STUDIO LEGALE
Nervi&Zulli

Via G. Pisanelli, 4
00196 - Roma
Tel. 06-87 88 97 08
segreteria@studionervizulli.it

NOVITÀ

Cybersecurity e Vertici Aziendali: Responsabilità Diretta nel Decreto NIS II

Avv. Miriam Zulli
zulli@studionervizulli.it

in

Dott. Emanuele Filippo Ciulla
ciulla@studionervizulli.it

in

Il Decreto NIS II introduce una responsabilità diretta per gli organi di amministrazione e direttivi in materia di sicurezza informatica, imponendo obblighi di vigilanza, formazione e supervisione. I vertici aziendali non possono più delegare completamente la gestione della cybersecurity, ma devono garantire un controllo attivo e costante per evitare sanzioni e tutelare l'organizzazione.

Responsabilità diretta dei vertici aziendali nella sicurezza informatica

Il D. Lgs. 138/2024 (c.d. Decreto NIS II) prevede, in tema di *cybersecurity*, il coinvolgimento diretto degli organi di amministrazione e direttivi dei soggetti essenziali e importanti. Questo comporta che chi ricopre posizioni di vertice non può delegare totalmente la responsabilità della sicurezza informatica, ma deve occuparsene personalmente.

Segnatamente, l'art. 23 del Decreto NIS II prevede che i vertici aziendali dei soggetti NIS II (*i*) approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica, (*ii*) sovraintendono all'implementazione degli obblighi di gestione del rischio per la sicurezza informatica e di notifica degli incidenti e (*iii*) sono direttamente responsabili delle violazioni delle previsioni del Decreto NIS II.

Gli organi direttivi, inoltre, sono obbligati a seguire personalmente un corso di formazione in materia di sicurezza informatica e a promuovere periodicamente una formazione, sempre in materia di *cybersecurity*, diretta ai loro dipendenti.

La ragione principale dell'attribuzione di una responsabilità diretta ai vertici delle organizzazioni essenziali o importanti è da rintracciare nel ruolo chiave che queste organizzazioni svolgono in settori vitali (come energia, trasporti, infrastrutture finanziarie e gestione dei rifiuti) non solo per i singoli utenti, ma per l'intera collettività.

La responsabilità cumulativa nel Decreto NIS II

Il legislatore italiano con il Decreto NIS II, da un lato, ha voluto definire gli obblighi per gli operatori di servizi essenziali e importanti; dall'altro, ha voluto stabilire, non solo la responsabilità amministrativa a carico dell'entità giuridica, ma anche la responsabilità diretta delle persone fisiche che detengono poteri decisionali all'interno dell'organizzazione.

In particolare, l'articolo 38, comma 5, stabilisce che: *"Qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso, assicura il rispetto delle disposizioni di cui al presente decreto. Tali persone fisiche possono essere ritenute responsabili dell'inadempimento in caso di violazione del presente decreto da parte del soggetto di cui hanno rappresentanza."*

Questo modello di responsabilità (c.d. responsabilità cumulativa) rappresenta un'innovazione significativa, in quanto alla responsabilità dell'entità giuridica si cumula la responsabilità della persona fisica che esercita poteri direttivi nell'organizzazione.

La delega e la vigilanza degli organi di amministrazione e direttivi

La delineata responsabilità diretta degli organi di amministrazione e direttivi, pone il problema della trasferibilità di detta responsabilità, attraverso lo strumento della delega, ad altri soggetti.

Le disposizioni normative contenute nel Decreto NIS II suggeriscono un cauto approccio all'istituto della delega. Infatti, i dirigenti non possono limitarsi a delegare l'attività di sicurezza informatica senza prevederne una supervisione. Invero, in ogni caso devono approvare le strategie di gestione del rischio e verificare che siano effettivamente applicate. Inoltre, la delega è possibile solo se chi riceve l'incarico ha risorse e mezzi adeguati.

Questa interpretazione restrittiva è confermata dall'art. 23 del Decreto NIS II che impone agli organi di amministrazione e direttivi l'obbligo di approvare "*le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica*" e di vigilare sull'implementazione degli obblighi relativi alla gestione del rischio informatico e alla notifica degli incidenti.

Chi delega, dunque, non si libera della propria responsabilità, ma assume un altro tipo di onere, quello di garantire che l'azione di direzione sia effettivamente esercitata tramite una costante vigilanza, indirizzo e verifica dei risultati ottenuti tramite la delega.

Da ciò si deduce che l'obbligo di vigilanza non è delegabile e deve essere svolto dal vertice dell'organizzazione, altrimenti il principio di garanzia e protezione sotteso dalla normativa verrebbe compromesso.

Conclusione

La cybersecurity non è più un aspetto marginale o facoltativo, ma un tema cruciale che richiede l'impegno diretto dei vertici aziendali e istituzionali. È un impegno che implica la presa in carico di responsabilità chiare, da gestire con competenza e consapevolezza.

In questo contesto, la sicurezza informatica non riguarda più la sola protezione delle capacità produttive di un'azienda, ma è diventata una vera e propria responsabilità d'impresa. Questo significa che clienti, investitori e utenti finali posso agire giudizialmente per chiedere tutela in caso di mancata protezione dei dati.

Oggi, questa responsabilità non è più una mera formalità, ma è ancorata a un sistema sanzionatorio rigoroso, effettivo e dissuasivo, che non ammette scappatoie. La sicurezza è diventata un impegno serio, da cui non si può più prescindere.