NIS2: i 13 pilastri dell’implementazione tecnica



La direttiva europea Network and Information Security 2 (NIS2) rappresenta una pietra miliare nell’evoluzione del panorama normativo della cybersecurity europea, introducendo requisiti tecnici e metodologici significativamente più stringenti rispetto al predecessore NIS. L’implementazione di questa direttiva richiede un approccio strutturato e metodico che tenga conto delle specificità operative di ciascuna organizzazione, rappresentando al contempo una sfida e un’opportunità per elevare il livello complessivo di sicurezza informatica.

Il framework normativo di riferimento

La Commissione Europea ha pubblicato il regolamento di attuazione (UE) 2024/2690 del 17 ottobre 2024, che stabilisce i requisiti tecnici e metodologici per le misure di gestione del rischio di cybersecurity previste dall’articolo 21(2) della direttiva (UE) 2022/2555. Questo regolamento si applica a entità essenziali e importanti operanti in settori critici quali infrastrutture digitali, energia, trasporti e sanità.

La pubblicazione della guida tecnica ENISA nel giugno 2025 segna un momento cruciale per l’ecosistema europeo della cybersecurity. Questa tempistica, che precede di pochi mesi le scadenze implementative più stringenti, evidenzia la volontà delle istituzioni europee di fornire un supporto concreto alle organizzazioni nell’interpretazione e applicazione dei requisiti normativi.

Entità soggette alla normativa

Il perimetro di applicazione comprende:

- Fornitori di servizi del sistema dei nomi di dominio (DNS);
- Registri di domini di primo livello;
- Fornitori di servizi di cloud computing;
- Fornitori di servizi di data center;
- Fornitori di reti di distribuzione dei contenuti;
- Fornitori di servizi gestiti e di sicurezza gestiti;
- Fornitori di piattaforme di marketplace online, motori di ricerca e social network;
- Fornitori di servizi fiduciari.

La scelta di concentrare l'armonizzazione europea su questi specifici settori riflette una comprensione matura dell'interconnessione digitale moderna. Tuttavia, l'esclusione di altri settori critici dall'armonizzazione europea potrebbe creare disparità normative significative tra Stati membri, con potenziali implicazioni per la competitività e la sicurezza dell'ecosistema digitale nel suo complesso.

I 13 pilastri dell'implementazione tecnica

L'ENISA ha strutturato la guida implementativa attorno a tredici requisiti tecnici e metodologici fondamentali, che rappresentano un framework integrato di cybersecurity enterprise-grade. Questi pilastri costituiscono l'architettura portante per la conformità NIS2 e richiedono un'implementazione coordinata e sinergica.

1. Politica sulla sicurezza dei sistemi di rete e informativi

La politica deve definire l'approccio dell'entità alla gestione della sicurezza, essere complementare agli obiettivi

strategici aziendali e includere un impegno al miglioramento continuo. Elementi essenziali includono:

- Approvazione formale da parte degli organi di gestione;
- Comunicazione sistematica a tutto il personale pertinente e parti esterne interessate;
- Definizione di ruoli e responsabilità secondo quanto previsto dal punto 1.2 dell'Allegato al Regolamento (UE) 2024/2690;
- Elenco della documentazione da conservare e durata di conservazione;
- Indicatori e misure per monitorare l'implementazione e il livello di maturità.

Questo primo pilastro sottolinea l'importanza della governance di alto livello. La richiesta di approvazione formale da parte degli organi di gestione non è meramente procedurale ma rappresenta un cambio paradigmatico verso la cybersecurity governance, ponendo la responsabilità strategica direttamente sul top management.

2. Politica di gestione del rischi

L'implementazione richiede l'adozione di metodologie strutturate per l'identificazione, analisi e valutazione dei rischi. Il framework deve integrare:

- Approccio all-hazards considerando minacce cyber, naturali e antropiche;
- Metodologia di gestione del rischio strutturata;
- Livelli di tolleranza e criteri di accettazione del rischio;
- Identificazione dei punti critici di fallimento (single point of failure);
- Monitoraggio continuo dell'implementazione delle misure di trattamento;
- Revisioni indipendenti della sicurezza delle informazioni e della rete.

