Whitepaper:

NIS2 e la gestione del rischio aziendale

Dario Dal Mas

02/10/2024

LAVORA SENZA COMPROMESSI

P.zza degli Alpini, 15 Lentiai
32026 Borgo Valbelluna (BL)

TEL: 0437 552337 - FAX: 0437 552338
in@sersis.com - www.sersis.com

Introduzione

La nuova direttiva europea **NIS2** (Network and Information Security Directive) rappresenta un aggiornamento cruciale nella regolamentazione della sicurezza informatica per le infrastrutture critiche e i servizi essenziali all'interno dell'Unione Europea.

Questo Whitepaper esplora la **gestione del rischio aziendale**, con un focus specifico sugli sviluppi normativi italiani, e su come le organizzazioni possono affrontare le sfide normative e rafforzare la loro resilienza contro le minacce informatiche.

---

1. Contesto Normativo della NIS2

1.1 Origini della NIS2

La direttiva NIS2 è stata adottata dall'Unione Europea nel dicembre 2022, come risposta alle crescenti minacce informatiche e alla necessità di migliorare la sicurezza delle reti e dei sistemi informativi essenziali. Rispetto alla NIS1, la nuova direttiva prevede regole più stringenti e una maggiore cooperazione tra gli Stati membri, al fine di proteggere le infrastrutture critiche.

1.2 Settori Interessati

La NIS2 amplia l'ambito di applicazione rispetto alla direttiva precedente, includendo settori chiave per il funzionamento della società e dell'economia, tra cui:

- Energia
- Trasporti
- Sanità
- Finanza
- Infrastrutture digitali (cloud, data center)
- Servizi pubblici (acqua potabile, gestione rifiuti)

---

2. La Gestione del Rischio nell'Era della NIS2

2.1 Perché la Gestione del Rischio è Cruciale?

La direttiva NIS2 pone grande enfasi sull'importanza di un approccio sistematico e proattivo alla **gestione del rischio**. Le minacce informatiche possono causare gravi interruzioni operative, perdite finanziarie e danni reputazionali. Pertanto, una gestione efficace del rischio non è solo una questione di conformità, ma è cruciale per garantire la continuità operativa delle organizzazioni.

2.2 Le Principali Componenti della Gestione del Rischio

La gestione del rischio aziendale secondo la NIS2 prevede una serie di passaggi fondamentali:

- **Identificazione delle minacce**: Le aziende devono individuare tutte le minacce informatiche rilevanti, sia interne che esterne.

P.zza degli Alpini, 15 Lentiai
32026 Borgo Valbelluna (BL)

TEL: 0437 552337 - FAX: 0437 552338
in@sersis.com - www.sersis.com

- **Valutazione delle vulnerabilità**: Devono essere eseguiti audit regolari per identificare e mitigare le vulnerabilità.
- **Misure di mitigazione del rischio**: Le aziende devono implementare misure organizzative e tecniche adeguate per proteggere le loro reti e sistemi.
- **Monitoraggio e risposta**: È essenziale disporre di meccanismi di monitoraggio continui e di piani di risposta agli incidenti.

---

3. NIS2 e la Normativa Italiana

3.1. Il Quadro Normativo Italiano

In Italia, la direttiva NIS2 sarà recepita nell'ambito del sistema normativo esistente, che già include regolamenti specifici per la sicurezza informatica. Il decreto legislativo n. 65 del 18 maggio 2018 ha recepito la prima direttiva NIS (NIS1), introducendo obblighi per i cosiddetti **Operatori di Servizi Essenziali (OSE)** e i **Fornitori di Servizi Digitali (FSD)**.
La direttiva **NIS2** è stata ufficialmente adottata dall'Unione Europea il **27 dicembre 2022**. Gli Stati membri hanno **21 mesi** di tempo, a partire da questa data, per recepire la direttiva nella propria legislazione nazionale.

3.2. Il **Decreto Legislativo 4 settembre 2024, n. 138** pubblicato **Martedì, 1° ottobre 2024** nella Gazzetta Ufficiale n°230 recepisce ufficialmente in Italia la **Direttiva NIS2** (Direttiva UE 2022/2555), fissando nuove regole per garantire un livello comune elevato di cybersicurezza nell'Unione Europea. Il decreto introduce cambiamenti significativi rispetto alla precedente direttiva NIS (UE 2016/1148), che viene abrogata con l'entrata in vigore delle nuove disposizioni il **16 ottobre 2024**.

---

4. Principali novità introdotte dal Decreto 138/2024

4.1. Estensione dell'ambito di applicazione:

La normativa non si limita più agli **Operatori di Servizi Essenziali (OSE)** e ai **Fornitori di Servizi Digitali (FSD)**, ma distingue tra **soggetti essenziali** e **soggetti importanti**, includendo una gamma più ampia di settori, tra cui **energia**, **trasporti**, **bancario**, **sanità**, **infrastrutture digitali**, **gestione dei rifiuti** e altri settori critici come la **produzione chimica** e l'**alimentare**.

