NIS2: Verso un nuovo paradigma per la sicurezza integrata

Roberto Sammarchi

Avvocato, Consigliere nazionale AIAS

Associazione Italiana Ambiente e Sicurezza

Innovazione digitale e prevenzione negli ambienti di lavoro: obbligo, non scelta

- I soggetti la cui **posizione di garanzia** è delineata nelle norme in materia di obblighi prevenzionali **devono** applicare le misure idonee per la gestione e la riduzione del rischio. Il **T.U. Sicurezza**, **Art. 15** – Misure generali di tutela, comma 1), lettera c) prevede l'eliminazione dei rischi e, ove ciò non sia possibile, la loro riduzione al minimo **in relazione alle conoscenze acquisite in base al progresso tecnico**.

- **SE** nuove tecnologie intelligenti, approccio safety by design, intelligenza artificiale, internet delle cose, nuovi paradigmi in materia di interazione fra lavoratori e apparati tecnico- produttivi, ecc., consentono eliminazione o riduzione dei rischi, **ALLORA** l'adozione di tali approcci e metodologie è **OBBLIGATORIA** e la **NON ADOZIONE** costituisce **CONDOTTA OMISSIVA** rilevante ai sensi dell'**art. 40, secondo comma del Codice Penale**.

L’invisibile confine fra sicurezza digitale e sicurezza fisica (safety)

- Nell'attuale contesto lavorativo, caratterizzato dall'avanzamento dell'intelligenza artificiale e delle tecnologie digitali, **l'integrazione tra sicurezza digitale e fisica** diventa cruciale. Questa necessità emerge dalla crescente complessità delle minacce che riguardano la sicurezza delle persone, dei processi produttivi e della gestione aziendale.

- L'Unione Europea, con la direttiva NIS2, mira a rafforzare la **sicurezza digitale**, richiedendo un impegno concreto da parte degli Stati membri entro ottobre 2024. Un impegno che sottolinea **l'integrazione di capacità gestionali e competenze tecnico-scientifiche** come risposta alle nuove minacce globali.

NIS2: (Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio)
misure per un livello comune elevato di cybersicurezza nell'Unione

- **Risposta agli Incidenti e gestione dei rischi**: Tutti gli enti inclusi sono obbligati a prendere **misure** appropriate per gestire i rischi per la sicurezza delle loro **reti** e **sistemi informativi** e a **segnalare** incidenti gravi alle autorità nazionali competenti.

- **Misure di sicurezza e conformità**: Impone misure tecniche e organizzative dettagliate per garantire un alto livello di sicurezza delle reti e dei sistemi informativi, con un'enfasi particolare sulla **resilienza** agli attacchi cibernetici.

- **Sanzioni**: Introduce sanzioni più severe per il mancato rispetto degli obblighi.

NIS2 e safety: un silenzio apparente

- NIS2 si concentra sulla sicurezza delle reti e dei sistemi informativi e non tratta direttamente la sicurezza fisica delle persone, tuttavia sostiene l'approccio della **sicurezza integrata**, tramite:

- **Protezione delle infrastrutture critiche**

- **Cooperazione e scambio di informazioni**

- **Misure di emergenza e continuità operativa**

- **NIS2** va letta in modo integrato con le norme europee in materia di resilienza dei prodotti che integrano elementi digitali e di responsabilità per danno da prodotto, nonché nella prospettiva del Regolamento Macchine.

NIS2 e assicurazione dei rischi: nuove sfide

- La Direttiva NIS2 influisce sugli obblighi delle **coperture assicurative** in modo significativo, soprattutto per le organizzazioni che operano nei settori essenziali o forniscono servizi digitali critici. Con l'introduzione di requisiti più stringenti di sicurezza e notifica, le aziende devono riconsiderare le proprie politiche assicurative per coprire potenziali rischi e sanzioni.

- Gli obblighi di resilienza e continuità operativa imposti dalla NIS2 possono spingere le aziende a cercare polizze assicurative che offrano copertura per perdite finanziarie causate da **interruzioni di attività** dovute ad attacchi informatici o altri incidenti di sicurezza.

- Le aziende potrebbero essere ritenute responsabili per qualsiasi danno derivante dalla **mancata protezione adeguata** dei dati o dalla **mancata prevenzione** di attacchi cibernetici. Polizze di assicurazione che coprano la responsabilità per **nuove ipotesi causali** di danni possono diventare necessarie.

Il quadro sanzionatorio in NIS2

- **Sanctions for Non-Compliance**: Gli Stati membri sono tenuti a stabilire regole su sanzioni per le violazioni della direttiva e devono garantire che queste sanzioni siano effettive, proporzionate e dissuasive..

- **Maximum Financial Penalties**: Per le violazioni gravi, le sanzioni finanziarie possono arrivare fino a un massimo di 10M€ o del 2% del fatturato annuo totale a livello mondiale dell'ente infrangente.

- **Specific Violations**: Mancata attuazione delle misure di sicurezza adeguate, mancata notifica tempestiva degli incidenti, non rispetto delle disposizioni relative alla gestione del rischio e alla segnalazione degli incidenti.

- **Daily Penalties**: In alcuni casi, possono essere imposte sanzioni giornaliere fino a quando non viene risolta la non conformità.

- **Public Statements**: Gli Stati membri possono prevedere l'obbligo di fare dichiarazioni pubbliche riguardo alle non conformità.

- **La cybersicurezza richiede competenze integrate per società, ambienti di lavoro, sistemi di produzione e prodotti più sicuri.**

- **L'attenzione alla cybersicurezza può dare un importante contributo al miglioramento della cultura della sicurezza nella società e nelle organizzazioni.**

Grazie per l'attenzione

Roberto Sammarchi
rsammarchi@networkaias.it