HWG Sababa

Direttiva NIS 2: Come cambia la cybersecurity in Europa



La nuova Direttiva europea amplia l'ambito di applicazione della precedente NIS – Network Information Systems - e adotta un approccio articolato che si basa sul concetto di "multirischio".

Nei successivi paragrafi i punti chiave che le imprese e le organizzazioni dovrebbero conoscere per adempiere alle nuove linee guida.
Il 17 gennaio 2023 è entrata in vigore la Direttiva europea 2022/2555, nota come Direttiva NIS 2. Nello stesso giorno è cominciata la decorrenza del termine di ventuno mesi entro i quali vanno assolti due obblighi: il primo riguarda gli Stati membri dell'Unione, tenuti ad adottare e pubblicare i relativi provvedimenti nazionali di recepimento; il secondo è diretto ai soggetti pubblici e privati interessati dalla normativa, che devono preparare e allineare organizzazioni e processi ai nuovi obblighi di sicurezza.

La Direttiva NIS 2 introduce misure più specifiche e stringenti sul terreno del cyber risk management e amplia il novero dei settori e dei soggetti interessati dall'originaria Direttiva NIS, dalla quale il nuovo atto europeo prende forma e sostanza.



Considerato unanimemente come il primo capitolo della strategia legislativa europea in materia di cybersecurity, la Direttiva NIS (2016/1148) è stata recepita in Italia attraverso il Decreto Legislativo 65/2018 e rimarrà in vigore fino al 18 ottobre 2024.

Il suo contenuto – in estrema sintesi – fissa specifici obiettivi di cyber risk management; obiettivi che, tuttavia, si sono da subito rivelati difficili da raggiungere, richiedendo un pressoché immediato aggiornamento delle misure legislative da adottare.

Dalla NIS alla NIS 2: analisi di un passaggio necessario

La Direttiva NIS ha svolto un ruolo cruciale nell'incrementare l'awareness degli Stati membri sul tema della cybersecurity; tuttavia è necessario evidenziare anche i limiti della normativa, soprattutto nella fase di attuazione. Diversi sono i fattori che hanno contribuito alle difficoltà di attuazione della già complessa normativa. Tra questi, l'arrivo imprevedibile della pandemia di Covid-19 ha mutato repentinamente il sistema socio-economico globale, obbligando organizzazioni pubbliche, aziende private e professionisti a una rapidissima integrazione di nuove soluzioni e servizi digitali nei processi produttivi, spesso trascurando la necessaria attenzione sul tema della sicurezza informatica. Vanno tuttavia evidenziate anche le lacune del legislatore europeo nell'immaginare la complessità dell'armonizzazione delle norme europee con gli ordinamenti giuridici nazionali.

La direttiva NIS ha evidenziato limiti di attuazione, accentuati dall'accelerazione tecnologica impressa dalla pandemia.

I Paesi membri hanno goduto, in fase di recepimento della Direttiva NIS, di grandissima autonomia. Questo ha portato incertezze e disomogeneità su più piani: da chi doveva applicare le norme alle misure di sicurezza da implementare, fino ad arrivare alla condivisione, a livello europeo, delle informazioni relative agli incidenti.

Il tempo ha poi fatto emergere nuove categorie di soggetti divenute essenziali nell'ambito del corretto funzionamento del mercato europeo, che però risultavano escluse dall'ambito di applicazione della Direttiva NIS. Ciò ha reso le stesse categorie più deboli nella gestione di minacce e incidenti informatici.

L'evoluzione ha fatto emergere nuovi soggetti essenziali per il mercato UE, non adeguatamente tutelati dalla direttiva NIS.



