evidente come tali astrazioni, entrando in conflitto con l'art. 27 Cost., minino l'autorevolezza del principio costituzionale secondo cui la responsabilità penale è personale.

Tuttavia, non si può escludere, come i processi evolutivi che hanno portato la società a creare metodi decisionali non più centrati sul singolo, obblighino oggi a ripensare a tali principi tradizionali, in una visione vieppiù allargata, che ricomprenda e, soprattutto, accetti, accanto alla responsabilità del singolo (responsabilità che pur rimane), l'esistenza di processi decisionali decentrati e di gruppo, che costituiscono qualcosa in più rispetto alla semplice somma delle scelte di soli individui.

Ma, al di là delle questioni di legittimità che la presente legge pone, si è giunti a concludere che il reato non può più appartenere solo al singolo, bensì deve essere ascritto all'intera organizzazione, alla struttura complessivamente intesa, qualora essa non sia stata in grado di dotarsi di quei meccanismi interni di prevenzione, utili ad evitare il rischio di reato.

Una tutela preventiva debitamente eseguita, infatti, in base al disposto normativo della L.231/2001, permette all'azienda che si sia corredata di un modello organizzativo che le consenta di prevenire il reato (art.6, 1° co.), di tirarsi fuori da responsabilità. La scelta preventiva compiuta dall'organizzazione, infatti, mette l'azienda stessa nella condizione di provare di aver fatto tutto il possibile per evitare il danno, un' inversione dell'onere della prova, necessaria per sottrarsi alla responsabilità oggettiva, che, generalmente, è in capo a chi gestisce situazioni di rischio.

Quando si fa riferimento a modelli organizzativi idonei a prevenire il verificarsi dei reati informatici a cui la Convenzione rinvia, significa avere particolare riguardo rispetto all'intero flusso comunicativo e informativo che ruota attorno a tutta la struttura aziendale, comprendendo anche le informazioni e i documenti in fase di ingresso, sia quelli in fase di uscita, che rientrano, per legge, nelle more dell'azienda e, dunque, nell'ambito della sua responsabilità.

Occorre, altresì, dotarsi di strumenti e meccanismi che permettano di evitare non solo la perdita di dati e informazioni importanti per l'azienda, ma anche la loro modifica o la loro alterazione, strumenti di gestione di tali documenti e atti che permettano di mantenerne la stabilizzazione temporale e l' integrità complessiva e che permettano di risalire pacificamente al titolare del documento, rendendo facilmente individuabile il soggetto cui quel documento o quella semplice informazione sono ascrivibili. Tutto questo nel rispetto della privacy.

Naturalmente il risultato del modello di gestione dipenderà dalla maniera in cui è stata effettuata l'analisi preventiva sull'azienda e dalla corretta valutazione del rischio, un rischio, ovviamente, differente rispetto alle singole realtà aziendali.

Ogni struttura aziendale avrà, perciò, il suo risk management, un modello ad hoc, cucito addosso alla singola azienda e peculiare solo ad essa.

Un altro elemento di riuscita da considerare per un modello gestionale che schivi la configurazione di reati informatici è, di certo, la flessibilità del modello stesso. Nel senso che esso dovrà necessariamente essere costituito da una componente fissa, standard e da una componente variabile che si adatti facilmente all'evoluzione della struttura aziendale, alle sue performance, nonchè all'evoluzione della tecnologia.

Senza dimenticare la formazione necessaria nei confronti di tutti coloro che entrano in contatto con documenti informatici e che avranno a che fare con il modello organizzativo di riferimento.

Il modello di risk management sarà ovviamente più adeguato, laddove verrà costantemente monitorato e aggiornato.

Per questo appare plausibile, che l'azienda trasferisca tali incombenze all'esterno, attraverso la creazione di contratti di outsourcing con realtà di consulenza che si occupano specificamente di tali processi e che possono garantire, pertanto, la vera riuscita di questa nuova scommessa sociale.

12/03/2008