REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere **SICURI?**

NIS2 e Governance by Design: quando la sicurezza diventa una responsabilità di tutta l'azienda

Controlli e misure per NIS 2

Relatore Cesare Gallotti

Agenda

1- Le misure di sicurezza della NISD
2- Implementing act per i fornitori di servizi IT
3- Le misure di sicurezza richieste da ACN
4- Categorizzazione e misure di sicurezza

Le misure di sicurezza della NISD – Valutazione del rischio

NIS2, articolo 21: «Le misure di cui al paragrafo 1 sono basate su un approccio multirischio».

Le misure devono portare a un “livello appropriato” di sicurezza. Vanno quindi realizzate sulla base di una valutazione del rischio.

Rischio: la potenziale perdita o perturbazione causata da un incidente; è espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che l'incidente si verifichi.

Quindi il rischio:

- include quelli logico, fisico, di governo, di lock in tecnologico, relativo alle utilities;
- deve considerare l’impatto sociale ed economico.

La NISD non fornisce indicazioni su quale approccio seguire.

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.

Le misure, come riportate dal D. Lgs. 138:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
b) gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche;
c) continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;
d) sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;
f) politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;

g) pratiche di igiene di base e di formazione in materia di sicurezza informatica
   - NOTA: L'articolo 23 impone agli organi di amministrazione e gli organi direttivi dei soggetti NIS 2 una formazione in materia di sicurezza informatica;

h) politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura
   - NOTA: non chiara la differenza tra crittografia e cifratura, presente anche in inglese tra cryptography e encryption;

i) sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;

j) 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 da parte del soggetto al proprio interno, ove opportuno.

Le misure di sicurezza della NISD – Catena di approvvigionamento (1/2)

La NIS 2 descrive più approfonditamente le necessità di controllo della catena di approvvigionamento:

> *i soggetti tengono conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.*

Vanno quindi monitorati i lavori del Gruppo di cooperazione NIS (https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group).

Le misure di sicurezza della NISD – Catena di approvvigionamento (2/2)

Rischi relativi alla catena di approvvigionamento (supply chain):

- Interruzione di servizi di fornitori (inclusi ISP, CSP, DR site, supporto tecnico specialistico, esternalizzazione attività). Per esempio a causa di fallimento, chiusura, incidenti.
- Dipendenza da un unico fornitore
- Compromissione dei sistemi IT dei fornitori
- Rivelazione di informazioni da parte dei fornitori
- Malfunzionamenti o compromissione software sviluppati dai fornitori

Le misure di sicurezza sono trattate anche in altri articoli del D. Lgs. 138.

Eccone alcuni:

- l'articolo 27 prevede che ACN può imporre l'uso di prodotti certificati;
- l'articolo 29 è specifico per chi si occupa dei nomi di dominio, ma non presenta misure di sicurezza vere e proprie;
- gli articoli 35 e 36 dicono che ACN può imporre VA-PT o audit da parte di soggetti selezionati.

Implementing act per i fornitori di servizi IT

Regolamento di esecuzione (UE) 2024/2690 della Commissione del 17 ottobre 2024 recante *modalità di applicazione della direttiva (UE) 2022/2555 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza e l'ulteriore specificazione dei casi in cui un incidente è considerato significativo per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari.*

Implementing act per i fornitori di servizi IT – Le misure (1/2)

Le misure sono riportate quasi come nell'articolo 21 della Direttiva (simile a quanto riportato nel D. Lgs. 138). In 13 capitoli (come la precedente ISO/IEC 27002:2013):

1. Politica di sicurezza dei sistemi informativi e di rete
2. Politica di gestione dei rischi
3. Gestione degli incidenti
4. Continuità operativa e gestione delle crisi
5. Sicurezza della catena di approvvigionamento
6. Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete
7. Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza

Implementing act per i fornitori di servizi IT – Le misure (2/2)

8. Pratiche di igiene informatica di base e formazione in materia di sicurezza
9. Crittografia
10. Sicurezza delle risorse umane
11. Controllo dell'accesso
12. Gestione delle risorse
13. Sicurezza ambientale e fisica

ACN ha pubblicato le misure «di base» per i soggetti importanti ed essenziali. L'ultima versione è nella Determinazione del 18 dicembre 2025.

Le misure sono distribuite secondo le 4 categorie del NIST cyber-security framework (CSF):

1. Governo (Govern)
2. Identificazione (Identify)
3. Protezione (Protect)
4. Rilevamento (Detect)
5. Risposta (Respond)
6. Ripristino (Recover)

Spesso si tratta di una risistemazione delle misure presenti nell'Implementing Act 2690.

L'implementing act non è mai nominato e questo può creare problemi di interpretazione.

Utili (ma non troppo) le Linee Guida NIS - Specifiche di base - Guida alla lettura.

Categorizzazione e misure di sicurezza (1/2)

Determinazione di ACN relativa all'art. 30 del D. Lgs. 138 (ultima versione del 14/04/2026).

ACN richiede ai soggetti NIS di elencare e categorizzare «tutte le attività svolte e dei servizi erogati, internamente ed esternamente, suddivisi nelle macro-aree di cui a un modello di categorizzazione» fornito da ACN.

E' richiesto di fornire una categoria di rilevanza a ciascuna attività «sulla base di una propria valutazione dell'impatto di una possibile compromissione dell'attività o del servizio sulla capacità del soggetto di svolgere correttamente le attività e i servizi NIS».

Categorizzazione e misure di sicurezza (2/2)

I livelli sono 4 (ma non per la PA, che ne prevede 3):

a) impatto alto;
b) impatto medio;
c) impatto basso;
d) impatto minimo.

ACN ha fatto sapere che farà ulteriori richieste di misure di sicurezza da applicare a seconda della categoria di rilevanza.

Si prevede che tali richieste, con le relative scadenze, saranno fatte dopo ottobre 2026.