NOTE SULLA NIS2

Di Cesare Gallotti

Due parole sulla NIS 2

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

NIS2 dovrà essere recepita entro ottobre 2024.

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

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. La NIS2 è applicabile quindi a:

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

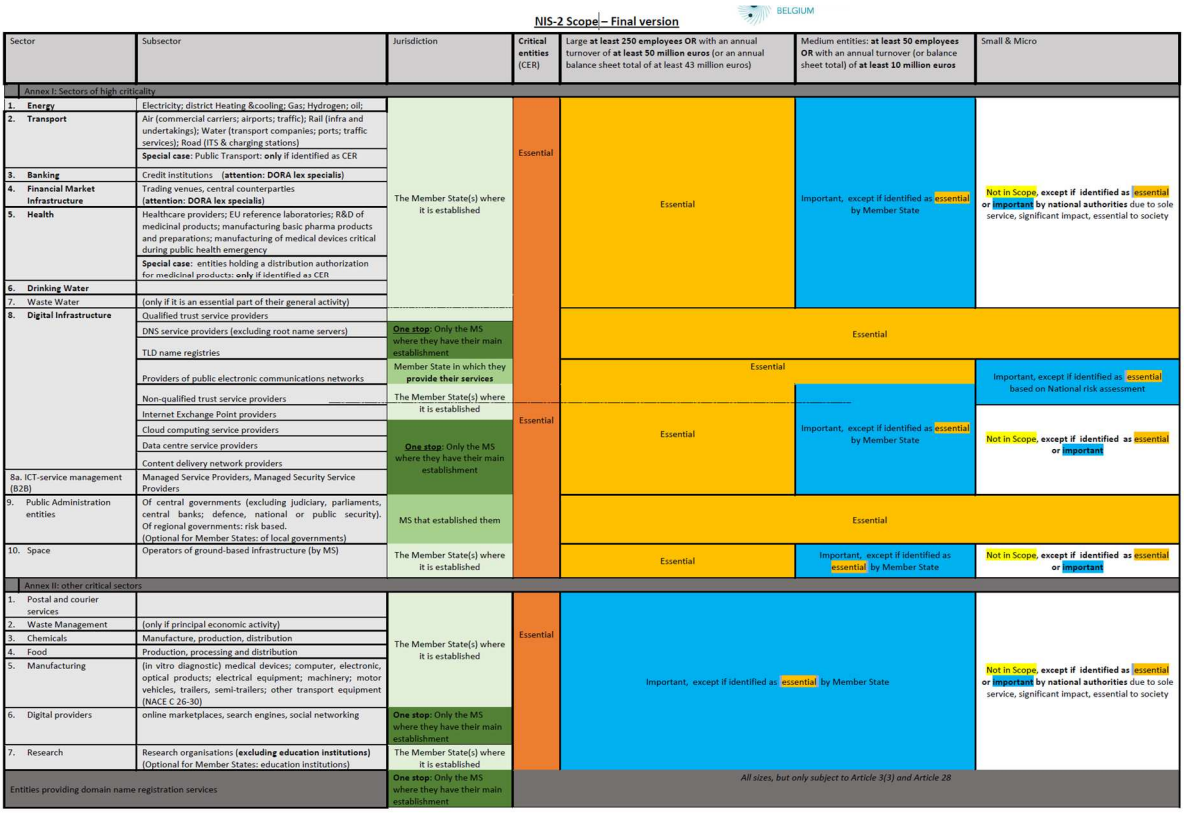
La differenza pratica riguarda i controlli e le sanzioni.

La NIS2 coinvolge più aziende rispetto al PNCS.

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 secondo regole che saranno fornite.

Sulla base delle registrazioni, entro il 17 aprile 2025, gli Stati membri creano un elenco dei soggetti essenziali e importanti e dei soggetti che forniscono servizi di registrazione dei nomi di dominio.

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").



