PRESENTAZIONE DI RINA

RINA, gruppo a cui fanno capo la prima società di certificazione e la prima società di ingegneria italiana, fornisce un'ampia gamma di servizi nei settori Energia, Marine, Infrastrutture & Mobilità, Certificazione, Industria, Real Estate.

Da dicembre 2023, al fianco dell'azionista di maggioranza Registro Italiano Navale, ha fatto il proprio ingresso nella compagine sociale anche Fondo Italiano d'Investimento SGR con un pool di co-investitori da esso guidati. Con ricavi al 2023 pari a 797 milioni di euro, 5.800 dipendenti e 200 uffici in 70 paesi nel mondo, RINA partecipa alle principali organizzazioni internazionali, contribuendo da sempre allo sviluppo di nuovi standard normativi.

I servizi di cybersicurezza sviluppati da RINA si rivolgono a soggetti che operano in diversi settori. Questi includono, ma non sono limitati a, infrastrutture critiche, bancario, assicurativo, spazio, difesa, automotive, marittimo, energia, utilities e produzione industriale. I servizi vengono eseguiti tramite attività di consulenza o attraverso l'uso di strumenti specifici. In particolare, le attività relative alla Cybersecurity sono declinate:

- in chiave consulenziale, attraverso servizi di verifica della security posture, vulnerability assessment, test di sicurezza di prodotti IT, introduzione di misure tecnico-organizzative per la gestione dei rischi cyber e il supporto alla valutazione della sicurezza dei prodotti IT secondo schemi e certificazioni quali i Common Criteria e per la parte OT la IEC 62443;
- in veste di organismo di certificazione, attraverso attività di audit e certificazione indipendente rispetto ai principali standard italiani ed internazionali per la sicurezza delle informazioni e la cybersecurity, con circa 900 certificati emessi.

Il Gruppo, dunque, attraverso le proprie competenze supporta le aziende situate in diverse aree geografiche a migliorare la loro postura di sicurezza, indipendentemente dal livello iniziale di maturità informatica dal quale essi partono, offrendo attività di cybersicurezza sia nel campo della tecnologia dell'informazione (IT) sia nel campo industriale della tecnologia operativa (OT).

IL QUADRO NORMATIVO ALLA LUCE DELLA DIRETTIVA NIS2 E DEL DECRETO DI RECEPIMENTO

Nelle intenzioni del Parlamento europeo e del Consiglio, la Direttiva NIS2 viene incontro alle crescenti esigenze di cybersicurezza nell'Unione, per quanto riguarda i settori coinvolti e i requisiti di sicurezza più stringenti, imponendo obblighi di notifica e un maggior coordinamento sia fra le Autorità nazionali, che a livello comunitario.

In linea con la tempistica di recepimento prevista dall'articolo 41 della Direttiva, il Decreto legislativo attualmente all'esame delle competenti Commissioni parlamentari porterà chiarezza sull'attribuzione di competenze alle Autorità nazionali, sui loro compiti, sui poteri e sulle reciproche interazioni in regime ordinario e in caso di eventi dannosi per la cybersicurezza.

Saranno dettagliati gli obblighi di gestione dei rischi per la sicurezza ricadenti sui soggetti che contribuiscono al mantenimento di adeguati livelli di cybersicurezza nello Stato membro.

Saranno stabiliti i criteri e le modalità di vigilanza sull'applicazione delle misure di gestione del rischio, esplicitando le sanzioni applicabili in caso di mancato rispetto degli obblighi.

Dunque, lo Schema di decreto legislativo in esame contribuirà sicuramente all'aumento della consapevolezza da parte delle aziende sui rischi di sicurezza informatica.

OSSERVAZIONI E SUGGERIMENTI SUL RECEPIMENTO DELLA DIRETTIVA NIS2

Con riferimento allo Schema di decreto legislativo recante "*recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) 910/2014 e della direttiva (UE) n. 2018/1972 e che abroga la direttiva (UE) 2016/1148*", RINA ha individuato i seguenti punti che si ritiene opportuno chiarire:

- **Articolo 7 (*Identificazione ed elencazione dei soggetti essenziali e dei soggetti importanti*)** - In questo articolo sarebbe utile specificare che vi sono soggetti che, pur non rientrando in altre fonti normative precedenti (compresa la Direttiva NIS precedente), potranno registrarsi di propria iniziativa, purché rispettino quanto indicato dall'articolo 3 e dall'articolo 6.

