“Responsabilità Aziendale”

Rubrica a cura di Lorenzo Nicolò Meazza

Cybercrimes e Modello 231

Tempo di lettura: 2 minuti

Responsabilità aziendale nasce dalla collaborazione con l'avv. **Lorenzo Nicolò Meazza**, il cui Studio ha sede a Milano e opera a livello nazionale, prestando assistenza a italiani e stranieri, privati, piccole e medie imprese, ma anche a multinazionali ed enti pubblici, in tutti i settori del diritto penale, dai più tradizionali, al diritto d'impresa.

Oltre all'opera al assistenza in tutte le fasi del giudizio a indagati, (imputati, persone offese e parti civili, lo Studio offre anche la propria consulenza stragiudiziale nella redazione di pareri, nell'elaborazione di modelli di organizzazione e gestione degli enti ex D.Lgs. 231/01 e dei sistemi di deleghe e funzioni.

In questo numero di Newcert Magazine parleremo del Modello 231 come base per la ***"cyber resilience"***.

I cd. ***Cybercrimes*** **- reati informatici** sono le fattispecie che prevedono comportamenti messi in atto attra-verso l'uso di computer o della rete che in questa occasione diventano strumenti e/o luoghi di commissione del reato.

La particolare sensibilità del legislatore relativamente questo specifico ambito di criminalità ha trovato massima espressione con la Legge 48/2008, la quale ha introdotto una serie di modifiche al codice penale e al codice di procedura penale concernenti i reati in materia informatica e ha introdotto, nel D.Lgs. 231/2001, l'**art. *24bis*** recante la previsione di nuove fattispecie di reato in merito a **delitti informatici** e al **trattamento illecito di dati.**

In particolare, i reati informatici, così come emendati dalla novella normativa si possono distinguere in tre gruppi:

il primo gruppo comprende i reati che puniscono **danneggiamento di hardware, di software e di dati** (artt. 615ter, 617quater, 617 quinquies, 635bis, 635ter, 635quater 635quinquies c.p.), i quali si concretizzano mediante l'accesso abusivo ad un sistema e l'intercettazione o l'interruzione di dati compiuti attraverso l'installazione di appositi programmi;

il secondo gruppo è costituito dai reati che

puniscono la detenzione e la diffusione abusiva di software e/o di attrezzature informatiche diretti danneggiare/ interrompere un sistema informatico e la detenzione/diffusione abusiva di codici di accesso a sistemi informatici o telematici (artt. 615quater 615quinquies c.p.);

il terzo gruppo, infine, comprende i reati con cui viene punita la violazione dell'integrità dei documenti informatici e della loro gestione attraverso la falsificazione di firma digitale (artt. 491 bis e 640quinquies c.p.).

Con riguardo alla attività aziendale, in particolare, la diffusione della criminalità online ha fatto sì che i digital crimes non costituiscano più solamente una minaccia interna al perimetro dell'azienda, ma colpiscano anche soprattutto dall'esterno, attraverso **attacchi cyber e data breach.**

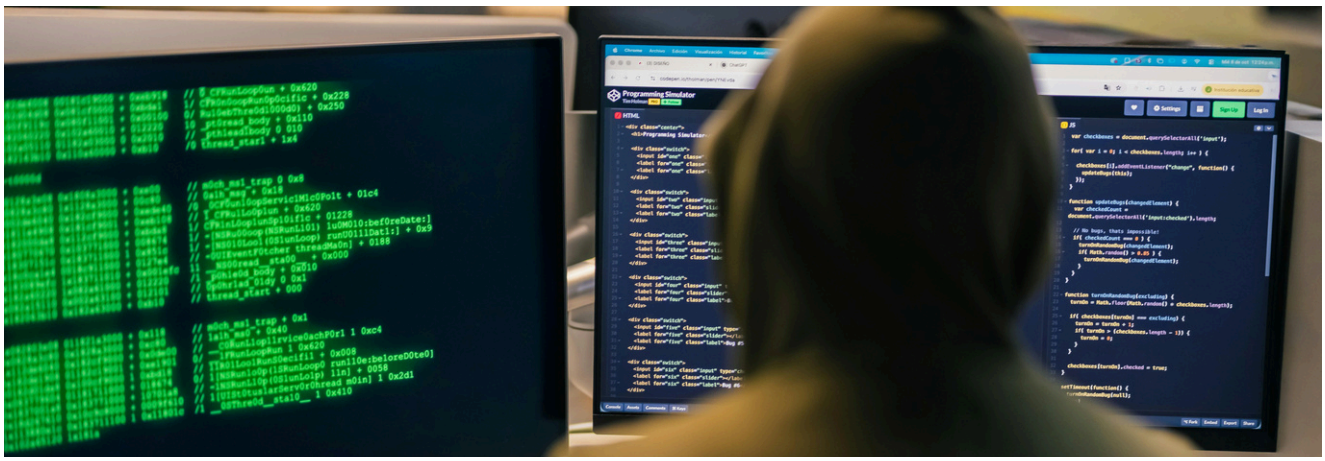
A fronte di sempre più diffusi episodi di **violazione dei sistemi informativi aziendali** perpetrati dagli hackers e tra l'altro incrementati dalla peculiare situazione geo-politi-ca che stiamo vivendo, gli enti sono tenuti a prendere maggiore coscienza della necessità di provvedere non so- alla difesa della rete aziendale interna, ma anche ad un'azione di tutela rivolta verso l'esterno.

