lawalert

21 settembre
2022

Decreto Certificazioni
D.Lgs. n. 123 del 3 agosto 2022

È stato pubblicato nella Gazzetta Ufficiale del 20 agosto 2022 il D.Lgs. n. 123 del 3 agosto 2022 (nel seguito il "Decreto Certificazioni").

Si tratta del Decreto recante le norme di adeguamento della normativa italiana alle disposizioni del Titolo III "Quadro di certificazione della cibersicurezza" del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

Questo decreto individua:

- Le modalità di cooperazione dell'organizzazione dell'autorità nazionale di certificazione della cibersicurezza in Italia (Agenzia per la cibersicurezza nazionale o "ACN") ed i compiti di vigilanza e rilascio dei certificati di cibersicurezza attribuiti alla stessa;
- Le modalità di cooperazione dell'ACN con le altre autorità nazionali ed europee e con l'Organismo di accreditamento;
- Un sistema sanzionatorio applicabile in caso di violazione delle norme previste dal Decreto Certificazioni.

Il Decreto Certificazioni fa salve espressamente le disposizioni specifiche in materia di pubblica sicurezza, difesa, sicurezza nazionale che continuano a trovare applicazione e l'attività dello Stato relativa all'ambito penalistico.

Grazie a questo decreto viene previsto che l'ACN sia divisa internamente in due parti, una dedicata alla emissione delle certificazioni di cibersicurezza ed una riservata alle attività di vigilanza dell'ACN.

Compiti di vigilanza dell'ACN

Il decreto - come anticipato sopra - attribuisce all'ACN il compito di vigilare affinché nel territorio italiano le norme in materia di certificazione della cibersicurezza siano correttamente applicate. I poteri di vigilanza dell ACN si estendono in particolare al controllo dei fornitori e dei fabbricanti emittenti le dichiarazioni UE di conformità, dei titolari dei certificati europei di cibersicurezza e degli organismi di valutazione della conformità.

L'ACN può esercitare tali poteri anche effettuando indagini od audit nei confronti dei soggetti sopra indicati, accedendo ai locali di questi, nonché revocare i certificati, irrorare sanzioni pecuniarie ed accessorie e prelevare prodotti.

Qualora a seguito di tali attività l'ACN dovesse riscontrare la sussistenza di un certificato non conforme, potrà revocare tale certificato nei casi espressamente previsti all'art. 5 (vigilanza nazionale) del Decreto Certificazioni.

L'ACN potrà altresì richiedere all'organismo emittente il certificato di ripetere in tutto o in parte l'attività di valutazione o di integrarla al fine di ricondurre il certificato a conformità entro 120 giorni o revocare il certificato. Qualora l'organismo ometta di compiere queste attività è prevista la decadenza del certificato.

L'ACN può anche effettuare valutazioni di sicurezza informatica ed i soggetti sottoposti a tali valutazioni hanno l'obbligo di cooperare con l'ACN.

Il Decreto Certificazioni prevede che gli oneri per le attività di verifica dell'ACN siano a carico del soggetto sottoposto all'attività di vigilanza di quest'ultima.

Rilascio dei certificati di cibersicurezza

Salve leggi speciali in senso contrario, la certificazione della cibersicurezza viene prevista come volontaria. Si tratta di un documento rilasciato da un organismo di certificazione che attesta che un determinato prodotto, servizio o processo ICT è stato oggetto di una valutazione di conformità rispetto agli standard di sicurezza nazionali ed europei.

Qualora la certificazione sia prevista come obbligatoria, il Decreto Certificazioni prevede sanzioni ed il ritiro dei prodotti dal mercato per i fabbricanti o fornitori che immettano sul mercato prodotti o servizi ICT privi della certificazione.