L’approccio all-hazards rappresenta un’evoluzione significativa nella gestione del rischio informatico, riconoscendo l’interconnessione tra rischi fisici, ambientali e digitali. Questa visione olistica riflette le lezioni apprese da eventi recenti quali la pandemia COVID-19 e i conflitti geopolitici, dove le disruptions fisiche hanno avuto impatti digitali significativi.

3. Gestione degli incidenti

Il processo di incident handling deve comprendere un ecosistema integrato di capacità:

3.1 Politica di gestione degli incidenti

- Sistema di categorizzazione coerente con la valutazione e classificazione degli eventi;
- Piani di comunicazione efficaci inclusi escalation e reporting;
- Assegnazione di ruoli per rilevamento e risposta appropriata;
- Documentazione operativa inclusi manuali, grafici di escalation e modelli.

3.2 Monitoraggio e logging

- Procedure e strumenti per monitoraggio e registrazione delle attività;
- Automazione per minimizzare falsi positivi e negativi;
- Sincronizzazione temporale tra tutti i sistemi per correlazione;
- Protezione dell’integrità dei log da accessi non autorizzati.

3.3 Meccanismi di segnalazione degli eventi

- Canali semplificati per dipendenti, fornitori e clienti;
- Formazione regolare sull’utilizzo dei meccanismi;
- Comunicazione del meccanismo a fornitori e clienti.

3.4 Valutazione e classificazione degli eventi

- Criteri predefiniti per determinare se eventi sospetti costituiscono incidenti;
- Processo di triage per prioritizzazione;
- Analisi di correlazione dei log;
- Riclassificazione basata su nuove informazioni.

3.5 Risposta agli incidenti

- Procedure documentate per contenimento, eradicazione e recupero;
- Piani di comunicazione con CSIRT e autorità competenti;
- Registrazione delle attività di risposta e raccolta delle evidenze;
- Test periodici delle procedure.

3.6 Revisioni post-incidente

- Analisi delle cause principali quando possibile;
- Lezioni apprese documentate per ridurre occorrenze future;
- Miglioramento continuo dell’approccio alla sicurezza.

4. Continuità operativa e gestione delle crisi

La business continuity richiede un approccio strutturato su quattro componenti fondamentali:

4.1 Piano di continuità operativa e disaster recovery

- Piani basati sui risultati della valutazione del rischio,
- Ordine di recupero per le operazioni;
- Obiettivi di recupero specifici per operazioni;
- Risorse richieste inclusi backup e ridondanze.

4.2 Gestione di backup e ridondanza

- Copie di backup complete e accurate;
- Ubicazioni sicure per conservazione;

- Controlli di accesso appropriati;
- Tempi di recupero che non superino gli obiettivi definiti;
- Verifiche di integrità regolari.

4.3 Gestione delle crisi

- Processi per gestione delle situazioni di crisi;
- Criteri di attivazione per dichiarazione di crisi;
- Mezzi di comunicazione appropriati con autorità competenti;
- Misure per mantenimento della sicurezza durante le crisi.

L'introduzione del concetto di Service Delivery Objective (SDO) accanto ai tradizionali RTO e RPO rappresenta un affinamento significativo nella pianificazione della continuità operativa. Questo riconosce che la resilienza moderna non riguarda solo il "quando" (RTO) e il "quanto" (RPO) del recupero, ma anche il "come" – ovvero il livello di servizio durante le fasi di degradazione operativa.

5. Sicurezza della catena di fornitura

L'approccio alla supply chain security deve includere:

5.1 Politica di sicurezza della catena di fornitura

- Criteri di selezione per fornitori e prestatori di servizi;
- Requisiti contrattuali inclusi accordi di livello di servizio;
- Identificazione del ruolo nella catena di fornitura;
- Monitoraggio e valutazione continui.

5.2 Registro di fornitori e prestatori di servizi

- Registro aggiornato di fornitori diretti;
- Punti di contatto per ciascun fornitore;
- Elenco di prodotti, servizi e processi ICT forniti.

I requisiti di sicurezza della catena di fornitura acquisiscono particolare rilevanza nel contesto geopolitico attuale. La richiesta di valutare la “giurisdizione legale” dei fornitori e la considerazione delle “valutazioni nazionali delle minacce” riflette una crescente consapevolezza delle implicazioni di sicurezza nazionale nella digitalizzazione.

