NOTE SULLA NIS2 E SUL SUO RECEPIMENTO ITALIANO

Di Cesare Gallotti

Aggiornato al 3 ottobre 2024

Due parole sulla NIS 2

NIS 2 (Direttiva UE 2022/2055) entrata in vigore il 17 gennaio 2023.

NIS2 è recepita dal 17 ottobre 2024 in Italia con il D. Lgs. 138 del 2024.

Rispetto alla NIS1:

- Aumentano i soggetti.
- Richiede un'analisi dei rischi.
- Le misure dovrebbero essere adeguate al contesto, considerando quindi anche la capacità di spesa.

L'autorità italiana per la NIS2 è ACN.

Nota generale sulla traduzione
Nota generale è che purtroppo il D. Lgs. 138 non ricalca esattamente la Direttiva 2055 e questo crea confusione. Inoltre alcuni termini non coincidono tra il D. Lgs. 138 e la traduzione ufficiale della Direttiva (il D. Lgs. 138 usa "sicurezza informatica" e la Direttiva "cibersicurezza", quando poi altra normativa italiana usa l'orrido "sicurezza cibernetica"; ancora, "asset" è tradotto nel D. Lgs. 138 come "assetti" e nella Direttiva come "attivi", senza poi considerare la traduzione "beni" in uso da parecchi anni).

Scadenze

Un riassunto:

- Entro il 17 gennaio 2025 bisogna valutare se si è soggetto essenziale o importante e registrarsi sulla piattaforma ACN. Entro il 15 aprile, ACN dirà se si è dentro;
- entro il 17 ottobre 2025, bisogna adeguarsi all'articolo 25 (notifica incidenti, stabilendo il processo);
- entro il 1 gennaio 2026, bisogna essere adeguati all'art. 30 (aggiornare le informazioni richieste dalla piattaforma ACN con l'elenco di attività e servizi e la descrizione delle loro caratteristiche);
- entro giugno 2026, bisogna adeguarsi agli articoli 23, 24 (gestione dei rischi e misure di sicurezza) e 29 (banca dati nomi a dominio).

Articolo significativo è questo dal titolo "Recepimento della Direttiva NIS 2: niente panico": https://www.cybersecitalia.it/recepimento-della-direttiva-nis-2-niente-panico/39245/. Qui il calcolo è diverso dal mio e prevedono scadenze poco più lunghe per l'adeguamento agli articoli 25, 23, 24 e 29. Non capisco ancora il perché.