Keyword

Approccio multirischio | Direttiva NIS | Cyber Risk | Imprese | Unione Europea | Pubblica Amministrazione | Legislazione | Direttiva NIS 2 | Cybersecurity

Direttiva NIS 2: l'ambito di applicazione

Su queste basi e proprio a causa di questi punti critici, l'Unione Europea ha ampliato il campo di applicazione della Direttiva NIS 2. I sette settori contemplati dalla precedente direttiva restano invariati: energia, trasporti, banche, infrastrutture dei mercati finanziari, acqua potabile, sanità e infrastrutture digitali. Ai privati che vi operano si aggiungono invece i fornitori di servizi digitali, in particolare nei settori dell'e-commerce, dei motori di ricerca e del cloud computing. Un ampliamento dell'area dei destinatari della Direttiva NIS 2 si è avuto includendo ulteriori soggetti attivi in settori definiti "Ad alta criticità", che comprendono acque reflue, gestione dei servizi ICT (business-to-business), Pubblica Amministrazione e spazio.

La direttiva NIS 2 amplia l'area di applicazione rispetto alla NIS, aggiungendo ai sette precedenti due nuovi ambiti critici.

A chiudere l'ambito di applicazione della nuova direttiva è il corposo insieme degli "Altri settori critici", costituito dai seguenti:

- servizi postali e di corriere;
- gestione dei rifiuti;
- fabbricazione, produzione e distribuzione di sostanze chimiche;
- produzione, trasformazione e distribuzione di alimenti;
- fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro;
- fabbricazione di computer e prodotti di elettronica e ottica;
- fabbricazione di apparecchiature elettriche;
- fabbricazione di macchinari e apparecchiature Nca (Non Codificato/ Altrove);
- fabbricazione di autoveicoli, rimorchi e semirimorchi;
- fabbricazione di altri specifici mezzi di trasporto;
- fornitori di servizi digitali;
- organizzazioni di ricerca.

Oltre ad ampliare l'ambito di applicazione rispetto alla precedente direttiva, la NIS 2 precisa i concetti di "Operatore di servizi essenziali" e di "Fornitore di servizi digitali", identificati dagli Stati membri dell'Unione per mezzo di criteri disomogenei. Sono stati quindi stabiliti criteri uniformi per consentire un'identificazione più coerente e organica degli operatori pubblici e privati, così da includerli con esattezza in due nuove categorie di attori: i "Soggetti essenziali" e i "Soggetti importanti".

La nuova normativa detta criteri uniformi per identificare i destinatari in modo più coerente e organico.

Il criterio principale è la dimensione del soggetto: la NIS 2 si applica a tutti quei soggetti pubblici o privati ricompresi nelle due tipologie di cui sopra ("Alta criticità" o "Altri settori critici"), che presentino queste caratteristiche:

- prestino i loro servizi o svolgano le loro attività all'interno dell'Unione;
  siano considerati medie imprese (secondo quanto stabilito dall'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE), o superino i massimali per le medie imprese di cui al paragrafo 1 del medesimo articolo.

Un altro criterio di identificazione riguarda le particolari tipologie di soggetti.
Per esempio, rientrano nell'ambito di applicazione della NIS 2:

- i fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico;
- i fornitori di servizi di registrazione dei nomi di dominio; alcuni enti della pubblica amministrazione;
- i soggetti definiti "Critici" dalla Direttiva europea 2022/2557 (nota come Direttiva CER, anch'essa appena pubblicata).

Entro il 17 aprile 2025 gli Stati membri definiranno un elenco puntuale dei soggetti essenziali e importanti, sulla base delle informazioni fornite dagli stessi soggetti interessati.
La Direttiva prevede inoltre che l'elenco venga aggiornato ogni due anni, al fine di garantire un'applicazione corretta e sempre precisa.