6. Sicurezza nell’acquisizione, sviluppo e manutenzione

Questo pilastro comprende dieci sotto-componenti che coprono l’intero ciclo di vita dei sistemi:

6.1 Sicurezza nell’acquisizione di servizi o prodotti ICT

- Processi per gestione dei rischi da acquisizione;
- Requisiti di sicurezza per servizi/prodotti da acquisire;
- Informazioni sui componenti hardware e software;
- Metodi di validazione per conformità ai requisiti.

6.2 Ciclo di vita sicuro dello sviluppo

- Regole per sviluppo sicuro covering tutte le fasi;
- Analisi dei requisiti di sicurezza;
- Principi di cybersecurity-by-design;
- Processi di security testing.

6.3 Gestione della configurazione

- Configurazioni documentate per hardware, software, servizi e reti;
- Processi automatizzati per applicazione e verifica;
- Controllo delle modifiche con procedure di approvazione.

6.4 Change management, riparazioni e manutenzione

- Procedure di controllo per modifiche ai sistemi;
- Test e valutazione dell’impatto prima dell’implementazione;

- Documentazione dei risultati e spiegazioni per emergenze.

6.5 Security testing

- Politica e procedure per test di sicurezza;
- Metodologie documentate per test;
- Documentazione dei risultati con azioni di mitigazione.

6.6 Gestione delle patch di sicurezza

- Procedure per applicazione tempestiva delle patch;
- Test prima dell'applicazione in sistemi di produzione;
- Verifica dell'integrità delle patch da fonti fidate;
- Misure aggiuntive quando patch non disponibili.

6.7 Sicurezza di rete

- Architettura di rete documentata e aggiornata;
- Controlli per protezione da accessi non autorizzati;
- Configurazioni per prevenire comunicazioni non necessarie;
- Controlli per accesso remoto.

6.8 Segmentazione di rete

- Segmentazione basata sui risultati della valutazione del rischio;
- Zone demilitarizzate per comunicazioni sicure;
- Separazione delle reti amministrative da quelle operative;
- Controlli di accesso tra zone diverse.

6.9 Protezione contro software malevolo e non autorizzato

- Misure di rilevamento e prevenzione;
- Software di rilevamento e risposta aggiornato regolarmente;
- Configurazioni per scansioni periodiche e in tempo reale.

6.10 Gestione e divulgazione delle vulnerabilità

- Monitoraggio delle informazioni sulle vulnerabilità;
- Scansioni periodiche e registrazione dei risultati;
- Gestione tempestiva delle vulnerabilità critiche;
- Procedure di divulgazione coordinate,

L'integrazione obbligatoria del SSDLC rappresenta probabilmente la sfida implementativa più significativa per molte organizzazioni, particolarmente quelle con pratiche di sviluppo legacy. Tuttavia, l'investimento iniziale può tradursi in benefici economici sostanziali attraverso la riduzione dei costi di rimediazione post-deployment.

7. Politiche e procedure per valutare l'efficacia delle misure

Questo pilastro richiede:

- Politica per valutazione dell'efficacia dell'implementazione;
- Determinazione delle misure da monitorare e misurare;
- Metodi per monitoraggio e valutazione;
- Tempistiche per analisi e valutazione dei risultati;
- Responsabilità per monitoraggio e analisi.

8. Pratiche di igiene informatica e formazione sulla sicurezza

8.1 Sensibilizzazione e pratiche di igiene informatica

- Programmi di sensibilizzazione per tutti i dipendenti;
- Copertura delle misure di gestione del rischio;
- Pratiche di igiene informatica per utenti;
- Test di efficacia e aggiornamenti periodici.

8.2 Formazione sulla sicurezza

- Identificazione di dipendenti con competenze di sicurezza;

- Programmi di formazione in linea con le politiche;
- Formazione specifica per ruolo e funzione;
- Valutazione dell’efficacia della formazione.

9. Crittografia

La politica crittografica deve stabilire:

- Tipo, forza e qualità delle misure crittografiche;
- Protocolli e algoritmi approvati;
- Approccio alla gestione delle chiavi crittografiche;
- Revisioni periodiche considerando lo stato dell’arte.

