QUADERNI DI SOSTENIBILITÀ

RECEPIMENTO DELLA DIRETTIVA UE 2022/2555

NIS 2

Gestione strategica della cyber sicurezza

Dopo mesi di attesa, è stato pubblicato ieri in Gazzetta Ufficiale il Decreto Legislativo 138/2024 che recepisce nel nostro ordinamento la Direttiva NIS 2.
Innanzitutto, nel testo normativo si legge che **le disposizioni si applicheranno** a decorrere dal 16 ottobre 2024.
Inoltre, gli enti dovranno necessariamente **attendere ancora qualche mese** per sapere con precisione se e a quali obblighi sono tenute.
Il primo passo, infatti, sarà quello di **identificare puntualmente** gli operatori che rientreranno nell'ambito di applicazione della normativa. Nello specifico, riprendendo il testo europeo, il Decreto Legislativo 138/2024 stabilisce anzitutto che tra questi vi saranno i soggetti privati e pubblici che operano nei settori indicati rispettivamente dagli allegati I-II e III-IV del decreto. Rispetto alla Direttiva europea, però, il testo italiano aggiunge una piccola precisazione statuendo che **gli operatori devono essere soggetti alla giurisdizione nazionale**.

Inoltre, è confermato che la normativa non si applicherà alle piccole imprese a meno che l'ente non sia:

- identificato come "**critico**" ai sensi della Direttiva RCE;
- fornitore di **reti pubbliche di comunicazione elettronica** o di **servizi di comunicazione elettronica** accessibili al pubblico;
- prestatore di **servizi fiduciari**;
- **gestore di registri di dominio** di primo livello o fornitore di servizi di sistema dei nomi a dominio;
- **fornitore di servizi di registrazione** dei nomi a dominio;
- già stato identificato come operatore di **servizi essenziali** o fornitore di **servizi digitali** ai sensi della Direttiva NIS;
- l'unico fornitore nazionale di un servizio essenziale;
- fornitore di un servizio che, se perturbato, potrebbe comportare un **rischio sistemico** significativo;
- critico per la sua **particolare importanza a livello nazionale**;
- critico in quanto elemento **sistemico della catena di approvvigionamento di soggetti essenziali o importanti**.

La Catena del Valore

La normativa di recepimento della Direttiva NIS 2 non si focalizza solo sui s**ettori ritenuti ad alta criticità o critici**, ma, in maniera lungimirante, **anche sui loro fornitori** andando ad ampliare notevolmente il novero di soggetti che verosimilmente saranno interessati dall'applicazione del Decreto Legislativo.

Inoltre, la Direttiva NIS 2 e il Decreto 138/2024 si applicheranno **anche a tutte le Società che esercitano un'influenza dominante o che possono, in altro modo, influire sulle decisioni relative alla gestione della sicurezza informatica di un soggetto essenziale o importante o che ne gestiscano a vario titolo i sistemi informatici**.
Tra gli enti così identificati, la normativa prevede altresì una suddivisione tra soggetti essenziali ed importanti a seconda delle dimensioni e dei servizi erogati.
Tuttavia, come già anticipato brevemente, nonostante tali indicazioni preliminari, sarà necessario attendere ancora qualche mese per avere una precisa identificazione degli enti che saranno chiamati ad attuare le disposizioni della Direttiva NIS 2. Infatti, coloro che possono essere qualificati come soggetti essenziali o importanti dovranno registrarsi a partire dalla data di pubblicazione su un'apposita piattaforma messa a disposizione dall'Agenzia per la Cybersicurezza Nazionale (ACN) la quale, entro aprile 2025, redigerà l'elenco delle aziende e delle PA interessate.

Analogamente a quanto già avvenuto con la Direttiva NIS 1 e con il Perimetro di Sicurezza Nazionale Cibernetica, l'ACN provvederà anche a notificare singolarmente a ciascuna entità l'avvenuta inclusione nell'elenco di soggetti a cui si applicherà la disciplina.

Riprendendo la formulazione adottata dal legislatore europeo, il Decreto Legislativo **impone ai soggetti essenziali ed importanti di adottare misure tecniche, operative e organizzative adeguate e proporzionate** alla gestione dei rischi posti alla sicurezza dei sistemi informativi utilizzati nella fornitura dei servizi e per ridurre l'impatto degli incidenti per i destinatari dei servizi.
Ancora una volta, il Decreto Legislativo non entra nel merito delle misure di sicurezza che dovranno essere adottate. Il dettaglio sarà definito dall'ACN sulla base dei seguenti parametri:

- il grado di esposizione al rischio;
- la dimensione dell'ente;
- la probabilità che si verifichino incidenti e
- la gravità (incluso l'impatto economico e sociale).

