La rivoluzione normativa in tema Cyber: nuove responsabilità e attività di compliance

B-RIGHT
lawyers

PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Il legislatore ha individuato nella L. 133/2019 l'impalcatura del sistema di sicurezza che vuole creare demandando ad appositi **provvedimenti attuativi** l'implementazione delle procedure esecutive ed organizzative.
Ciascun provvedimento attuativo del Perimetro disciplinerà gli adempimenti a carico dei soggetti inclusi al suo interno.

predisporre, aggiornare e trasmettere annualmente la mappatura delle reti, dei sistemi informativi e dei servizi informatici (DPCM 131/2020)

notificare gli incidenti con impatto rilevante sulle funzioni ed i servizi essenziali per lo Stato (DPCM 81/2021)

implementare le misure di sicurezza prescritte (DPCM 81/2021)

comunicare al CVCN gli acquisti di beni ICT e integrare bandi e contratti secondo gli esiti dei test del CVCN (Reg. 54/2020 e DPCM 15 giugno 2021)

collaborare con le autorità nelle loro attività di ispezione e verifica

IL DPCM 81/2021 E LE MISURE DI SICUREZZA

B-RIGHT
lawyers

- DPCM 81/2021: misure di sicurezza e notifiche
- Tempistiche implementazione: **6 mesi** o **30 mesi** a seconda che le misure di sicurezza siano ricondotte alla categoria A o B nell'apposita tabella allegata al decreto

Seguendo il modello del Framework nazionale di cybersecurity, le misure di sicurezza si suddividono in categorie. Queste si suddividono, a loro volta, in sottocategorie che dettagliano le singole misure di sicurezza.

L'implementazione delle misure di sicurezza richiede attenzione al contesto normativo anche estraneo alle norme sulla cybersecurity, come la data privacy e il diritto del lavoro (Cfr 3.1.3. PROTECT, ACCESS CONTROL)

Altro esempio: all'interno della categoria IDENTIFY si trova la sottocategoria GOVERNANCE, che prevede tra le altre misure quella di considerare nel risk management i rischi connessi alla cybersecurity. Di qui la valutazione di una **assicurazione cyber (Cfr. 2.2.2. IDENTIFY, GOVERNANCE)**.

MDS	DESCRIZIONE CATEGORIA	PREMESSE ALLE DOMANDE	ID DOMANDA	DOMANDE
ID.GV-4	La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity.	PRIMO GRUPPO DI DOMANDE – PREPARAZIONE PER STIPULA O RINNOVO POLIZZA CYBER RISK	1	L'HR ha un piano diffuso di education per aumentare la consapevolezza dei rischi cyber e per formare la popolazione aziendale per prevenire e gestire gli stessi?
			2	L'Organizzazione è in grado di dimostrare che le varie funzioni aziendali ed i singoli, compreso il senior management, hanno svolto la formazione relativa al rischio cibernetico?
			3	Le funzioni di business/finance hanno evidenziato i collegamenti tra le linee di business e le minacce cibernetiche?
			8	Il DPO o la funzione privacy sono in grado di identificare le tipologie di dati personali gestiti (sanitari, giudiziari, finanziari, di HR, di minori) anche al fine della valutazione dell'impatto di un potenziale incidente?
			11	Sono stati effettuati recentemente audit sui fornitori e tali audit sono documentati e resi disponibili per l'assicuratore o potenziale assicuratore?
			12	La compagnia di assicurazione scelta offre servizi di assessment, pre-breach e risk management (la valutazione fatta dall'assicurazione sullo stato di cybersecurity del potenziale cliente viene offerta come servizio)?
		SECONDO GRUPPO DI DOMANDE – COMPRENSIONE DELLE CONDIZIONI DI POLIZZA	18	La polizza sottoscritta dall'Organizzazione copre i danni legati ad incidenti informatici causati da imprudenze, errori, imperizie o negligenze di soggetti interni?
			20	Nel caso in cui l'Organizzazione si sia dotata di una assicurazione che copra il rischio relativo ad attacchi informatici, la polizza copre anche i danni causati DA terze parti (es. fornitori)?
			21	La polizza assicurativa prevede la copertura dei costi di Business interruption a partire da subito oppure è previsto un waiting period?
			24	L'assicurazione offre servizi di prevenzione, quali la simulazione di breach per verificare la reazione dell'organizzazione e la lista fornitori controllati in punto cybersecurity (domanda specifica per piccole/medie imprese e assicurazioni)?
			32	La polizza consente all'Organizzazione di avvalersi di esperti di propria fiducia?
			34	La polizza prevede il risarcimento dei costi derivanti dall'assistenza di esperti scelti dall'Organizzazione (i.e. costi per il supporto degli specialisti IT, legali, digital forensic investigation)?

B-RIGHT
lawyers

SANZIONI

B-RIGHT
lawyers

Le violazioni degli obblighi previsti dal perimetro (attività di mappatura ICT, notifica degli incidenti, comunicazione al CVCN) comporta sanzioni:

Sanzioni amministrative pecuniarie fino ad € 1.800.000

Contestazione di reato

Con la revisione della Direttiva NIS le sanzioni potranno arrivare a 10 milioni di euro o fino al 2% del fatturato totale annuo mondiale dell'impresa interessata.

Reati presupposto d.lgs. 231/01

Sanzione amministrativa accessoria

L'impiego di prodotti e servizi sulle reti, sui sistemi e per l'espletamento di servizi in assenza della comunicazione o di superamento dei test del CVCN o in violazione delle condizioni dallo stesso imposte comporta, oltre le sanzioni pecuniarie, la sanzione accessoria **dell'incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese per tre anni a decorrere dall'accertamento della violazione.**


B-RIGHT
lawyers