lawalert

31 agosto
2022

DPCM4
Decreto del Presidente del Consiglio dei Ministri del 18 maggio 2022

Il quarto ed ultimo decreto attuativo del decreto-legge 21 settembre 2019 n. 105 ("Perimetro di Sicurezza Cibernetica" o "Legge Perimetro") è stato pubblicato in Gazzetta Ufficiale in data 15 luglio 2022.

Si tratta del Decreto del Presidente del Consiglio dei Ministri del 18 maggio 2022 o "DPCM4[1]" che, assieme ai DPCM 30 luglio 2020, n. 131 (cd. DPCM1, recante il regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'art. 1, comma 2 della Legge Perimetro), 14 aprile 2021, n. 81 (cd. DPCM2, recante il regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui alla Legge Perimetro, e di misure volte a garantire elevati livelli di sicurezza) e 15 giugno 2021 (cd.DPCM3, recante l'individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'art. 1, comma 6, lett. a) della Legge Perimetro), completa l'architettura del Perimetro di sicurezza nazionale cibernetica.

Grazie a questo decreto - come confermato dall'Agenzia per la Cybersicurezza Nazionale - "*si è compiuto un importante passo per raggiungere gli obiettivi contenuti nella Strategia Nazionale di Cybersicurezza, volto ad innalzare il livello di sicurezza della supply chain di infrastrutture da cui dipende l'erogazione dei servizi essenziali dello Stato*".

Come richiesto dalla Legge Perimetro, il DPCM4 stabilisce le procedure e le modalità per l'accreditamento dei centri di valutazione (o "CV") e dei laboratori accreditati di prova, nonché per la gestione dei raccordi del Centro di valutazione e certificazione nazionale (cd. "CVCN") con i centri di valutazione accreditati e con i laboratori accreditati di prova (cd. "LAP"), anche al fine di "*assicurare il coordinamento delle rispettive attività e proseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio*".

Il CVCN, a sua volta, potrà accreditare laboratori sia pubblici che privati, destinati a costituire la rete a supporto dello stesso CVCN nonché dei CV del Ministero della Difesa e del Ministero dell'Interno nelle attività di valutazione tecnologica di specifiche categorie di beni ICT utilizzati nel Perimetro di Cybersicurezza Nazionale.

Inoltre, il DPCM è abilitante alla realizzazione delle misure 1[2] , 2[3] , 5[4] , 8[5] e 53[6] previste dal Piano di Implementazione della Strategia Nazionale di Cybersicurezza per gli anni 2022-2026 pubblicata dall'Agenzia per la Cybersicurezza Nazionale.

1. Recante il "regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133".
2. sezione "scrutinio tecnologico": rafforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain delle particolari categorie di asset rientranti nel Perimetro e per l'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati.
3. sezione "scrutinio tecnologico": sviluppare le capacità dei Centri di Valutazione del Ministero dell'Interno e del Ministero della Difesa accreditati dall'ACN, quali organismi di valutazione della conformità, per i sistemi di rispettiva competenza.
4. sezione "definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente": supportare lo sviluppo, valutandone l'adeguatezza in termini di sicurezza nazionale, degli schemi di certificazione in materia di cybersicurezza e, in collaborazione con il settore privato, promuoverne l'adozione e l'utilizzo da parte dei fornitori di servizi e delle imprese italiane, favorendo lo sviluppo del tessuto imprenditoriale nazionale specializzato al fine di conseguire un vantaggio competitivo sul mercato.
5. sezione "definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente": introdurre norme giuridiche volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale.
6. sezione "impulso all'innovazione tecnologica e alla digitalizzazione": promuovere ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, riguardo a prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore, anche valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali.

Grazie a quanto previsto dal DPCM4, il CVCN avrà il potere di accreditare laboratori di prova pubblici e privati, che supporteranno lo stesso CVCN, i CV nelle attività tecniche di valutazione della sicurezza tecnologica dei beni ICT già definiti dal DPCM3.

In particolare, DPCM4 è strutturato come segue:

• Il Capo I del DPCM4 definisce l'ambito di applicazione dello stesso, stabilisce i compiti del CVCN, istituisce la commissione di accreditamento presso il CVCN con compiti consultivi, stabilisce la possibilità per il CVCN di collaborare con le Forze di polizia per la verifica dei requisiti soggettivi e dei motivi ostativi ai fini dell'accreditamento dei laboratori di prova, nonché stabilisce le modalità di determinazione delle aree di accreditamento;

• Il Capo II invece concerne le procedure di accreditamento dei laboratori di prova, definendo in particolare i requisiti generali per l'accreditamento, i requisiti soggettivi e i motivi ostativi ai fini dell'accreditamento dei laboratori di prova, le modalità di presentazione della domanda di accreditamento dei laboratori di prova di cui è titolare un soggetto privato e di quelli istituiti presso amministrazioni o enti pubblici, la procedura di accreditamento dei laboratori di prova, gli obblighi dei LAP, la vigilanza sulle attività dei LAP, le ipotesi di sospensione e la revoca dell'accreditamento, la procedure di rinnovo e variazione dell'accreditamento, la responsabilità dei LAP ed i corrispettivi per le attività di accreditamento e vigilanza effettuate dal CVCN;

• Il Capo III è dedicato all'accreditamento dei CV;

• Il Capo IV definisce i raccordi tra il CVCN da una parte e i CV e i LAP dall'altra;

• Il Capo V riguarda le procedure di notifica degli incidenti al CSIRT.

Lo scopo del DPCM4 - in conclusione - è quello di costituire una rete di laboratori accreditati e consentire di rafforzare la sicurezza delle infrastrutture digitali nazionali.

Con questo ultimo DPCM diventa operativo anche l'ultimo tassello del Perimetro di sicurezza nazionale cibernetica: un passo importante che va a completare lo scudo cibernetico a difesa delle infrastrutture critiche italiane.

***

Questo articolo è redatto a scopo informativo. Non si tratta di un parere legale esaustivo in materia di Cybersecurity. Per eventuali ulteriori informazioni e approfondimenti specifici vi invitiamo a contattare Roberto Camilli (Roberto.Camilli@bdo.it), Gabriele Ferrante (Gabriele.Ferrante@bdo.it) e Sofia Ferri (Sofia.Ferri@bdo.it).

Contatti:
BDO Law S.r.l. Sta

Milano
Viale Abruzzi, 94