Tuttavia, è possibile che numerosi enti che saranno soggetti alla normativa in analisi avranno già una cyber maturity tale da consentirgli di attuare misure che siano più che altro migliorative rispetto a quelle già esistenti. Dunque, verosimilmente, questa normativa **non si pone come una rivoluzione rispetto al passato**. Per questo motivo, in un'ottica di adeguamento, **sarà prezioso il contributo di professionisti di area tecnica e legale con un'ampia esperienza sul tema, che sappiano mappare e valorizzare le attività già svolte dall'ente**.

La Gestione delle situazioni critiche

Il Decreto di recepimento prevede che i soggetti che saranno qualificati come essenziali o importanti dovranno comunicare e aggiornare annualmente, tramite la **piattaforma messa a disposizione da ACN**, un elenco delle attività svolte e dei servizi erogati. In tal modo, sarà possibile garantire un'applicazione proporzionata e graduale degli obblighi che saranno differenziati in base a:

- le categorie di rilevanza individuate dall'Agenzia;
- il settore, sotto-settore e tipologia di soggetto, anche in considerazione del grado di cyber maturity iniziale;
- la classificazione come essenziale o importante.

Inoltre, il Decreto di recepimento **rinforza gli obblighi di notifica degli incidenti**, prevedendo che dovranno essere segnalati al CSIRT Italia, senza ingiustificato ritardo, gli incidenti che hanno un impatto significativo sulla fornitura dei servizi, ossia quelli che:

- hanno causato o possono causare una grave perturbazione dei servizi o perdite finanziarie;
- hanno avuto ripercussioni o possono avere ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Il processo di notifica prevede **tempistiche** serrate:

- una prenotifica entro **24 ore** che indichi se l'incidente ha una natura illecita o malevola e se può avere un impatto transfrontaliero;
- una notifica entro le **72 ore** dall'evento che aggiorni le informazioni della prenotifica e contenga una valutazione iniziale sulla gravità e sull'impatto, nonché gli indicatori di compromissione;
- una **relazione intermedia**, se richiesta dal CSIRT Italia;

- **una relazione finale entro un mese** dall'evento in cui si fornisca una descrizione di maggior dettaglio, la causa, le misure adottate e l'eventuale impatto transfrontaliero. Qualora, al momento della relazione finale l'incidente sia ancora in corso, sarà necessaria anche **una relazione mensile sui progressi**.

Inoltre, per la prima volta il Decreto Legislativo formalizza l'obbligo per il CSIRT Italia di fornire un supporto agli enti che hanno subito un attacco informatico. Infatti, entro 24 ore dalla prenotifica, il CSIRT Italia è tenuto a dare un riscontro sull'incidente ed eventuali orientamenti sulle possibili misure di mitigazione. In aggiunta, su richiesta del soggetto, dovrà anche fornire un supporto di natura tecnica. Il ruolo del CSIRT, però, non si ferma qui. Qualora vi sia il sospetto che l'incidente abbia carattere criminale, dovrà fornire altresì orientamenti sull'opportunità di segnalare l'evento all'organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione.

Infine, il Decreto di recepimento della Direttiva NIS 2 non si limita a prevedere un obbligo di notifica alle autorità. Infatti, **i soggetti essenziali e importanti sono tenuti a notificare gli incidenti significativi anche ai destinatari dei loro servizi laddove possano ripercuotersi negativamente sulla fornitura**. Ove possibile, sentito il CSIRT, è necessario comunicare anche eventuali minacce significative a cui tali destinatari dovessero essere soggetti fornendo un'indicazione delle possibili misure o azioni correttive o di mitigazione che questi possono adottare.

Come prepararsi

E' necessario un **attento assessment** che aiuti gli enti a definire le situazioni in cui è opportuno procedere con tali comunicazioni, anche alla luce del contesto in cui si muove l'operatore. Ciò anche in considerazione del fatto che dall'entrata in vigore del Decreto Legislativo discendono anche **obblighi di comunicazione delle vulnerabilità** e, di conseguenza, la **necessità di definire una strategia in materia**.

Inoltre, in linea con quanto già previsto dalla precedente versione della Direttiva, è prevista la facoltà per l'ACN di informare il pubblico di eventuali incidenti significativi, al fine di evitare che gli effetti dello stesso si propaghino o per una migliore gestione dell'evento. Un'ulteriore ipotesi in cui è ammessa la divulgazione di tali informazioni è quella in cui vi sia un interesse pubblico.

Al di là degli obblighi di notifica sopra delineati, coerentemente con il testo europeo, il Decreto di recepimento prevede anche **la facoltà di notificare gli incidenti su base volontaria**. Questa possibilità è riconosciuta non solo ai soggetti essenziali ed importanti, che potranno notificare gli eventi che non hanno un impatto significativi, ma anche a tutti gli altri attori nazionali.

