Cyber Risk e Sistema finanziario

Pref. Bruno Frattasi - Direttore Generale ACN

Convegno SADIBA – Varignana (Bologna), 28 marzo 2025

Percorso di avvicinamento e applicazione della NIS 2

- Legge 28 giugno 2024, n. 90, *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*
  - ✓ dotarsi, ove non sia già presente, di una **struttura per la cybersicurezza;**
  - ✓ istituire la figura del **referente per la cybersicurezza;**
  - ✓ obbligo di notifica di incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge n. 105 del 2019, così come convertito con modificazioni dalla legge n. 133 del 2019 (il "Decreto Perimetro").

La legge 90 ha introdotto, inoltre, una modifica all'articolo 8 del decreto-legge n. 82 del 2021, prevedendo un nuovo comma 4.1 ai sensi del quale in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese, il Nucleo per la cybersicurezza può essere convocato nella composizione ristretta, di volta in volta estesa alla partecipazione di un rappresentante:

- **della Direzione nazionale antimafia e antiterrorismo;**
- **della Banca d'Italia;**
- **di uno o più operatori di cui all'articolo 1, comma 2-bis, del decreto-legge n. 105 del 2019. Si fa riferimento ai soggetti iscritti nel Perimetro di sicurezza nazionale cibernetica;**
- **nonché di eventuali altri soggetti interessati alle stesse questioni.**

Direttiva NIS 2 e decreto legislativo di recepimento

- Legge di delegazione europea 2022-2023 A.C. 1342;
- Decreto legislativo 4 settembre 2024, n. 138, Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione
  - ✓ censimento e registrazione dei soggetti avvenuta nel periodo 1° dicembre 2024 - 28 febbraio 2025;
  - ✓ aprile 2025: elaborazione e adozione obblighi di base;
  - ✓ tassonomia incidenti;
  - ✓ obbligo di notifica di base a partire da gennaio 2026.

Attacchi Denial of Service (DoS) e Distributed Denial of Service (DDoS)

- Lo scorso 22 febbraio ACN ha pubblicato un rapporto sulla minaccia **Denial of Service (DoS) e Distributed Denial of Service (DDoS)**, analizzando le strategie d'attacco più diffuse e fornendo raccomandazioni specifiche per la mitigazione del rischio.
- **Motivazioni alla base di un attacco DDoS:**
  - ✓ economiche: attacchi condotti per estorcere denaro in cambio dell'interruzione dell'attacco, oppure per danneggiare la concorrenza sabotandone le operazioni;
  - ✓ ideologiche: azioni mirate a promuovere cause politiche o sociali, tipiche del fenomeno dell'hacktivismo;
  - ✓ personali: attacchi mossi da vendetta, desiderio di dimostrare abilità tecniche o ricerca di notorietà all'interno della comunità hacker.
- Numeri di attacchi **DDoS** al sistema finanziario:
  - ✓ nel periodo compreso tra il **1° gennaio 2024** e il **27 marzo 2025, sono stati registrati** 78 attacchi al settore finanziario. Tra questi, solo il 15% ha determinato disservizi, che si sono rivelati comunque di carattere temporaneo (tipicamente circa un'ora di irraggiungibilità della risorsa attaccata).

Minaccia Ransomware

- Minaccia ransomware duplicemente insidiosa perché compromette la sicurezza dei dati, la cui esfiltrazione e crittazione è funzionale al ricatto estorsivo, e la sicurezza economica, che ne viene incrinata in misura notevole.
- Il 20 dicembre 2024 **ACN ha pubblicato un rapporto sullo stato dell'arte della minaccia ransomware** in Italia e nel mondo.
- Legge 28 giugno 2024, n. 90, ha modificato il delitto di estorsione di cui all'art. 629 c.p., introducendo al comma 3, una nuova fattispecie di reato, la c.d. estorsione informatica, con un severo inasprimento di pena.
- La diffusione mondiale di tale minaccia e il suo inasprirsi hanno portato, inoltre, alla costituzione di una vasta alleanza internazionale, la Counter Ransomware Initiative (**C.R.I.**), il cui obiettivo consiste nel definire un piano d'azione condiviso, capace di contrapporsi in maniera coesa al fenomeno.

Banche dati critiche

- **Ulteriori iniziative di ACN per il rafforzamento della resilienza e della sicurezza cibernetiche:**

  ✓ Il 25 novembre u.s, ACN ha "varato" le Linee guida per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio.
  Si tratta di un importante documento volto a rafforzare la prevenzione e il contrasto del rischio di accessi abusivi, sia da parte di *insider* (*insider threats*) che da minacce esterne.

  ✓ Modifica in itinere DPCM tassonomia incidenti per i soggetti PSNC.

RAPPORTO DORA-NIS 2

Specializzare non significa disunire, ma armonizzare.

Raccordo e integrazione tra i due quadri normativi.

Il crescente grado di digitalizzazione e interconnessione amplifica i rischi informatici, rendendo anche il sistema finanziario più esposto alle minacce e alla loro rapida diffusione.

Necessità di raccordo e integrazione rispetto al quadro orizzontale di cybersicurezza dell'Unione stabilito dalla direttiva NIS 2.