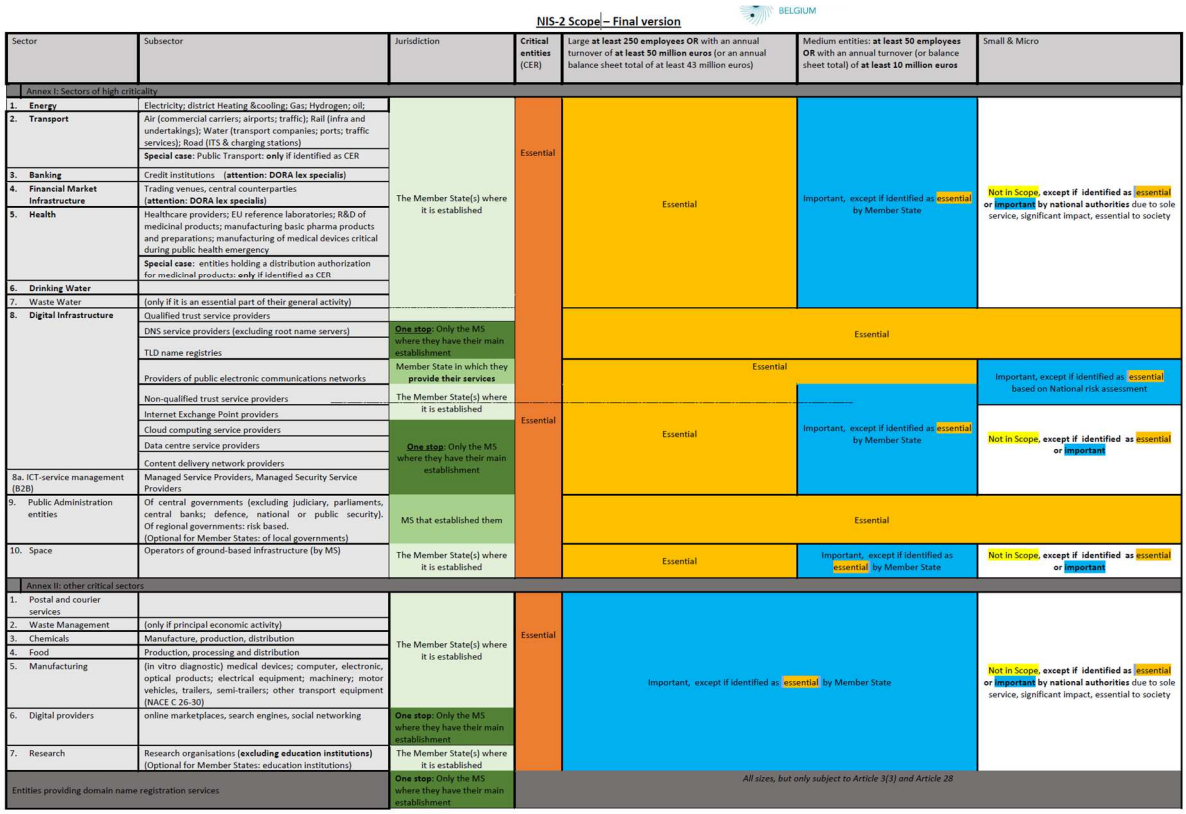
Soggetti a cui si applica la NIS2

L'applicabilità dipende dai settori e dalla dimensione (più di 50 addetti e giro d'affari superiore ai 10 milioni di Euro; escludendo quindi le piccole) dell'organizzazione.

Con la NIS 2 le entità dovranno riconoscersi come soggetti che devono applicare la NIS 2, non è più l'autorità che le designa come tali. E' previsto che le entità si registrino autonomamente presso ACN, poi ACN confermerà o meno l'applicabilità della NIS2 (art. 7).

Sulla base delle registrazioni, entro il 17 aprile 2025, gli Stati membri creano un elenco dei soggetti a cui è applicabile la NIS2.

Lo schema seguente si trova sul sito https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization (mio file "2023-NIS-2 Scope visual.pdf"). Si basa sulla Direttiva, non sul D. Lgs. italiano.



Alcune note sul come stabilire se si rientra nell'applicabilità della NIS 2 (gran parte dei criteri sono all'articolo 3; qui non sono riportati tutti, ma ci sono anche elementi presenti in altri articoli):

- gli allegati I, II, III e IV riportano i settori a cui appartengono le imprese a cui è applicabile la NIS 2; in alcuni casi, le micro e piccole imprese sono escluse;
- gli allegati I e II ricalcano quelli della Direttiva 2055, mentre gli allegati III e IV sono specifici per l'Italia, come previsto dalla Direttiva stessa;
- l'Allegato III riporta le PA incluse e all'articolo 4 ci sono gli enti esclusi;
- l'Allegato IV aggiunge, ai settori già presenti nella Direttiva NIS 2 e quindi negli Allegati I e II, il trasporto pubblico locale, gli istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, società in house, società partecipate e società a controllo pubblico; in questo caso, però, questi soggetti non devono registrarsi autonomamente presso ACN, ma devono ricevere notifica da ACN se a loro è applicabile la NIS 2;
- per alcuni fornitori di servizi informatici sono considerati i casi per cui sono soggetti ad altre giurisdizioni in ambito UE e quindi l'esclusione dall'ambito italiano;
- rientrano nel perimetro di applicazione anche i soggetti definiti "critici" dalla Direttiva (UE) 2022/2557, meglio nota come Direttiva CER, recepita in Italia con D. Lgs. 134 del 2024.

