Whitepaper

NIS2 – Direttiva UE sulla sicurezza delle reti e dei sistemi informativi **Guida alla conformità NIS2 e al rafforzamento della resilienza cibernetica**

Indice dei **contenuti**

01	Sintesi esecutiva
02	Introduzione: una nuova era di obblighi per la cybersecurity
03	Ambito di applicazione ampliato: chi rientra nella NIS2?
04	Il cuore della conformità: misure di gestione chiave
05	Obblighi di segnalazione e responsabilità della direzione
06	Sanzioni sostanziali per non conformità
07	Information Technology (IT) vs Operational Technology (OT)
08	La prospettiva di DEKRA: dalla conformità al vantaggio competitivo
09	Raccomandazioni strategiche per l'implementazione
10	Come DEKRA può supportarvi
11	Conclusione: dalla conformità alla resilienza

Sintesi esecutiva

Guida alla conformità NIS2 e al rafforzamento della resilienza cibernetica

La Direttiva NIS2 alza l'asticella della sicurezza informatica in tutta l'UE, estendendo gli obblighi di legge a una gamma più ampia di organizzazioni rispetto al passato. I soggetti essenziali e importanti devono ora soddisfare chiari requisiti di gestione del rischio, tempistiche definite per la segnalazione degli incidenti e un coinvolgimento più stretto della direzione nella supervisione della cybersecurity.

Per la maggior parte delle organizzazioni, l'approccio migliore consiste in un processo continuo anziché in un singolo progetto, toccando la governance, i contratti della catena di fornitura, i controlli tecnici e la formazione del personale. Le organizzazioni che usano questa opportunità per far maturare la propria postura di sicurezza complessiva sono ben posizionate per trasformare un requisito normativo in una resilienza duratura e in un reale vantaggio competitivo.

Questo whitepaper illustra chi rientra nella NIS2, cosa richiede la Direttiva e la prospettiva di DEKRA su come le organizzazioni possono affrontare questi requisiti con sicurezza.

Introduzione

Una nuova era di obblighi per la cybersecurity

La direttiva UE rivista sulla sicurezza delle reti e dei sistemi informativi (NIS2) rappresenta un avanzamento significativo nella strategia di sicurezza informatica dell'Unione Europea. La direttiva mira a rafforzare la resilienza cibernetica dei settori critici nell'UE in risposta alla crescente frequenza e sofisticazione delle minacce informatiche.

La NIS2 si concentra sui soggetti essenziali e importanti che sostengono la società, l'economia e i servizi pubblici. Molti di questi soggetti gestiscono infrastrutture critiche, rendendo essenziale per le organizzazioni adottare una solida mentalità di cybersecurity e promuovere una cultura di igiene informatica. Per raggiungere questo obiettivo, le organizzazioni coperte dalla direttiva devono implementare procedure di segnalazione degli incidenti robuste, rafforzare le pratiche di gestione del rischio e garantire la sicurezza delle proprie catene di fornitura. Ciò include la responsabilità di evitare che prodotti e servizi non sicuri introducano vulnerabilità sfruttabili per compromettere i sistemi critici. La direttiva stabilisce inoltre un quadro sanzionatorio e di controllo completo, comprese sanzioni sostanziali in caso di non conformità, sottolineando l'importanza di una governance lungimirante della cybersecurity.

Questo whitepaper fornisce una panoramica dei principi e requisiti chiave della Direttiva NIS2 e delinea un approccio strategico per raggiungere, mantenere e dimostrare la conformità.

Ambito di applicazione ampliato
Chi rientra nella NIS2?

Un obiettivo centrale della Direttiva NIS2 è l'ampliamento del suo ambito di applicazione. La precedente distinzione tra operatori di servizi essenziali e fornitori di servizi digitali viene eliminata. La Direttiva categorizza gli enti interessati in due tipologie principali:

- **Soggetti essenziali:**
  Settori critici per la società e l'economia, es. energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali e spazio.