L’enfasi sull’approccio crypto-agile anticipa la transizione post-quantistica, riconoscendo che le organizzazioni devono prepararsi oggi per le minacce crittografiche di domani. Questa lungimiranza normativa è particolarmente apprezzabile considerando i tempi di sviluppo tipici dei sistemi enterprise.

10. Sicurezza delle risorse umane

10.1 Sicurezza delle risorse umane

- Responsabilità di sicurezza per dipendenti e fornitori;
- Meccanismi per igiene informatica;
- Consapevolezza per utenti con accesso privilegiato;
- Procedure di assunzione qualificate.

10.2 Verifica dei precedenti

- Criteri per ruoli che richiedono verifica;
- Processo di verifica prima dell’inizio delle responsabilità;
- Considerazioni per leggi e requisiti aziendali.

10.3 Procedure di terminazione o cambio di impiego

- Responsabilità definite contrattualmente;
- Clausole di riservatezza e doveri post-impiego;
- Revoca tempestiva degli accessi.

10.4 Processo disciplinare

- Processo per gestione delle violazioni delle politiche;
- Considerazioni legali e requisiti aziendali;
- Comunicazione e mantenimento del processo.

11. Controllo degli accessi

11.1 Politica di controllo degli accessi

- Politiche documentate per controllo logico e fisico;
- Accesso per persone inclusi personale e visitatori;
- Accesso per processi dei sistemi informatici;
- Autenticazione adeguata degli utenti;

11.2 Gestione dei diritti di accesso

- Principi di need-to-know e privilegio minimo;
- Autorizzazione da persone pertinenti;
- Registro dei diritti di accesso concessi;
- Registrazione della gestione dei diritti.

11.3 Account privilegiati e di amministrazione sistema

- Politiche per gestione di account privilegiati;
- Autenticazione forte inclusa multi-fattore;
- Account specifici per operazioni di amministrazione;
- Individualizzazione dei privilegi.

11.4 Sistemi di amministrazione

- Restrizione e controllo dell’uso;
- Uso esclusivo per scopi amministrativi;
- Separazione logica da altri software;
- Protezione dell’accesso tramite autenticazione e crittografia.

11.5 Identificazione

- Gestione del ciclo di vita delle identità;
- Identità univoche per sistemi e utenti;

- Collegamento dell’identità utente a singola persona;
- Registrazione della gestione delle identità.

11.6 Autenticazione

- Procedure e tecnologie di autenticazione sicura;
- Forza appropriata alla classificazione dell’asset;
- Gestione delle informazioni di autenticazione segrete;
- Metodi all’avanguardia quando fattibile.

11.7 Autenticazione multi-fattore

- Fattori multipli o meccanismi di autenticazione continua;
- Forza appropriata alla classificazione dell’asset;
- Implementazione basata sui requisiti di accesso.

12. Gestione degli asset

12.1 Classificazione degli asset

- Livelli di classificazione per tutti gli asset;
- Sistema di livelli di classificazione;
- Associazione di tutti gli asset con livelli;
- Revisioni periodiche delle classificazioni.

12.2 Gestione degli asset

- Politica per gestione appropriata degli asset;
- Copertura del ciclo di vita completo;
- Istruzioni per uso, conservazione e trasporto sicuri;
- Trasferimento sicuro secondo il tipo di asset.

12.3 Politica sui supporti rimovibili

- Politica sulla gestione dei supporti di memorizzazione rimovibili;
- Proibizione tecnica della connessione senza motivo organizzativo;
- Disabilitazione dell’auto-esecuzione e scansione per codice malevolo;

- Misure per controllo e protezione dei dispositivi.

12.4 Inventario degli asset

- Inventario completo e accurato;
- Granularità appropriata alle esigenze dell’entità;
- Elenco delle operazioni e servizi;
- Aggiornamenti regolari e documentazione delle modifiche.

12.5 Deposito, restituzione o cancellazione degli asset

- Procedure per garanzia del deposito, restituzione o cancellazione;
- Documentazione del processo;
- Misure alternative quando non possibile la restituzione.