Direttiva NIS 2: i principali adempimenti

L'obiettivo della Direttiva – così come della precedente NIS – è chiaro: imporre ai soggetti essenziali e importanti l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate nel cyber risk management, cioè nella gestione dei sistemi informatici e delle reti utilizzate nel corso delle attività aziendali e della fornitura dei servizi. Il fine sono la prevenzione e la riduzione al minimo dell'impatto delle conseguenze di eventuali incidenti informatici. Per raggiungere l'obiettivo, la Direttiva NIS 2 adotta un approccio cosiddetto "multirischio", basato su una metodologia tecnica e organizzativa complessa. Gli elementi sui quali si articola questo approccio sono numerosi. Alcuni di essi coincidono con gli elementi classici del cyber risk assessment come policy di analisi dei rischi e di sicurezza dei sistemi informatici, gestione degli incidenti e business continuity. Altri sono invece più specifici, per esempio:

- la sicurezza della catena di approvvigionamento (che include i rapporti tra ciascun soggetto e i suoi diretti fornitori);
- la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete;
- la gestione e la comunicazione delle vulnerabilità;
- le strategie e le procedure di valutazione della gestione del cyber risk;
- la formazione e l'awareness sulla cybersecurity;
- le policy e le procedure di crittografia e cifratura;
- la sicurezza delle risorse umane;
- la Multifactor Authentication (MFA);
- la protezione di comunicazioni vocali, video, testuali;
- la protezione di comunicazioni di emergenza.

L'obiettivo della NIS 2 è aiutare le organizzazioni pubbliche e private nella miglior gestione possibile del cyber risk.

La Direttiva NIS 2 invita gli Stati membri a prevedere che gli organi di gestione dei soggetti interessati approvino le misure di governance di quanto sopra elencato, poiché possono essere ritenuti responsabili della violazione di eventuali obblighi previsti in fase di recepimento.

Ciò è coerente con la normativa italiana sul Perimetro di Sicurezza Nazionale Cibernetica, che prevede responsabilità personali nei confronti del “Responsabile dell’attuazione del Perimetro”.

I soggetti interessati sono responsabili della violazione di eventuali obblighi previsti nella fase di recepimento delle norme.

Altro punto chiave della NIS 2 è l’obbligo di segnalazione degli incidenti. Previsto anche dalla Direttiva NIS, e poi modificato con un processo che meglio si adatta alla reale gestione di un attacco, prevede obblighi precisi nei termini di comunicazione dell’evento, nella reportistica e nella valutazione della gravita dell’incidente.

Per quanto riguarda infine le sanzioni in caso di violazione delle misure di gestione del cyber risk o degli obblighi di segnalazione, il legislatore europeo ha stabilito quanto segue:

i soggetti essenziali saranno sottoposti a sanzioni pecuniarie amministrative pari a un massimo di 10 milioni di euro (ridotti a 7 milioni per i soggetti importanti) o a un massimo del 2% (ridotto a 1,4% per i soggetti importanti) del totale del fatturato mondiale annuo per l’esercizio precedente, se tale importo è superiore.



Direttiva NIS 2: come prepararsi all’adozione

La pubblicazione della Direttiva NIS 2 va inevitabilmente inserita in un contesto di norme europee che contempla anche il Regolamento DORA e la Direttiva CER.

I ventuno mesi previsti dall'entrata in vigore sono fondamentali per permettere ai soggetti interessati di investire tempo e risorse per prepararsi al recepimento della Direttiva e adeguare i processi aziendali.



Il tema è, in tutta evidenza, quello della valutazione e armonizzazione delle policy interne di sicurezza dei sistemi e delle informazioni, della loro continuità operativa, dei processi di gestione degli incidenti, di procurement e di sicurezza della supply chain.

Non è quindi da escludere che i soggetti interessati debbano ripensare da zero i principali processi interni di cybersecurity, per tararli sui nuovi obiettivi e sui nuovi obblighi soprattutto considerando l'implementazione di un approccio complesso come quello "multirischio" introdotto dal legislatore europeo.

*** L'approccio "multirischio" introdotto dalla NIS 2 obbligherà a ripensare le policy e i processi interni di cybersecurity.**

HWG Sababa

Follow us on:

www.hwgsababa.com