- **Soggetti importanti:**
  Ulteriori settori chiave quali servizi postali e di corriere, gestione dei rifiuti, fabbricazione/produzione di beni, industria chimica, produzione e distribuzione di alimenti, nonché alcuni settori della ricerca e del digitale.

La classificazione è determinata dal settore e dalle dimensioni dell'azienda, oltre che da eccezioni definite per legge. In molti casi, sono coperte principalmente le medie e grandi imprese (in genere a partire da 50 dipendenti o 10 milioni di euro di fatturato annuo o totale di bilancio). A seconda del tipo di ente, tuttavia, l'applicabilità può estendersi anche oltre le classiche soglie dimensionali.

Decisive sono le definizioni e le classificazioni specifiche contenute nelle leggi di recepimento di ciascun Stato membro, insieme ai relativi obblighi (ad es. registrazione e segnalazione alle autorità nazionali competenti).

Il cuore della conformità
Misure di gestione chiave

La Direttiva NIS2 concretizza i requisiti di gestione del rischio informatico. Gli enti interessati devono implementare misure tecniche e organizzative adeguate e proporzionate al rischio. Tali misure riflettono i requisiti minimi di gestione del rischio di sicurezza informatica stabiliti dall'Articolo 21 della Direttiva NIS2 e includono in particolare:

1. **Politiche per l'analisi dei rischi e la sicurezza dei sistemi informativi**
   Attuazione di processi formali per l'identificazione, la valutazione e la mitigazione dei rischi.
2. **Gestione degli incidenti**
   Definizione di procedure solide per il rilevamento, la risposta e il ripristino in caso di incidenti di sicurezza.
3. **Continuità operativa e gestione delle crisi**
   Garanzia della capacità operativa tramite strategie di backup efficaci, piani di disaster recovery e protocolli di gestione delle crisi.
4. **Sicurezza della catena di fornitura**
   Gestione dei rischi informatici all'interno della catena di fornitura e nei rapporti con i fornitori di servizi.
5. **Gestione delle vulnerabilità**
   Implementazione di processi per la gestione e la divulgazione delle vulnerabilità nei sistemi.
6. **Valutazione dell'efficacia**
   Test e valutazioni regolari dell'efficacia delle misure di sicurezza informatica.
7. **Igiene informatica e formazione**
   Promozione delle pratiche di sicurezza di base e formazione regolare dei dipendenti.
8. **Crittografia**
   Uso della crittografia e di controlli crittografici, ove necessario, per proteggere i dati.
9. **Sicurezza del personale**
   Applicazione di politiche di controllo degli accessi e gestione sicura degli asset.
10. **Autenticazione a più fattori (MFA) e comunicazioni sicure**
    Uso della MFA e protezione delle comunicazioni interne.

Obblighi di segnalazione e responsabilità della direzione

La Direttiva NIS2 prevede obblighi di segnalazione rigidi e tempestivi. I soggetti essenziali e importanti devono segnalare gli incidenti di sicurezza significativi alle autorità nazionali competenti designate da ciascuno Stato membro.

La segnalazione avviene secondo scadenze precise:

- **Preavviso (Early warning)**: Entro 24 ore da quando si viene a conoscenza dell'incidente.
- **Notifica dell'incidente**: Entro 72 ore, inclusa una valutazione iniziale (gravità e impatto). Se applicabile, possono essere richiesti rapporti intermedi.
- **Rapporto finale**: Da presentare generalmente entro un mese*.

I requisiti stabiliscono una chiara responsabilità per la direzione. I vertici aziendali (C-level) non solo devono approvare le misure di gestione del rischio informatico, ma devono anche sovrintendere attivamente e garantire la loro efficace attuazione in tutta l'organizzazione. Ai sensi della NIS2, la direzione dell'azienda può essere ritenuta personalmente responsabile in caso di mancata leadership, governance e direzione strategica necessarie a garantire la conformità.

La direzione è inoltre responsabile di promuovere una solida cultura della sicurezza informatica garantendo che il personale riceva una formazione adeguata. Inoltre, i membri del top management sono tenuti a partecipare essi stessi regolarmente a corsi di formazione sulla cybersecurity.
Il mancato rispetto di tali obblighi può comportare misure sanzionatorie significative, comprese sanzioni amministrative e ingenti sanzioni pecuniarie.