Raccordo e integrazione tra DORA e NIS 2

- **<u>14 dicembre 2022</u>: contestuale approvazione** del **<u>Regolamento DORA,</u>** incentrato sulla resilienza operativa digitale del sistema finanziario, e della **<u>Direttiva NIS 2,</u>** relativa a misure volte a garantire un livello comune elevato di cybersicurezza nell'Unione.
- **Non si <u>tratta di una mera coincidenza temporale bensì di una sostanziale coerenza di impostazione tra i due provvedimenti europei</u>**.

Considerando 16 - DORA

- Considerando 16 - DORA:

✓ Maggiore livello di armonizzazione delle varie componenti della resilienza digitale.

✓ Incremento dell'armonizzazione anche con riguardo ai requisiti di cui alla direttiva NIS 2.

✓ **DORA è *lex specialis* rispetto alla direttiva NIS 2.**

✓ **Mantenere un saldo rapporto tra il settore finanziario e il quadro orizzontale di cybersicurezza dell'Unione, come attualmente stabilito nella direttiva NIS 2.**

✓ **Garantire coerenza con le strategie di cybersicurezza adottate dagli Stati membri e permettere alle Autorità di vigilanza finanziaria di venire a conoscenza degli incidenti informatici che colpiscono altri settori contemplati dalla direttiva NIS 2.**

Considerando 16 – DORA: Effetto

Considerando 16 - DORA: **Effetto**

- Un'entità finanziaria le cui attività rientrano nel campo di applicazione sia della NIS 2 che del Regolamento DORA può considerarsi "**compliant**" riguardo ai requisiti di cybersicurezza se rispetta le disposizioni previste da quest'ultimo Regolamento.
- **Un approccio integrato** tra DORA e NIS 2 favorisce una strategia di risposta coordinata a livello europeo.

Considerando 18 - DORA

- Considerando 18 - DORA:

  Per consentire **<u>l'apprendimento intersettoriale</u>** e attingere efficacemente alle **esperienze di altri settori nella lotta alle minacce informatiche,** le entità finanziarie, cui si applica anche la NIS 2, dovrebbero continuare a fare parte dell'«ecosistema» di tale direttiva.

Considerando 18 - DORA: **Effetto**

- Le entità finanziarie tenute a ottemperare alle disposizioni previste dal Regolamento DORA sono chiamate a fare parte dell'ecosistema NIS.
- L'art. 47 del Regolamento DORA: "**Cooperazione con le strutture e le autorità istituite dalla direttiva NIS 2**".

Adeguamento della disciplina nazionale al Regolamento DORA

Il D.lgs. 10 marzo 2025, n. 23, «adeguamento della disciplina nazionale al Regolamento DORA»:

- **notifica dei gravi incidenti anche al CSIRT Italia** (art. 4);
- forme di coordinamento operativo e informativo tramite la stipula di uno o più **protocolli d'intesa.**
- Protocolli d'intesa con l'Agenzia per la cybersicurezza nazionale per regolare lo scambio di informazioni pertinenti, istituire forme di consulenza e assistenza tecnica reciproca e meccanismi di coordinamento efficaci e di risposta rapida nel caso di incidenti (art. 5)

La Direttiva NIS 2: Considerando 22

Considerando 22 – NIS 2

Atti settoriali e Atti di esecuzione

- ✓ Evitare la frammentazione delle disposizioni in materia di cybersicurezza.
- ✓ Qualora gli atti di esecuzione della NIS 2 non risultino adeguati a garantire un livello elevato di cybersicurezza in tutta l'Unione, gli atti giuridici settoriali potrebbero contribuire a garantire tale scopo, tenendo pienamente conto delle specificità e delle complessità dei settori interessati.
- ✓ **L'adozione di ulteriori atti giuridici settoriali dell'Unione** deve tenere conto della necessità di un quadro di sicurezza informatica globale e coerente.

La Direttiva NIS 2: Considerando 28

Considerando 28 – NIS 2

DORA è *lex specialis*

- Il Regolamento DORA è atto giuridico settoriale dell'Unione europea in relazione alla direttiva NIS 2 per quanto riguarda i soggetti del settore finanziario.
- Gli Stati membri non dovrebbero, pertanto, applicare le disposizioni della NIS 2 ai soggetti finanziari contemplati dal Regolamento DORA.
- E' importante mantenere una solida relazione e lo scambio di informazioni con il settore finanziario.

CONCLUSIONI

Conclusioni

Necessario approccio integrato tra i due quadri normativi

- DORA è *lex specialis* rispetto alla disciplina NIS 2.
- **Stretta collaborazione e continuo scambio di informazioni tra le Autorità competenti dei due quadri normativi**.
- **Approccio integrato** per una maggiore resilienza operativa e una risposta coordinata agli incidenti cibernetici su scala europea.
- Miglioramento complessivo della sicurezza delle infrastrutture digitali.
- **Collaborazione** e **coordinamento per una strategia di cybersicurezza coesa e robusta** in tutta l'Unione europea.


Parco della Cyber sicurezza
Infosharing e Rete degli ISAC
Cyber Innovation Network
Autonomia Strategica
Centro di Valutazione e Certificazione Nazionale
Rete dei CERT
Strategia Nazionale
AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT
Nucleo per la Cybersicurezza
Centro Nazionale di Coordinamento
PNRR – M1C1 Inv1.5 Cybersecurity
HyperSOC
Grazie
www.acn.gov.it