Il Decreto Certificazioni stabilisce che i certificati di cibersicurezza con livello di affidabilità elevato vengano rilasciati dall'ACN tramite l'Organismo di Certificazione della Sicurezza informatica (cd. "OCSI"), e la medesima procedura verrà

utilizzata in caso di concessione di certificati con livello di affidabilità sostanziale o di base quando uno specifico sistema di certificazione prevede che questi vengano rilasciati mediante un organismo pubblico (in alternativa il rilascio della certificazione in quest'ultimo caso potrà avvenire ad opera di un altro organismo di certificazione della conformità pubblico accreditato dall'Organismo di Accreditamento, monitorato, vigilato e designato dall'ACN).

È previsto che gli oneri per il rilascio dei certificati siano a carico del soggetto che ne richiede il rilascio.

Le dichiarazioni UE di conformità

Il Decreto Certificazione prevede inoltre che i fornitori o fabbricanti di prodotti, servizi o processi relativi al settore della Tecnologia dell'Informazione e della Comunicazione (cd. "Prodotti TIC") possano rilasciare sotto la propria responsabilità dichiarazioni UE di conformità di livello base[1] per dimostrare di possedere i requisiti previsti dalla normativa.

Tali soggetti dovranno rendere disponibili le dichiarazioni all'ACN ed a ENISA, unitamente alla documentazione tecnica e a tutte le altre informazioni pertinenti e relative alla conformità dei prodotti.

Qualora l'ACN ritenga non conforme una certificazione il fornitore o fabbricante del Prodotto ICT avrà l'obbligo di revisionare o revocare la propria dichiarazione entro 30 giorni.

Sanzioni

In caso di violazioni delle disposizioni del Decreto Certificazioni l'ACN ha il potere di irrogare sanzioni pecuniarie piuttosto importanti. Infatti, tali sanzioni possono arrivare nei casi più gravi ad Euro 5.000.000.

Reclami e ricorsi

Il Decreto Certificazioni indica le modalità mediante le quali le persone fisiche o giuridiche possono proporre reclamo avverso i certificati rilasciati dall'ACN o dai suoi organismi di certificazione.

Il Decreto certificazioni chiarisce altresì che l'impugnazione avverso i) le decisioni dell'ACN o degli organismi di valutazione della conformità o ii) il mancato o parziale accoglimento di un reclamo presentato all'ACN o agli organismi di valutazione della conformità devono essere proposte dinnanzi al Tribunale amministrativo regionale del Lazio – se riguardano le decisioni dell'ACN – o – se riguardano decisioni di altri organismi di certificazione - al Tribunale del luogo in cui ha sede tale l'organismo di certificazione.

Conclusione

Il Decreto Certificazioni si inserisce all'interno del telaio normativo che disciplina la difesa delle infrastrutture critiche italiane e che negli ultimi anni ha visto un costante e crescente sviluppo.
Gli operatori del mercato che intendessero richiedere una certificazione di cibersicurezza dovranno rispettare queste nuove previsioni per evitare di incorrere in sanzioni.

***

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).

[1] Il Decreto Certificazioni prevede i seguenti tre livelli di conformità:

i) «**livello di affidabilità di base**»: livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al paragrafo 5 dell'articolo 52 del regolamento (UE) 2019/881 (assicura che i prodotti, i servizi e i processi ICT per i quali è rilasciato il certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Le attività di valutazione da intraprendere comprendono almeno un riesame della documentazione tecnica. Qualora tale riesame non sia appropriato, si ricorre ad attività di valutazione sostitutive di effetto equivalente);

ii) «**livello di affidabilità sostanziale**»: livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al paragrafo 6 dell'articolo 52 del regolamento (UE) 2019/881 (assicura che i prodotti, i servizi e i processi ICT per i quali è rilasciato il certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti, i servizi e i processi ICT attuano correttamente le necessarie funzionalità di sicurezza. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività di valutazione sostitutive di effetto equivalente); «**livello di affidabilità elevato**»: livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al paragrafo 7 dell'articolo 52 del regolamento (UE) 2019/881 (assicura che i prodotti, i servizi e i processi ICT per i quali è rilasciato il certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC, i servizi TIC o i processi TIC attuano correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività sostitutive di effetto equivalente).

Contatti:
BDO Law S.r.l. Sta

Milano
Viale Abruzzi, 94