- l'articolo 4 lascia la possibilità alle autorità di identificare altri soggetti a cui è applicabile la NIS 2 e che, per questo, riceveranno notifica da ACN;
- sono presenti considerazioni in merito ai Gruppi di imprese, non presenti nella Direttiva;
- per l'articolo 11, i criteri di applicabilità potranno essere ampliati con DPCM (bisognerà quindi prestare attenzione).

La NIS2, idealmente, dovrebbe includere le aziende già presenti nel PNSC (perimetro nazionale per la sicurezza cibernetica, da DL 105 del 2019).

I soggetti sono quindi suddivisi in (art. 6):

- soggetti essenziali (essential entities);
- soggetti importanti (important entities).

La differenza pratica riguarda i controlli e le sanzioni.

Valutazione del rischio

NIS2, come da articolo 24, è multirischio: logico, fisico, governo, lock in tecnologico, utilities. E considera l'impatto "sociale ed economico" e richiede un "livello appropriato" di sicurezza.

Il Belgio mette a disposizione un approccio piuttosto semplice (ma non capisco bene come funziona): https://ccb.belgium.be/en/choosing-right-cyber-fundamentals-assurance-level-your-organisation.

Interessante la tabella degli impatti, perché forse potrebbe essere riutilizzata per identificare gli incidenti significativi (vedere sotto e all'articolo 25, comma 4 del D. Lgs. 138).

Impact Level HIGH

Description		
The threat is expected to have serious or catastrophic disruptive effects on organisations' network and information systems (economic), organisations' assets (financial), individuals (health, privacy, daily life, well-being), the nation (security and public order) or the functioning of international institutions on Belgian territory. Serious or catastrophic disruptive impact means that the threat has an impact as below:		
Healthcare	Over 200 [1] dead, chronically ill or with long-term disability	• Over 75.000 (3) people with short-term health problems. • Severe environmental pollution affecting our country's natural habitat.
Personal sphere	Loss of personal data of more than 1.000.000 persons (GDPR Art 4.)	Individuals may face significant consequences, which they should be able to overcome, albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, summons, deterioration in health, etc.)
Daily life	Significant Impact on daily life of 75.000 [2] people	
Wellbeing	Impact on welfare (e.g. housing, provision of food and drinking water) for more than 75.000 people	Ecological contamination with long-term effects on more than 75.000 people.
Financial	Financial impact of minimum € 1.500 [3] on 75.000 people.	• Critical damage to organisations' assets. • Critical financial losses in organisations.
Economics	Loss of more than 0.1% of GDP	• Impact on more than 25% of the essential services in the sector. • Severe deterioration or reduction in the ability to perform the organisation's mission such that the organisation cannot perform one or more of its primary functions. • Destruction of essential infrastructure. • Serious threat to economic prosperity.
Security and public order	National impact on the protection of the state and services that ensure security and public order	• Difficulties for the state, and even an inability, to secure a regulatory function or one of its vital missions. • There is serious reputational damage to the state. There is risk of loss of confidence in the state creating fear, uncertainty and doubt. • Protection of the achievements of the democratic rule of law and its shared values is no longer assured. • The physical security of citizens and the physical integrity of our country is no longer assured.
International Institutions	Significant impact on the operation of international institutions on Belgian territory	• International order based on international law and multilateral frameworks is no longer assured. • The effective functioning of the European Union is no longer assured.

Gli Orientamenti della Commissione del 13.9.2023 indicano di considerare le seguenti minacce, sempre in una logica di multirischio:

- sabotaggi,
- furti,
- incendi,
- inondazioni,

- problemi di telecomunicazione,
- problemi di interruzioni di corrente,
- qualsiasi accesso fisico non autorizzato in grado di compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi,
- guasti del sistema,
- errori umani,
- azioni malevole, fenomeni naturali.