  Con riferimento ai soggetti essenziali e ai soggetti importanti, di cui al comma 2 dell'articolo in esame, apparirebbe utile specificare, al comma 5 dell'articolo 40 e all'articolo 17 del decreto, le caratteristiche di riservatezza dell'elenco dei soggetti sopracitati.

- **Articolo 24 (*Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica*)** – Al comma 3 dell'articolo 24 sarebbe utile specificare quale metodologia di analisi del rischio debbano adottare i soggetti interessati per garantire efficacia alla gestione dei rischi, in base a decisione dell'Autorità nazionale NIS. Per indicare ai soggetti essenziali e importanti, di cui all'Art.7 comma 3, punti a) e b), come debbano aderire alla Strategia nazionale di cybersicurezza di cui all'articolo 9, si suggerisce di chiarire le modalità attraverso le quali l'Agenzia per la cybersicurezza nazionale e/o le Autorità di settore NIS notificheranno le metodologie, i requisiti e le tempistiche da rispettare. Ad esempio, si potrebbe chiarire se queste informazioni giungeranno con la stessa comunicazione con la quale l'Autorità nazionale competente NIS comunica l'inserimento o la permanenza nell'elenco dei soggetti essenziali o importanti.

- **Articolo 27 (*Uso di schemi di certificazione della cybersicurezza*)** - Si suggerisce di indicare una metodologia di analisi dei rischi per i prodotti e le tecnologie che debbano gestire rischi di sicurezza delle informazioni, sulla base della quale i soggetti ai quali l'Autorità nazionale competente NIS imporrà

l'adozione di prodotti certificati possano avviare un processo di valutazione della sicurezza IT secondo il livello di garanzia che è risultato da tale analisi per quei prodotti. Inoltre, appare utile il richiamo al Regolamento (UE) 2024/482, emesso in esecuzione del Regolamento (UE) 2019/881, citato dall'articolo 27 del decreto legislativo in esame.

- **Articolo 28 (*Specifiche tecniche*)** - Ai fini di una migliore applicazione delle misure di gestione dei rischi per la sicurezza informatica previste dall'articolo 24, potrebbe essere utile indicare al comma 1 dell'articolo 28, in relazione alle "*specifiche tecniche europee ed internazionali*" promosse dall'Agenzia per la cybersicurezza nazionale, una più puntuale specificazione di norme (quali ISO/IEC 27001 e NIST Cybersecurity Framework), così come anche previsto dalla Direttiva NIS2 che, nel considerando n. 79, cita esplicitamente *"[…] Le misure di gestione dei rischi di cibersicurezza dovrebbero pertanto affrontare anche la sicurezza fisica e dell'ambiente dei sistemi informatici e di rete includendo misure volte a proteggere detti sistemi da guasti del sistema, errori umani, azioni malevole o fenomeni naturali, in linea con le norme europee e internazionali, come quelle di cui alla serie ISO/IEC 27000. […]".*

- **Articolo 34 (*Principi generali per lo svolgimento delle attività di vigilanza ed esecuzione*)** - Al fine di garantire maggiore chiarezza, si propone di specificare, al comma 7 dell'articolo 34, le caratteristiche che devono avere gli organismi indipendenti incaricati degli "*audit sulla sicurezza, periodici e mirati, nonché le scansioni di sicurezza di cui agli articoli 35 e 37*". Le caratteristiche tecnico-organizzative da specificare potrebbero essere, ad esempio, l'accreditamento presso Accredia o altri Enti firmatari dell'accordo di mutuo riconoscimento IAF MLA, ovvero l'appartenenza ad un albo istituito dall'ACN stessa.

- **Articolo 36 (*Verifiche e ispezioni*)** - Al fine di semplificare l'attività di controllo dell'ACN, si potrebbe pensare, in un'ottica di efficienza della stessa, di prevedere una procedura semplificata di controllo per tutti i soggetti che rientrano nell'ambito di applicazione del decreto, in possesso di certificazione ISO/IEC 27001. Con riferimento al comma 1, l'integrazione potrebbe essere: "*Qualora i soggetti siano titolari di una certificazione ISO/IEC 27001, rilasciata sotto accreditamento di un ente firmatario degli accordi di mutuo riconoscimento IAF MLA in relazione ad un campo d'applicazione correlato ai processi e servizi per i quali i soggetti rientrano nell'applicazione del presente Decreto, l'Autorità nazionale competente NIS può acquisire informazioni sulla vigenza e validità del certificato in vece delle azioni di cui ai punti a) e b)*".