13. Sicurezza ambientale e fisica

13.1 Servizi di supporto

- Prevenzione di perdite dovute a guasti dei servizi di supporto;
- Protezione da interruzioni di corrente e altre disruptions;
- Ridondanza nei servizi di pubblica utilità;
- Monitoraggio dei servizi di pubblica utilità.

13.2 Protezione contro minacce fisiche e ambientali

- Prevenzione o riduzione delle conseguenze di eventi fisici e ambientali;
- Misure di protezione contro minacce fisiche e ambientali;
- Soglie di controllo minime e massime;
- Monitoraggio dei parametri ambientali.

13.3 Controllo del perimetro e degli accessi fisici

- Prevenzione e monitoraggio dell’accesso fisico non autorizzato;
- Perimetri di sicurezza per protezione delle aree;

- Controlli di ingresso e punti di accesso appropriati;
- Monitoraggio continuo per accesso fisico non autorizzato.

I requisiti di segmentazione di rete riflettono l'evoluzione dalle architetture di sicurezza perimetrali verso modelli zero-trust. Questa transizione, sebbene tecnicamente complessa, è essenziale per la resilienza contro le minacce avanzate che caratterizzano il panorama contemporaneo.

Sfide implementative e considerazioni operative

Gestione del software open source

La direttiva NIS2 riconosce le specificità del software libero e open source (FOSS), richiedendo alle organizzazioni di:

- Valutare i rischi associati alle dipendenze open source;
- Supportare le comunità di sviluppo quando tecnicamente ed economicamente fattibile;
- Implementare processi di vulnerability management specifici per i componenti FOSS.

Il riconoscimento esplicito del ruolo del FOSS nella sicurezza informatica rappresenta un approccio pragmatico e lungimirante. Tuttavia, la richiesta di "supportare le comunità" potrebbe creare disparità competitive tra organizzazioni di diverse dimensioni e capacità finanziarie.

Approccio scalabile per diverse dimensioni organizzative

L'implementazione deve essere proporzionata alle dimensioni e alla complessità dell'organizzazione. Le entità di dimensioni ridotte possono adottare processi meno complessi mantenendo l'efficacia dei controlli di sicurezza.

Mentre la flessibilità per le organizzazioni più piccole è

apprezzabile, rimane la sfida di mantenere un livello di sicurezza efficace senza compromettere l'integrità del framework complessivo. La definizione di "proporzionalità" richiederà ulteriori chiarimenti implementativi.

Implicazioni economiche e competitive

Costi di implementazione

L'implementazione completa dei 13 pilastri NIS2 comporta investimenti significativi in:

- Tecnologie di sicurezza e monitoraggio;
- Formazione e sviluppo delle competenze;
- Processi e governance;
- Consulenza specializzata.

Sebbene i costi iniziali siano sostanziali, la ricerca indica che ogni euro investito in cybersecurity preventiva può generare risparmi di 3-5 euro in costi di rimediazione post-incidente. La NIS2, pertanto, può essere vista come un investimento strategico piuttosto che un mero costo di conformità.

Competitività del mercato europeo

La standardizzazione dei requisiti di sicurezza può:

- Livellare il campo competitivo tra Stati membri;
- Aumentare la fiducia dei consumatori nei servizi digitali europei;
- Migliorare la posizione competitiva dell'Europa nel mercato globale digitale.

Considerazioni di implementazione pratica

Timeline e prioritizzazione

Le organizzazioni dovrebbero adottare un approccio phased:

Fase 1 (Immediata): *Governance* e *policy foundation*

- Sviluppo delle politiche di sicurezza (Pilastri 1, 2);
- Identificazione degli asset critici (Pilastro 12);
- Baseline risk assessment (Pilastro 2);

Fase 2 (6-12 mesi): Controlli tecnici fondamentali

- Implementazione MFA e controlli di accesso (Pilastro 11);
- Sistemi di monitoraggio e logging (Pilastro 3);
- Incident response procedures (Pilastro 3).

Fase 3 (12-24 mesi): Maturità avanzata

- SSDLC completo (Pilastro 6);
- Automazione della conformità (Pilastro 7);
- Programmi di miglioramento continuo (tutti i pilastri).

Integrazione con altri framework

L'approccio più efficiente consiste nell'integrare NIS2 con:

- ISO 27001: per la gestione sistematica della sicurezza dell'informazione;
- NIST Cybersecurity Framework: per l'implementazione operativa;
- Framework nazionali: per la conformità locale.