Commento

L'auspicio è che, se saranno date indicazioni su come condurre una valutazione del rischio, non venga riproposto il modello formale, ma non utile, basato su asset, minacce e vulnerabilità, ma invece un modello, come poi si vede negli Orientamenti, basato sugli eventi, per cui non è utile avere un dettaglio di tutti gli asset a questo scopo (è invece necessario per attività operative).

Misure di sicurezza

Il D. Lgs. 138 identifica le misure di gestione del rischio (sono presenti alcune piccole aggiunte rispetto alla Direttiva 2055), ossia:

a) *politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;*
b) *gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26;*
c) *continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;*
d) *sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;*
e) *sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;*
f) *politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;*
g) *pratiche di igiene di base e di formazione in materia di sicurezza informatica* (NOTA: L'articolo 23, correttamente, impone agli organi di amministrazione e gli organi direttivi dei soggetti NIS 2 una formazione in materia di sicurezza informatica)*;*
h) *politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura* (NOTA: non chiara la differenza tra crittografia e cifratura, presente anche nella Direttiva tra cryptography e encryption)*;*
i) *sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;*
j) *uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.*

Catena di approvvigionamento

La NIS 2 descrive più approfonditamente le necessità di controllo della catena di approvvigionamento:

i soggetti tengono conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e

fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

Per questo sarà sicuramente necessario migliorare le pratiche di selezione, valutazione e rivalutazione dei fornitori e delle forniture. Purtroppo ritorneranno in voga gli inefficaci e inefficienti questionari, quando invece si dovrà pensare a qualcosa di meglio.

Da monitorare i lavori del Gruppo di cooperazione NIS.

Misure aggiuntive

La Direttiva prevede che entro il 17 ottobre 2024, la Commissione adotti atti di esecuzione che stabiliscono i requisiti tecnici e metodologici delle misure di cui sopra per quanto riguarda i fornitori di:

- servizi DNS,
- registri dei nomi di dominio di primo livello (TLD),
- servizi di cloud computing,
- servizi di data center,
- reti di distribuzione dei contenuti,
- servizi gestiti,
- servizi di sicurezza gestiti,
- mercati online,
- motori di ricerca online,
- piattaforme di servizi di social network,
- prestatori di servizi fiduciari.

Per quanto riguarda il D. Lgs. 138 italiano, gli articoli 30, 31 e 32 dicono che ACN potrebbe richiedere l'applicazione di "misure minime", qui chiamate "obblighi".

L'articolo 28 dice che ACN "promuove l'uso di specifiche tecniche europee e internazionali". Si può quindi sperare nella promozione di standard ISO, EN ed ETSI e non di altri (incluso il NIST CSF e il Framework nazionale per la cybersecurity e la data protection, anche se attualmente richiesti da ACN ai soggetti a cui si applica la NIS1). Si può sperare addirittura nella partecipazione di ACN alle attività di standardizzazione.

Le misure di sicurezza sono trattate anche in altri articoli. Eccone alcuni:

- l'articolo 27 prevede che ACN possa imporre l'uso di prodotti certificati;
- l'articolo 29 è specifico per chi si occupa dei nomi di dominio, ma non presenta misure di sicurezza vere e proprie;
- gli articoli 35 e 36 dicono che ACN può imporre VA-PT o audit da parte di soggetti selezionati;

Attenzione che le misure vanno applicate a tutte le attività operative operazioni e a tutti i servizi del soggetto interessato, non solo a risorse informatiche specifiche o a servizi critici forniti dal soggetto. Mia interpretazione: per evitare che un soggetto con servizi “sicuri” e “non sicuri” possa essere violato sfruttando le carenze dei servizi “non sicuri” per poi, con movimenti laterali, compromettere anche quelli “sicuri”.

Come esclusione, invece, l'art. 33 dice che, se un'impresa è nel PSNC (perimetro di sicurezza nazionale cibernetica, da DL 105 del 2019), non è tenuta ad applicare le misure previste in ambito NIS 2. Lo trovo un approccio criticabile perché dà maggiore importanza a una "invenzione italiana" rispetto a una omogeneità europea.

