NOTA
DECRETO LEGGE recante disposizioni urgenti in materia di
"PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA"

Il provvedimento, istituendo il cosiddetto "**Perimetro di sicurezza nazionale cibernetica"** ("Perimetro"), si affianca al D.Lgs. n. 65/2018 di recepimento della Direttiva europea "Network and Information Security" ("Direttiva NIS").

Lo **scopo della Direttiva NIS** è quello di stabilire misure volte a "*conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea",* al fine ultimo di ridurre la probabilità che accada un disservizio di rilevante impatto per la popolazione servita. A tal fine si prevede, tra l'altro, **l'individuazione degli Operatori di Servizi Essenziali** ("OSE") ed il rispetto da parte di questi e dei fornitori di servizi digitali di obblighi relativi all'adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante.

Sulla base di un approccio "**risk based**", la Direttiva NIS pone a carico degli operatori la responsabilità di valutare ed individuare le misure "adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni" tenuto conto di quanto previsto in linee guida predisposte dal gruppo di coordinamento o dalle autorità competenti NIS.

Il decreto legge sul Perimetro ha come obiettivo quello di ***"assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici*** *delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali, o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale".*
Sono, infatti, stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici relative a: politiche di sicurezza; gestione del rischio; prevenzione, mitigazione e gestione di incidenti; struttura organizzativa in materia di sicurezza; protezione fisica e logica; protezione dei dati; integrità delle reti e dei sistemi informativi; continuità operativa; gestione operativa; monitoraggio, test e controllo; formazione e consapevolezza; affidamento di forniture di beni, sistemi e servizi ICT.

Le nuove norme, tra l'altro:

- definiscono le finalità del perimetro e le modalità di individuazione dei soggetti pubblici e privati che ne fanno parte, nonché delle rispettive reti, sistemi informativi e servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica;
- prevedono il coinvolgimento del Comitato interministeriale per la sicurezza della Repubblica (CISR) nella fase attuativa;
- definiscono le procedure secondo cui i soggetti inclusi nel Perimetro notificano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano;
- prevedono che l'esercizio dei poteri speciali in relazione alle reti, ai sistemi informativi e ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G sia effettuato previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità da parte dei centri di valutazione individuati dalla nuova normativa e, con riferimento alle autorizzazioni già rilasciate ai sensi del decreto-legge 15 marzo 2012, n. 21, la possibilità di integrare o modificare le misure prescrittive già previste alla luce dei nuovi standard.

OSSERVAZIONI

1. Entro 4 mesi dalla data di entrata in vigore della legge di conversione del decreto legge sono individuati i soggetti inclusi nel perimetro che predisporranno e aggiorneranno con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici, **"comprensivo della relativa architettura e componentistica". Quest'ultimo aspetto genera incertezze applicative fra gli operatori, in quanto parlare di aspetti architetturali e componentistici è tanto indeterminato da poter includere opzioni infinite e di eccessivo dettaglio.**
   Se interpretata in senso estensivo, la comunicazione dell'elenco delle reti, comprensivo di schemi architetturali e dettagli sulla componentistica, rischia pertanto di trasformarsi in un adempimento macroscopico, ma di scarsa utilità pratica rispetto al vero obiettivo di tutela della sicurezza nazionale.

2. Nel particolare contesto del sistema elettrico è opportuno osservare che la presenza di un numero esteso e crescente di produttori di energia, soprattutto di piccole e medie dimensioni, potrebbe influire sulla sicurezza dell'intero sistema, considerato il fattore di scala con il quale un'eventuale comune vulnerabilità degli stessi potrebbe essere sfruttata per attacchi cibernetici su vasta scala.
   Ipotizzando che tali soggetti non rientrino tra quelli individuati nel perimetro di sicurezza cibernetica di cui al presente decreto, è auspicabile comunque che il quadro normativo e regolatorio in materia ricomprenda anche prescrizioni per i soggetti che gestiscono infrastrutture interconnesse con quelle dei grandi operatori.

3. Si introducono disposizioni che potrebbero portare ad una **vera e propria paralisi degli approvvigionamenti IT dei soggetti obbligati**, tra cui grandi operatori coinvolti nello sviluppo del digitale a sostegno e implementazione delle proprie attività. Infatti, **l'art. 1 comma 6 lett. a)** prevede a carico dei soggetti inclusi nel Perimetro che intendano procedere all'**approvvigionamento di beni, sistemi e servizi ICT** destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti, obblighi di comunicazione e cooperazione con il **Centro di Valutazione e Certificazione nazionale** ("CVCN" istituito presso il MISE). Il CVCN, **sulla base di una propria valutazione di rischio, potrà imporre condizioni e test di hardware e software (con oneri a carico dei fornitori) e, in tale ipotesi, integrare bandi di gara o contratti con clausole** che subordinino l'affidamento della fornitura o del servizio al rispetto delle condizioni e all'esito dei suddetti test.
   Per quanto riguarda l'ambito degli obblighi di comunicazione, il DL detta una definizione assai ampia, che include beni, sistemi e servizi ICT, quindi non solo devices ma anche servizi. Andrebbe meglio chiarito se e quali servizi di supporto informatico (ad es. sviluppo e manutenzione di sistemi applicativi) siano inclusi e che tipo di verifiche e test siano ipotizzabili.
   È, altresì, auspicabile che venga chiarita anche la gestione del ciclo di vita dei dispositivi oggetto di test hardware e software da parte del citato CVCN, considerato che si tratta di elementi normalmente sottoposti a periodici aggiornamenti durante il loro periodo di impiego all'interno di reti e sistemi informativi.
   Infine, spostando il focus sull'esecuzione di test formali su specifici prodotti, sistemi e servizi in fase di acquisizione, si rischia di svilire l'importanza dell'approccio risk based, già fondamento della direttiva NIS, del GDPR e peraltro enunciato dallo stesso DL all'art.1, comma 3, punto 1) lett. b).

In conclusione, considerate anche le misure organizzative, tecniche ed operative che i soggetti OSE sono già tenuti ad adottare per il rispetto della Direttiva NIS, si suggerisce che il potere in capo al CVCN di imporre test venga adeguatamente circoscritto nel suo effettivo ambito di applicazione, riferendolo ad un numero estremamente limitato di ambiti e componenti e prevedendo modalità e tempi chiari e definiti, in modo da non turbare i normali processi di approvvigionamento.

L’esigenza di garanzia di adeguati standard di sicurezza potrebbe essere garantita attraverso l’adozione di apposite linee guida ed attraverso un meccanismo di certificazione dei prodotti integrativo rispetto a quelli europei già presenti e da ultimo disciplinati dal Regolamento (UE) 2019/881 (c.d. Cybersecurity Act), proprio a maggior tutela della sicurezza nazionale.