Le organizzazioni che hanno già implementato ISO 27001 si trovano in una posizione vantaggiosa, potendo leveraggiare strutture di governance esistenti per accelerare la conformità NIS2.

Monitoraggio e misurazione dell'efficacia

Key Performance Indicators (KPI)

Le organizzazioni dovrebbero sviluppare metriche che includano:

- Indicatori di resilienza: Mean Time to Detection (MTTD),

Mean Time to Response (MTTR);
- Indicatori di conformità: percentuale di asset inventariati, copertura dei controlli di sicurezza;
- Indicatori di maturità: livello di automazione dei processi, efficacia della formazione.

Benchmarking settoriale

L'ENISA sta sviluppando meccanismi per il benchmarking anonimo tra organizzazioni dello stesso settore, permettendo:

- Valutazione relativa della postura di sicurezza;
- Identificazione di best practice settoriali;
- Ottimizzazione degli investimenti in sicurezza.

Prospettive future e evoluzioni normative

Evoluzione tecnologica

La guida ENISA è progettata come "documento vivente", con revisioni periodiche per incorporare:

- Minacce emergenti;
- Nuove tecnologie (AI, quantum computing, IoT);
- Evoluzione delle best practice settoriali.

Armonizzazione internazionale

L'approccio NIS2 influenzerà probabilmente:

- Standard ISO/IEC in sviluppo;
- Regolamentazioni di cybersecurity in altre giurisdizioni;
- Accordi internazionali di cooperazione nella cybersecurity.

L'Europa si sta posizionando come leader globale nella standardizzazione della cybersecurity, con potenziali benefici per l'export di soluzioni e servizi di sicurezza europei.

Conclusioni e raccomandazioni

L’implementazione della direttiva NIS2 rappresenta una trasformazione fondamentale nel panorama della cybersecurity europea. I 13 pilastri tecnici non costituiscono semplicemente una checklist di conformità, ma piuttosto un framework integrato per la cyber-resilienza enterprise.

Raccomandazioni per i CISO

1. **Approccio olistico**: Non trattare NIS2 come un progetto isolato, ma come catalizzatore per la trasformazione digitale sicura dell’organizzazione;
2. **Investimento in competenze**: Prioritizzare lo sviluppo delle competenze interne, particolarmente in aree critiche come threat intelligence, incident response e security architecture;
3. **Automazione intelligente**: Leverage dell’automazione non solo per l’efficienza operativa ma come enabler di controlli di sicurezza più efficaci e consistenti;
4. **Partnership strategiche**: Sviluppare relazioni collaborative con fornitori, autorità competenti e peer dell’industria per condividere intelligence e best practice.

Considerazioni per il management

La NIS2 richiede un commitment organizzativo che va oltre l’investimento tecnologico. Il successo dipenderà dalla capacità di:

- Integrare la cybersecurity nella strategia aziendale;
- Sviluppare una cultura di sicurezza diffusa;
- Bilanciare controlli di sicurezza con agilità operativa;
- Mantenere la competitività mentre si incrementa la resilienza.

Impatto sull’ecosistema europeo

A lungo termine, l’implementazione uniforme di NIS2 dovrebbe:

- Ridurre la superficie di attacco complessiva dell’ecosistema digitale europeo;
- Aumentare la fiducia dei cittadini nei servizi digitali;
- Posizionare l’Europa come benchmark globale per la cybersecurity.

La direttiva NIS2 rappresenta più di una normativa di cybersecurity; è una dichiarazione di intenti per un’Europa digitalmente sovrana e resiliente. Il successo della sua implementazione determinerà non solo la sicurezza dei sistemi informatici europei, ma anche la competitività dell’economia digitale europea nel contesto globale.

La sfida ora è trasformare questi requisiti normativi in vantaggi competitivi sostenibili, dimostrando che sicurezza e innovazione non sono forze opposte ma complementari nell’ecosistema digitale del futuro. I 13 pilastri forniscono una roadmap dettagliata per questa trasformazione, richiedendo un approccio metodico ma flessibile per adattarsi alle specificità di ciascuna organizzazione.

Fonti:

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/nis2-implementazione/