L'occasione privilegiata per dare attuazione a una strategia di protezione si rivela essere la redazione e l'implementazione di un efficace **Modello 231**, che ponga le basi per un concreto progetto di "cyber resilience".

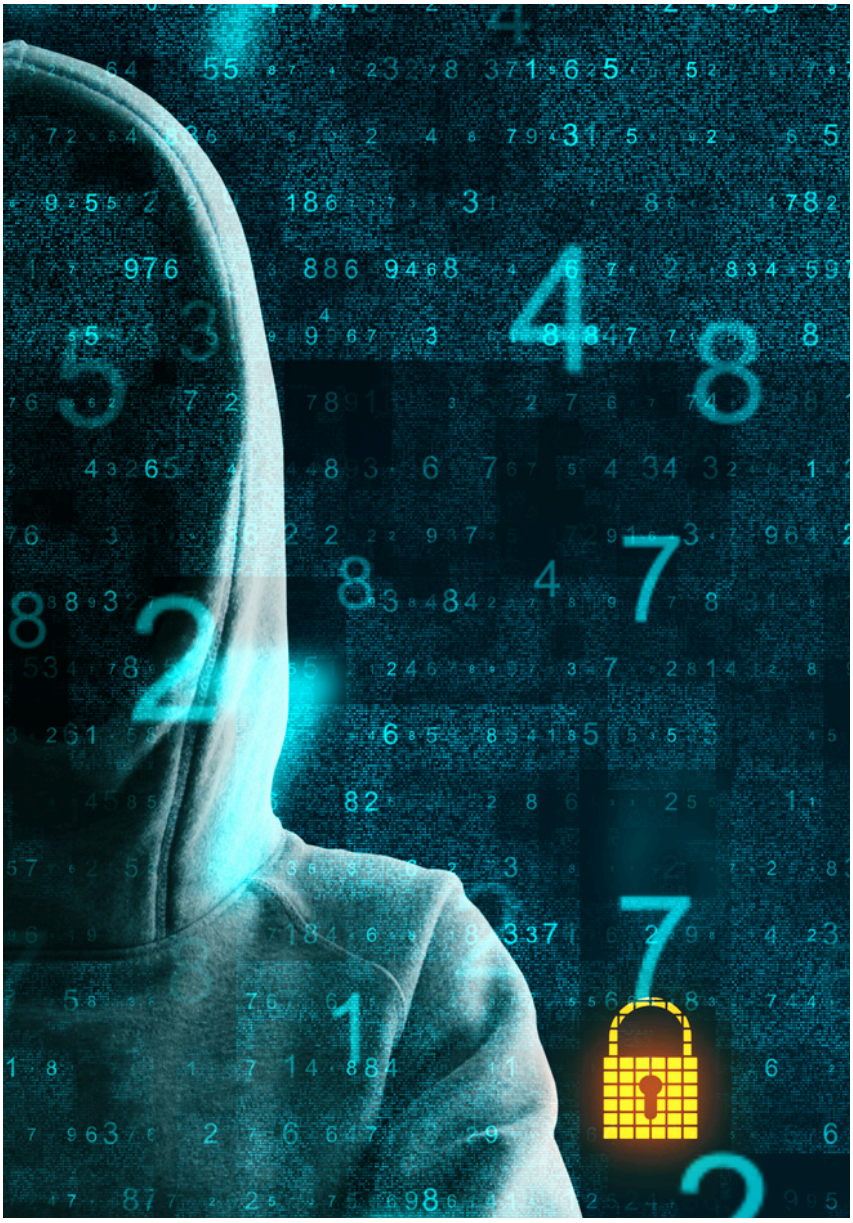
A tal fine, il primo step è da identificarsi con l'inventariazione delle attività aziendali, l'**identificazione delle aree di rischio** e dei reati rilevanti, per pol procedere all'analisi dei rischi di possibile commissione delle rilevanti condotte illecite.

A questo punto occorrerà provvedere alla redazione dei protocolli necessari per colmare il cd. rischio residuo emerso dalla mappatura alla luce dei presidi già in es-sere, rinforzando le procedure già attive con presidi adeguati alla prevenzione dei rischi informatici.

Entrando più nel dettaglio, gli enti dovranno verificare il loro livello di esposizione a rischio rispetto a questo tipo di reati e quindi, a seconda del livello di informatizzazione dell'ente e conseguente-mente del rischio emerso, dovranno implementare piani di cybersecurity adeguati che comprendano in maniera coordinata ed efficiente aspetti tecnologici (es. soluz tecnico-informatiche), organizzativi (es. formazione, policy e procedure) e legali (es. contrattualistica a supporto).



In particolare, il Modello di Organizzazione e Gestione dovrà essere progettato in modo da far sì che i rischi individuati siano ridotti ad un livello accettabile, attraverso l'attuazione di specifici protocolli e procedure funzionali volte ad innalzare il livello di sicurezza e ad indirizzare con azioni efficaci le corrette regole di comportamento, unitamente a un sistema adeguato di controllo e verifica.



Solo dopo aver posto in essere tutte queste misure si potrà dimostrare, in una eventuale sede giudiziaria che la commissione di uno dei reati presupposto sia stata realizzata necessariamente eludendo i presidi di controllo attivi, con tutte le conseguenze che ne potrebbero derivare in termini esimenti di responsabilità dell'ente.