Linee Guida per l'Implementazione della Direttiva NIS2

La **Direttiva NIS2 (Direttiva (UE) 2022/2555)** è il nuovo quadro normativo europeo sulla sicurezza informatica, che aggiorna e amplia la precedente direttiva NIS. Le linee guida seguenti aiutano le organizzazioni a conformarsi ai requisiti stabiliti.

---

1. Ambito di Applicazione

Settori e Entità Rilevanti

La NIS2 si applica a:

- **Entità essenziali (EE)** – Servizi critici (energia, trasporti, sanità, finanza, acqua, infrastrutture digitali).
- **Entità importanti (EI)** – Altre organizzazioni con impatto significativo (poste, gestione rifiuti, produzione alimentare, settore manifatturiero).

Soglie dimensionali

- **EE**: Indipendentemente dalle dimensioni.
- **EI**: Imprese con > 50 dipendenti e/o fatturato > €10 milioni.

---

2. Obblighi Principali

A. Gestione del Rischio e Sicurezza

- Adottare **politiche di sicurezza informatica** basate su standard riconosciuti (ISO 27001, NIST, CIS).
- Implementare:
  - Controlli di accesso e autenticazione robusta (MFA).
  - Protezione da malware e intrusioni.
  - Backup e disaster recovery.
  - Crittografia dei dati sensibili.

B. Reporting degli Incidenti

- Notificare gli incidenti significativi entro **24 ore** (segnalazione iniziale) e **72 ore** (report dettagliato) all'autorità competente (CSIRT nazionale).

C. Due Diligence nella Catena di Approvvigionamento

- Valutare i rischi legati a fornitori e terze parti.
- Includere clausole di sicurezza nei contratti.

D. Formazione e Consapevolezza

- Formare regolarmente il personale su minacce informatiche (phishing, ransomware).

---

3. Governance e Responsabilità

- Il **management** (C-level) è direttamente responsabile della conformità.
- Istituire un **responsabile della sicurezza informatica** (CISO o equivalente).

---

4. Sanzioni per Non Conformità

- **Amministrative**: Fino al **2% del fatturato globale** o **€10 milioni** (per EE).
- **Penali**: In casi gravi, responsabilità legale per i dirigenti.

---

5. Passi per l'Implementazione

1. **Valutazione iniziale**: Identificare asset critici e gap di sicurezza.
2. **Piano di adeguamento**: Allineare processi agli obblighi NIS2.
3. **Monitoraggio continuo**: Testare e aggiornare le misure di sicurezza.
4. **Collaborazione con autorità**: Coinvolgere il CSIRT nazionale e condividere best practice.

---

6. Scadenze

- **17 ottobre 2024**: Termine per il recepimento negli Stati membri.
- **18 ottobre 2024**: Piena applicazione della direttiva.

Risorse Utili

- Testo completo NIS2
- Linee guida ENISA e autorità nazionali (es. AgID in Italia).

Per ulteriori dettagli, consultare il **CSIRT nazionale** o un esperto in compliance cybersecurity.