NIS-2 Scope – Final version

BELGIUM

Sector	Subsector	Jurisdiction	Critical entities (CER)	Large **at least 250 employees OR** with an annual turnover of **at least 50 million euros** (or an annual balance sheet total of at least 43 million euros)	Medium entities: **at least 50 employees OR** with an annual turnover (or balance sheet total) of **at least 10 million euros**	Small & Micro
Annex I: Sectors of high criticality						
1. **Energy**	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important **by national authorities** due to sole service, significant impact, essential to society
2. **Transport**	Air (commercial carriers; airports; traffic); Rail (infra and undertakings); Water (transport companies; ports; traffic services); Road (ITS & charging stations)					
	Special case: Public Transport: **only** if identified as CER					
3. **Banking**	Credit institutions (**attention: DORA lex specialis**)					
4. **Financial Market Infrastructure**	Trading venues; central counterparties (**attention: DORA lex specialis**)					
5. **Health**	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. **Drinking Water**						
7. Waste Water	(only if it is an essential part of their general activity)					
8. **Digital Infrastructure**	Qualified trust service providers					
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment		Essential		
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they **provide their services**		Essential		Important, except if identified as essential based on National risk assessment
	Non-qualified trust service providers	The Member State(s) where it is established			Important, except if identified as essential by Member State	
	Internet Exchange Point providers		Essential	Essential		Not in Scope, **except if identified as** essential **or** important
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management (B2B)	Managed Service Providers, Managed Security Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security). Of regional governments: risk based. (Optional for Member States: of local governments)	MS that established them		Essential		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, **except if identified as** essential **or** important **by national authorities** due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have their main establishment				
7. Research	Research organisations (**excluding education institutions**) (Optional for Member States: education institutions)	The Member State(s) where it is established				
Entities providing domain name registration services		**One stop**: Only the MS where they have their main establishment	*All sizes, but only subject to Article 3(3) and Article 28*			

Rientreranno nel perimetro di applicazione anche i soggetti definiti “critici” dalla Direttiva (UE) 2022/2557, meglio nota come Direttiva CER.

Ulteriori soggetti potrebbero essere aggiunti dalla normativa nazionale.

Valutazione del rischio

NIS2 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).

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

La Direttiva identifica (articolo 21 paragrafo 2) le misure di gestione del rischio, ossia:

1. Politiche di analisi dei rischi e della sicurezza dei sistemi informatici
2. Sistemi di gestione degli incidenti
3. Soluzioni di business continuity capaci di garantire la continuità operativa e la gestione della crisi, dai backup al disaster recovery

4. Misure di sicurezza dell'intera supply chain, a comprendere perciò i rapporti tra ogni soggetto e i suoi fornitori
5. Sicurezza dell'acquisizione, sviluppo e manutenzione dei sistemi e delle reti informatiche, compresa la gestione e la divulgazione delle vulnerabilità
6. Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersecurity
7. Pratiche di igiene informatica basilari e formazione in materia di sicurezza informatica
8. Procedure relativa all'uso della crittografia e, se necessario, della cifratura
9. Misure per la sicurezza delle risorse umane grazie a strategie e politiche di controllo degli accessi (log management) e gestione degli asset
10. 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 all'interno dell'entità, ove opportuno.

Perri dice che c'è un indice sulla valutazione delle competenze, ma io non l'ho trovato (o forse ho capito male); forse nelle interpretazioni.

Entro il 17 ottobre 2024, la Commissione adotta 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.

Alcuni prevedono che siano quindi da applicare:

- requisiti specifici settoriali stabiliti dalla Commissione (o, in alternativa, requisiti raccomandati da ENISA o dalle autorità nazionali);
- requisiti di base comuni (o, in alternativa, certificazione ISO/IEC 27001).

Il Belgio (come l'Italia) propone elenchi di misure basati sul NIST CSF: https://ccb.belgium.be/en/cyberfundamentals-framework.

Allo stato attuale (13 marzo 2024) non sono state stabilite le misure da adottare. In Italia sappiamo che adesso, per i soggetti sotto NIS, sono richieste quelle del Framework Nazionale per la Cybersecurity e la Data Protection (https://www.cybersecurityframework.it/framework2) e così in altri Paesi. Forse con la NIS 2 seguiranno altri schemi.

Attenzione che le misure stabilite dagli Stati membri e di cui all'articolo 21 paragrafo 1 della NIS2 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".

Commento

Personalmente spero sia adottata la ISO/IEC 27001. Potrebbero anche lasciare più scelte ai soggetti. Infatti delegati italiani potrebbero partecipare agli aggiornamenti e alle estensioni della ISO/IEC 27001, e non subire passivamente gli aggiornamenti del NIST.

In tutti i casi, raccomando di cominciare a implementare la ISO/IEC 27001, su cui, eventualmente, innestare le richieste specifiche che saranno fatte. Un'implementazione ISO/IEC 27001 può essere facilmente convertibile per NIST CSF o altri.

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).

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.

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

Obbligatorietà:

- Articolo 23, stabilisce quando è obbligatorio notificare;
- Articolo 30, indica quando la notifica è volontaria (altri incidenti, minacce, quasi incidenti, anche da parte degli altri soggetti).

Nella NIS2 c'è la definizione di "incidente significativo" nell'articolo 23, paragrafo 3: se ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato o se si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Vanno quindi definiti meglio e forse la tabella degli impatti usata per valutare il rischio.

Definiti anche i «quasi incidenti». 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).

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.