Un importante elemento di novità è rappresentato dalla possibilità per l'Agenzia per la Cybersicurezza Nazionale di **imporre ai soggetti essenziali e importanti l'utilizzo di determinati prodotti, servizi e processi "TIC"**, ossia relativi alle tecnologie dell'informazione e della comunicazione.
L'obbligo in questione si applicherebbe sia che essi siano sviluppati dal soggetto essenziale o importante stesso, che siano acquistati presso terze parti.

Tale disposizione sicuramente fornirà un'accelerazione ai processi di certificazione a livello di Unione europea, favorendo così lo sviluppo di un mercato più sicuro e affidabile.

Il medesimo obiettivo è conseguito anche attraverso la facoltà riconosciuta all'ACN di promuovere l'uso di specifiche tecniche e di **predisporre e aggiornare periodicamente** un elenco delle categorie di **tecnologie più idonee ad assicurare l'effettiva implementazione di misure di gestione dei rischi**. Tale elenco non è vincolante né esaustivo e dovrà essere pubblicato sul sito dell'Agenzia.

Tale disposizione sicuramente fornirà un'accelerazione ai processi di certificazione a livello di Unione europea, favorendo così lo sviluppo di un mercato più sicuro e affidabile.

Regime sanzionatorio

Nonostante sia ancora necessario attendere qualche tempo per avere contezza degli esatti obblighi che saranno posti dalla normativa, il Decreto Legislativo introduce **una certezza: vi sarà una responsabilità degli organi di amministrazione e direttivi**. Seguendo la falsariga di quanto già stabilito dal Regolamento DORA per le entità finanziarie, gli organi di gestione delle società saranno chiamati ad avere un ruolo attivo nella compliance alla normativa.

Infatti, **essi dovranno approvare le modalità di implementazione delle misure per la gestione dei rischi per la sicurezza, sovrintendere all'implementazione degli obblighi stabiliti dalla normativa e saranno considerati responsabili per le violazioni.**

Inoltre, dovranno essere tempestivamente informati degli incidenti informatici notificati al CSIRT Italia. E' opportuno che le attività di compliance siano pianificate in un'ottica che non sia di natura esclusivamente tecnica, ma bensì che tenga in considerazione possibili responsabilità sul piano legale.

Il compito di supervisionare la corretta applicazione delle disposizioni della Direttiva NIS 2 e di esercitare i poteri sanzionatori è stato attribuito alla nostra Agenzia per la Cybersicurezza Nazionale.

Il trattamento sanzionatorio viene differenziato in base al tipo di violazione e alla qualifica del soggetto. In particolare, la violazione dei seguenti obblighi è sanzionata, **in caso di soggetti essenziali**, fino a 10 milioni o fino al 2% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, o, **in caso di soggetti importanti**, fino a 7 milioni o fino al 1,4% del totale del fatturato mondiale:

- **l'inosservanza degli obblighi imposti agli organi di amministrazione**;
- **la mancata implementazione delle misure tecniche, organizzative ed operative**;
- **l'assenza di notifica**.

Una novità introdotta dal Decreto Legislativo è la previsione di un minimo edittale delle sanzioni che è un ventesimo o di un trentesimo del massimo edittale rispettivamente per i soggetti essenziali e quelli importanti.

È prevista una sanzione fino al 0,1% o fino allo 0,07% del fatturato mondiale annuo per le violazioni considerate meno gravi, ossia:

- **la mancata registrazione, comunicazione o aggiornament**o delle informazioni sulla piattaforma dell'ACN;
- **l'inosservanza delle modalità stabilite da ACN per la registrazione, comunicazione o aggiornamento** dei dati;
- la **mancata comunicazione o aggiornamento dell'elenco delle attività e servizi** ai fini della loro categorizzazione;
- la **mancata attuazione degli obblighi relativi agli schemi di certificazione**;
- la **mancata collaborazione** con l'ACN nello svolgimento dei suoi compiti e nell'esercizio dei suoi poteri;
- la **mancata collaborazione** con il CSIRT Italia.

In caso di **reiterazione** delle violazioni, le sanzioni possono essere aumentate fino al triplo.

In aggiunta a quanto sopra, sono previste anche delle sanzioni che potremmo definire "accessorie". Infatti, in caso di diffida da parte dell'ACN che richieda l'implementazione di determinate misure che venga ignorata, è possibile sospendere temporaneamente un certificato o un'autorizzazione relativi ai servizi erogati dal soggetto. Inoltre, nella medesima ipotesi, le conseguenze possono ripercuotersi anche sul management, che non potrà svolgere funzioni dirigenziali nell'ente.

ATLANTE

#abilitatoridellasostenibilità

www.atlanteconsulting.it