Flash Report

protiviti®
Independent Risk Consulting

Reati informatici ex art. 24 bis Decreto 231/01

La Legge 48/08 di ratifica della Convenzione sulla Criminalità Informatica - pubblicata sulla Gazzetta Ufficiale della Repubblica Italiana n. 80 del 4 aprile u.s., Supplemento Ordinario n. 79 (di seguito allegata) - ha esteso, a far data dal 5 aprile u.s., la responsabilità amministrativa delle persone giuridiche ai reati di "criminalità informatica".

In particolare, la citata Legge ha introdotto nel D.Lgs. 231/01 l'art. 24-bis, che fa riferimento ai seguenti reati:

- falsità in un documento informatico pubblico o privato (491-bis c.p.)
- accesso abusivo ad un sistema informatico o telematico (615-ter c.p.)
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615-quater c.p.)
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (615-quinquies c.p)
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617-quater c.p.)
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (617- quinquies c.p)
- danneggiamento di informazioni, dati e programmi informatici (635-bis c.p.)
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635-ter c. p.)
- danneggiamento di sistemi informatici o telematici (635-quater c.p.)
- danneggiamento di sistemi informatici o telematici di pubblica utilità (635-quinquies c.p.)
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640-quinquies c.p.)

I reati citati si riferiscono, in via meramente esemplificativa e non esaustiva, alle seguenti possibili condotte, realizzate sempre nell'interesse o a vantaggio dell'ente:

- alterazione di documenti elettronici, pubblici o privati, con finalità probatoria
- creazioni/modifiche/cancellazioni fraudolente di dati di enti concorrenti, pubblici o privati
- accesso abusivo all'intranet di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate commerciali o industriali
- modifiche non autorizzate a programmi al fine di danneggiare enti concorrenti, pubblici o privati

- detenzione ed utilizzo abusivo di password di accesso a siti di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate commerciali o industriali
- intercettazione fraudolenta di comunicazioni di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate commerciali o industriali
- installazione fraudolenta di dispositivi per intercettazioni telefoniche e radio di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate commerciali o industriali
- diffusione tramite la rete aziendale di programmi illeciti o virus con la finalità di danneggiare enti concorrenti, pubblici o privati
- danneggiamento di strumenti di commercio elettronico di enti concorrenti, pubblici o privati
- modifica fraudolenta di informazioni di enti concorrenti, pubblici o privati

A fronte di questi delitti, l'ente è punito con sanzioni pecuniarie da cento a cinquecento quote nonché con le sanzioni interdittive di cui all'art. 9 del D.Lgs. 231/01, a seconda della fattispecie di reato.

Tale emendamento amplia la responsabilità amministrativa degli enti rendendo necessaria la verifica e l'eventuale aggiornamento dei Modelli organizzativi ex D.Lgs. 231/01 anche ai fini di valutare la rispondenza dei sistemi informativi - che rappresentano una componente rilevante dei sistemi di gestione e controllo aziendali - ai requisiti di legge e l'adeguatezza dei relativi presidi di controllo rispetto alle esigenze di tutela della società.

In considerazione del fatto che i nuovi ambiti applicativi della norma richiedono specifiche competenze tecniche per l'analisi delle possibili modalità di realizzazione, per la valutazione dei rischi informatici associati nonché per la verifica e successiva definizione dei relativi presidi di controllo, Protiviti è in grado di integrare le competenze ad oggi maturate sui temi "231" con un Team di consulenti esperti in servizi di Technology Risk Consulting, che potranno assistere - anche su questi temi - la Vostra organizzazione nell'aggiornamento dei Modelli "231" adottati.

Per maggiori informazioni, rivolgetevi all'ufficio Protiviti più vicino o contattate Luca Medizza, Massimo Minerva o Francesca Delfini al numero 02 6550 6301.