*Nota: le tempistiche esatte possono variare a seconda dello Stato membro.

Sanzioni sostanziali per non conformità

Le conseguenze finanziarie del mancato rispetto dei requisiti NIS2 sono considerevoli. La Direttiva impone agli Stati membri di prevedere sanzioni pecuniarie fino a:

- **Soggetti essenziali**: Fino a 10 milioni di euro o al 2% del fatturato annuo globale complessivo (se superiore).
- **Soggetti importanti**: Fino a 7 milioni di euro o all'1,4% del fatturato annuo globale (se superiore).

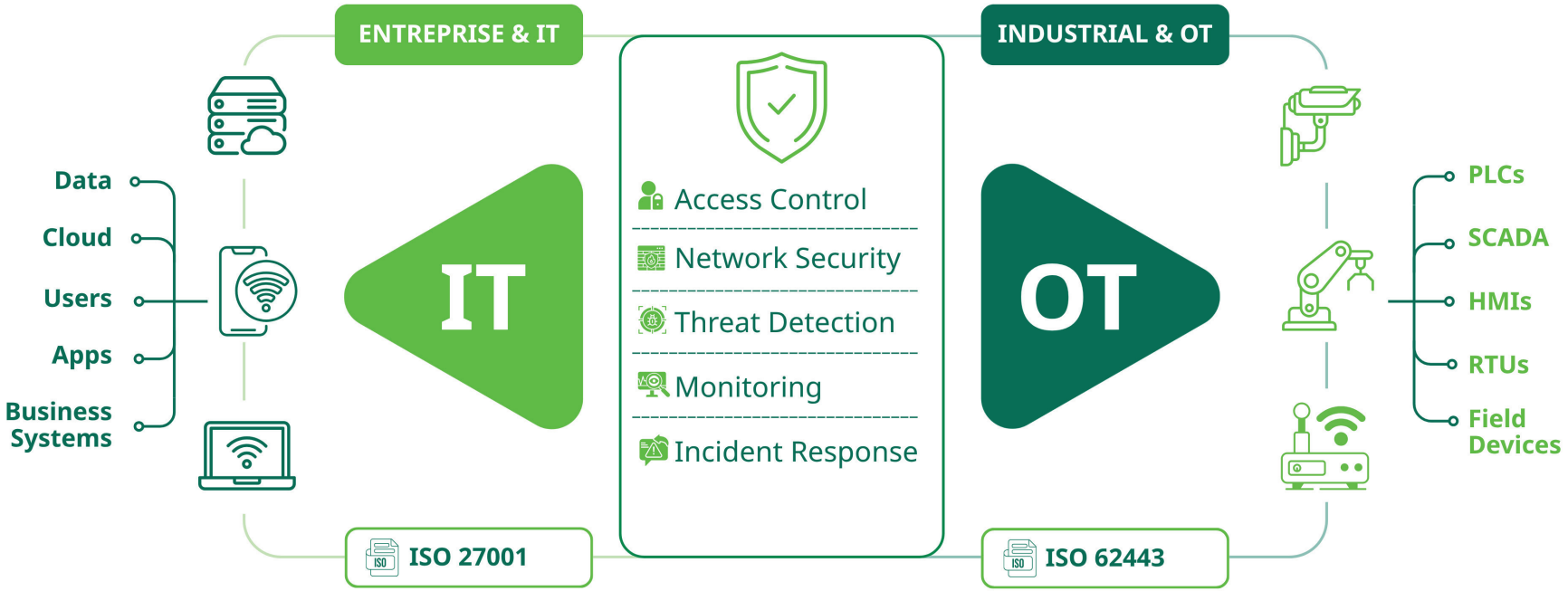
Oltre alle sanzioni pecuniarie, le autorità di vigilanza possono imporre misure correttive come istruzioni vincolanti, audit di sicurezza o ordini di conformità*.