Gestione incidenti

Come già previsto dalla Direttiva NIS 1, anche NIS 2 prevede l'obbligo di notifica al CSIRT e alle autorità competenti (oltre che ai destinatari stessi del servizio) degli incidenti significativi (incidenti informatici capaci di impattare in modo significativo sulla fornitura del servizio).

Notifica

Le comunicazioni al CSIRT dovranno avvenire:

- Entro 24 ore dalla conoscenza dell'incidente con una notifica di preallarme (questo per attenuare la potenziale diffusione di incidenti e per consentire di chiedere assistenza);
    - deve riportare i dati strettamente necessari se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o se potrebbe avere (ossia se è probabile che abbia) un impatto transfrontaliero;
    - deve contenere una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione.
- Entro 72 ore dalla conoscenza dell'incidente con aggiornamenti rispetto alle informazioni fornite con il preallarme
- Entro 1 mese dalla conoscenza dell'incidente con una relazione finale a completamento del processo di segnalazione (questo per poter trarre insegnamenti preziosi dai singoli incidenti);
    - la relazione deve essere comprensiva della sua gravità e del suo impatto, il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente, le misure di mitigazione adottate e in corso e, se opportuno, l'impatto transfrontaliero dell'incidente.
- Se l'incidente non è ancora risolto, la normativa fornisce indicazioni su come procedere.
- Sono indicate eccezioni per i prestatori di servizi fiduciari, oltre che, all'articolo 33, per chi è compreso nel PNSC.

L'articolo 23 richiede che gli organi di amministrazione e gli organi direttivi dei soggetti NIS 2 vengano avvisati tempestivamente degli incidenti.

Alcuni soggetti sono soggetti a più normative e quindi a diverse modalità di notificazione degli incidenti. In alcuni casi, il recepimento può essere complesso.

E' prevista la possibilità di chiedere assistenza al CSIRT, che dovrà rispondere "fermo restando quanto previsto dall'articolo 15, comma 4", secondo quanto previsto dal D. Lgs. 138 (potrebbe essere tradotto con "se non avrà cose più importanti da fare"). A parte la mia ironia, è sicuramente positivo il coinvolgimento delle competenze del CSIRT.

Il D. Lgs. 138 dà indicazioni anche per le comunicazioni ad altri soggetti potenzialmente impattati dall'incidente. È previsto che prima venga "sentito il CSIRT Italia", introducendo un potenziale collo di bottiglia.

Incidenti significativi e quasi incidenti

Nel D. Lgs. 138, articolo 24, paragrafo 3, c'è la definizione di "incidente significativo": se ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato o se ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

E' possibile definire meglio questi criteri.

Definiti anche i «quasi incidenti» (in inglese "near-miss"): *un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato.*

Notare che la definizione della Direttiva è diversa: *Un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato.*

La NIS2 istituisce la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe).

Comunicazione delle vulnerabilità

All'articolo 16 è detto che lo CSIRT diffonde notizie in merito alle vulnerabilità e che tutti possono segnalarne.

L'articolo 17 dà la possibilità di scambiarsi, su base volontaria, pertinenti informazioni sulla sicurezza informatica.

Non è chiarito se è possibile la partecipazione anche ai soggetti a cui non si applica la NIS 2.

Altri argomenti

La NIS2 prevede ulteriori argomenti:

- Cooperazione tra Stati membri
- Sanzioni
- Punti di contatto nazionali
- Ruolo dell'ENISA

Questi però non rientrano nelle mie competenze e non li ho approfonditi.

Bibliografia

Sito web del Center for cyber security Belgium: https://ccb.belgium.be/en/choosing-right-cyber-fundamentals-assurance-level-your-organisation. Grazie ad Alessandro Cosenza per la segnalazione.

Presentazione "Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union ("NIS2 directive")".

Sito web della UE: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new. Però non fornisce indicazioni che io ritengo utili.

Criteri interpretativi sulla NIS2 della Commissione: https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive. Grazie a Pierluigi Perri.

Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (2003/361/CE). Grazie a Giancarlo Caroti.