4.2. Obblighi di gestione del rischio:

Le aziende classificate come "essenziali" o "importanti" dovranno adottare **misure tecniche e organizzative adeguate** per la gestione dei rischi informatici. La gravità di questi obblighi dipenderà dalla dimensione dell'azienda, dal settore e dal grado di **cyber-maturità** già raggiunto.

4.3. Obblighi di notifica degli incidenti:

Le aziende saranno obbligate a notificare incidenti significativi al **CSIRT Italia** (Computer Security Incident Response Team) senza indebito ritardo, e a rispettare precise tempistiche di notifica:

4.3.1.1. **Prenotifica entro 24 ore** per segnalare l'incidente e indicare il suo impatto potenziale.

P.zza degli Alpini, 15 Lentiai
32026 Borgo Valbelluna (BL)

TEL: 0437 552337 - FAX: 0437 552338
in@sersis.com - www.sersis.com

4.3.1.2. **Notifica completa entro 72 ore**, che deve includere maggiori dettagli e una valutazione d'impatto dell'incidente.

4.4. **Sanzioni**:
Le sanzioni per la non conformità sono molto elevate:

4.4.1.1. Fino a **10 milioni di euro** o il **2% del fatturato annuo mondiale** per i soggetti essenziali.

4.4.1.2. Fino a **7 milioni di euro** o **1,4% del fatturato annuo mondiale** per i soggetti importanti.

4.5. **Ruolo centrale dell'ACN (Agenzia per la Cybersicurezza Nazionale)**:
L'ACN sarà responsabile dell'**identificazione** e della **notifica** dei soggetti essenziali e importanti che rientrano nella normativa. Le aziende dovranno registrarsi sulla piattaforma dell'ACN a partire dal **31 marzo 2025**, con obblighi di aggiornamento annuale delle attività e dei servizi erogati.

---

5. Strumenti e Framework per la Conformità alla NIS2

5.1 Standard di Sicurezza Internazionali

Per aiutare le organizzazioni italiane a conformarsi alla NIS2, esistono diversi standard di sicurezza internazionale che offrono linee guida per la gestione del rischio, tra cui:

- **ISO/IEC 27001**: Standard internazionale per la gestione della sicurezza delle informazioni. Adottato da molte aziende italiane, rappresenta un framework solido per rispettare i requisiti della NIS2.
- **NIST Cybersecurity Framework**: Sebbene sviluppato negli Stati Uniti, il NIST è ampiamente utilizzato anche in Italia, soprattutto dalle grandi aziende multinazionali.

5.2 Tecnologie Abilitanti

Le aziende italiane possono rafforzare la loro sicurezza adottando tecnologie avanzate come:

- **Sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM)** per il monitoraggio e l'analisi in tempo reale.
- **Soluzioni di automazione della sicurezza**: L'uso dell'intelligenza artificiale per la rilevazione e risposta agli incidenti.
- **Crittografia dei dati**: Per proteggere i dati sensibili sia a riposo che in transito.

---

6. La Supply Chain e la Resilienza Informativa

6.1 Gestione del Rischio nella Supply Chain

P.zza degli Alpini, 15 Lentiai
32026 Borgo Valbelluna (BL)

TEL: 0437 552337 - FAX: 0437 552338
in@sersis.com - www.sersis.com

Un aspetto chiave della NIS2 è il riconoscimento che le minacce alla sicurezza possono derivare da fornitori e partner terzi. Le aziende italiane dovranno quindi valutare i rischi lungo tutta la supply chain, adottando misure di sicurezza anche nei confronti dei propri fornitori critici.

6.2 Resilienza e Continuità Operativa

La resilienza operativa è una priorità per la NIS2. Le organizzazioni italiane dovranno garantire la continuità dei loro servizi anche in caso di attacchi informatici, implementando piani di continuità operativa (BCP) e strategie di disaster recovery.

A tale proposito può essere un valido aiuto la certificazione **ISO 22301: Gestione della Continuità Operativa**

---

7. Strategie per l'Adeguamento alla NIS2 in Italia

7.1 Valutazione Preliminare

Le aziende italiane devono condurre un'analisi approfondita dei propri sistemi e infrastrutture digitali per identificare le aree di vulnerabilità e migliorare i propri processi di gestione del rischio.

7.2 Formazione del Personale

L'**alfabetizzazione digitale** del personale è fondamentale per affrontare efficacemente le sfide della NIS2. Le aziende devono promuovere la consapevolezza delle minacce informatiche attraverso sessioni di formazione specifiche.

7.3 Collaborazione con Esperti Esterni

Le aziende possono trarre vantaggio dalla collaborazione con esperti di sicurezza informatica e consulenti legali, soprattutto per quanto riguarda l'adeguamento normativo e la gestione delle minacce emergenti.

Conclusione

L'entrata in vigore della NIS2 porterà a un significativo rafforzamento delle infrastrutture di cybersicurezza in Italia. Le aziende che operano nei settori critici devono prepararsi ad affrontare nuove sfide normative implementando misure di gestione del rischio adeguate.

La conformità alla NIS2 non è solo un obbligo normativo, ma anche un'opportunità per proteggere le proprie operazioni in un contesto digitale sempre più complesso e pericoloso.