*Nota: l'importo esatto delle sanzioni e i meccanismi sanzionatori sono definiti dalle leggi nazionali di recepimento di ciascuno Stato membro, per l'Italia ciò è avvenuto in seguito all'entrata in vigore del D.Lgs. 138/2024, confermando i valori previsti dalla direttiva.

Information Technology (IT) vs Operational Technology (OT)

Information Technology (IT): Si concentra sulla protezione dei sistemi informativi aziendali e d'ufficio per garantire riservatezza, integrità e disponibilità delle informazioni. Lo standard ISO 27001 supporta questo ambito.

Operational Technology (OT): Comprende hardware e software che monitorano e controllano i processi fisici e le infrastrutture (es. reti elettriche, impianti idrici, reti di trasporto, linee di produzione, fino ai sistemi smart building per la gestione di illuminazione, e condizioni ambientali). Lo standard IEC 62443 supporta la progettazione e l'operatività sicura degli ambienti OT.



Differenza chiave
Un attacco a un sistema IT interrompe le operazioni aziendali; un attacco a un sistema OT può interrompere servizi essenziali, danneggiare apparecchiature, creare rischi ambientali o mettere a rischio la sicurezza delle persone. Pertanto, la cybersecurity OT pone maggiore enfasi su sicurezza (safety), resilienza, disponibilità continua e processi operativi sicuri.

La prospettiva di DEKRA

Dalla conformità al vantaggio competitivo

Mentre molte organizzazioni affrontano la NIS2 come un semplice esercizio di conformità isolato, l'integrazione di questo quadro con gli standard esistenti offre un valore nettamente superiore. NIS2, ISO/IEC 27001 e IEC 62443-2-1 condividono lo stesso obiettivo di fondo: la gestione sistematica del rischio informatico.

Le aree in cui le aziende trovano maggior margine di miglioramento sono:

- **Coinvolgimento diretto del management**: passare da un'approvazione formale a una supervisione attiva e dimostrabile.
- **Visibilità sulla catena di fornitura**: estendere il controllo anche ai fornitori.
- **Test dei piani di risposta agli incidenti**: verificare sul campo la capacità di rispettare la notifica delle 24 ore.

Le organizzazioni con un ISMS (ISO/IEC 27001) e/o un CSMS (IEC 62443-2-1) già avviati sono ben posizionate per soddisfare i requisiti della NIS2 sia per l'IT che per l'OT.

Raccomandazioni strategiche per l’implementazione

- **Eseguire una Gap Analysis IT/OT:** Valutare la postura di sicurezza attuale rispetto ai requisiti NIS2.
- **Rafforzare le fondamenta:** Stabilire misure che proteggano da accessi non autorizzati e attacchi.
- **Revisionare i contratti di fornitura:** Esplicitare le responsabilità di cybersecurity nei contratti con i fornitori (le certificazioni IEC 62443-2-1 / IEC 62443-2-4 sono d’aiuto).
- **Formare la direzione:** Sensibilizzare il top management sulle proprie responsabilità legali dirette.
- **Testare i piani:** Eseguire simulazioni periodiche sui piani di risposta agli incidenti e continuità operativa.

Come DEKRA può supportarvi

- Gap analysis e valutazioni del rischio.
- Supporto nello sviluppo di piani di incident response e business continuity.
- Formazione mirata per il personale tecnico e per la direzione.
- Formazione basata sugli standard OT.
- Valutazione e certificazione per gli standard OT IEC 62443 (IEC 62443-2-1, IEC 62443-2-4 e IEC 62443-3-3).

Conclusione

Dalla conformità alla resilienza

La Direttiva NIS2 è più di un ostacolo normativo: è un modello per costruire un'organizzazione più sicura e resiliente. Abbracciare questi requisiti permette di ridurre il rischio di sanzioni e di migliorare nettamente la capacità di respingere e gestire gli attacchi informatici, tutelando operatività, reputazione e clienti.

Vorresti maggiori informazioni?

Contattaci!

DEKRA

dekra.it

DEKRA ITALIA