di Roberto Setola e Giacomo Assenza

RECEPIMENTO DELLA DIRETTIVA NIS SULLA CYBER-SECURITY DELLE RETI

Roberto SETOLA è professore associato (settore ING-INF/04 Automatica) presso l'Università Campus BioMedico di Roma dove ricopre anche il ruolo di Direttore del Laboratori Sistemi Complessi e Sicurezza. È il Direttore Scientifico del Master universitario di II livello in "Homeland Security: Sistemi, Metodi e Strumenti per la Security ed in Crisis Management".

Giacomo ASSENZA dopo aver conseguito un Master in Intelligence and International Security presso il King's College of London collabora dal 2018 con il Laboratorio Sistemi Complessi e Sicurezza di UCBM svolgendo ricerca nell'ambito della cyber-war e cyber-security.

Il Decreto Legislativo del 18 maggio n.65, pubblicato sulla Gazzetta ufficiale il 9 giugno 2018 e in vigore dal 24 giugno, recepisce la Direttiva Europea 2016/1148 (Direttiva NIS), recante misure per un livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione. Il decreto è volto a promuovere una cultura di gestione del rischio e di segnalazione degli incidenti in ambito cyber, migliorare le capacità nazionali di cyber security e rafforzare la cooperazione a livello nazionale e comunitario.

Con la **direttiva 2016/1148 del 6 luglio 2016** [1] recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi, l'Unione Europea vuole affrontare con un approccio organico e trasversale l'emergente questione della cyber-security con l'intento di rafforzare la resilienza e la cooperazione tra stati membri. Come riportato nelle considerazioni introduttive della direttiva, reti, sistemi e servizi informativi svolgono un ruolo cruciale nel facilitare i movimenti di beni, servizi e persone, e la loro perturbazione potrebbe avere ripercussioni non solo sui singoli stati membri ma in tutta l'Unione danneggiando l'economia nel suo complesso. Risulta dunque necessario implementare dei livelli minimi comuni di protezione, in quanto l'attuale disomogeneità, anche alla luce delle strette interrelazioni e interdipendenze esistenti fra i diversi sistemi e componenti del cyberspace, è un fattore di insicurezza a livello comunitario.

Il legislatore europeo nella redazione della direttiva non ha adottato un orientamento prescrittivo. Il testo infatti, con un approccio similare a quanto fatto con il GDPR, non pone delle misure obbligatorie minimali da seguire pedissequamente, ma indica degli obbiettivi da raggiungere lasciando ai singoli soggetti un ampio margine di manovra nell'individuare e implementare mezzi e strumenti considerati più idonei per il loro raggiungimento.
Il **Decreto Legislativo n.65/2018** ha recepito e integrato la disciplina comunitaria nell'ordinamento giuridico nazionale. Il testo normativo persegue un triplice fine: promuovere una cultura di gestione del rischio e di segnalazione degli incidenti in ambito cyber; migliorare le capacità nazionali di cyber-security; e rafforzare la cooperazione a livello nazionale e comunitario. In particolare, per la realizzazione di tali obbiettivi il decreto opera su tre aspetti principali: identifica gli **operatori di servizi essenziali (OSE)** e **fornitori di servizi digitali (FSD)**, pone su di essi specifici **obblighi tecnico-amministrativi** e di **notifica degli incidenti**, e delinea **un assetto istituzionale** di organi con le relative competenze per la gestione e l'amministrazione in materia di cyber-security sia a livello nazionale che internazionale.

1. *Operatori Servizi Essenziali e Fornitori di Servizi Digitali*

Per l'identificazione degli **OSE** il decreto ripropone i medesimi criteri della direttiva NIS. Gli OSE sono definiti come tutti quei soggetti pubblici o privati che operano nei settori indicati nell'allegato II (energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, distribuzione acqua potabile, infrastrutture digitali) che (Art.4, comma 2):

(a) forniscono servizi essenziali per il mantenimento di attività sociali o economiche fondamentali;
(b) la fornitura di tali servizi dipende dalla rete e dai sistemi informativi;
(c) un incidente avrebbe effetti negativi rilevanti per la fornitura di tale servizio, dove la rilevanza è stabilita in base a fattori settoriali e intersettoriali.

I **FSD** invece, richiamando la Direttiva Europea 2015/1535, sono definiti come tutti i soggetti che forniscono servizi di e-commerce, cloud computing e motori di ricerca.

Sebbene l'adozione di fattori settoriali e intersettoriali sia simile a quanto previsto dalla direttiva 2008/114/CE sulle infrastrutture critiche, la NIS non adotta un criterio di valutazione basato sul rischio ma ne adotta uno legato all'impatto. Questo consente di limitare le assunzioni soggettive, semplificando di conseguenza le operazioni di "misurazione" della rilevanza dei singoli operatori. Nello specifico la NIS indica quali parametri da considerare (art. 5):

(a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato,
(b) la dipendenza di altri settori dal servizio fornito dal soggetto,
(c) l'impatto che gli incidenti potrebbero avere in termini di entità, durata, sulle attività economiche e sociali o sulla pubblica sicurezza,
(d) la quota di mercato di detto soggetto,
(e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente,
(f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio

Si noti che, a differenza di quanto previsto dalla Direttiva sulle infrastrutture critiche, nella disciplina NIS non vi è alcuna esplicita menzione ad eventuali "vittime" che potrebbero essere causate dall'incidente.

2. *Obblighi in materia di sicurezza e notifica degli incidenti*

Il capo VI del decreto attuativo prevede obblighi a carico degli OSE per arginare i rischi informatici, prevenire e gestire gli incidenti e ridurre i potenziali effetti negativi sulla continuità dei servizi essenziali. Il testo all'art. 12, non elenca in modo prescrittivo un insieme di misure minime (ovvero cosa fare), ma esprime l'**obbligo** di adottare **misure tecnico-organizzative** per assicurare un livello della sicurezza adeguato al rischio esistente, oltre a predisporre di misure e strumenti per prevenire e minimizzare gli effetti di incidenti relativi alla rete e ai sistemi informativi (ovvero quale obiettivo raggiungere). Il medesimo articolo specifica, però, che gli operatori, nell'adottare tali misure, devono tener conto delle linee guida elaborate dal gruppo di cooperazione o delle specifiche predisposizioni delle autorità competenti NIS. É dunque probabile che si delineerà un quadro di provvedimenti amministrativi con indicazioni più tecniche. Per altro ai sensi del comma 4 dell'art. 13, in presenza di acclarata non adeguatezza delle iniziative messe in atto dall'operatore, l'autorità competente NIS può emanare istruzioni vincolanti per gli OSE al fine di porre rimedio alle carenze individuate.

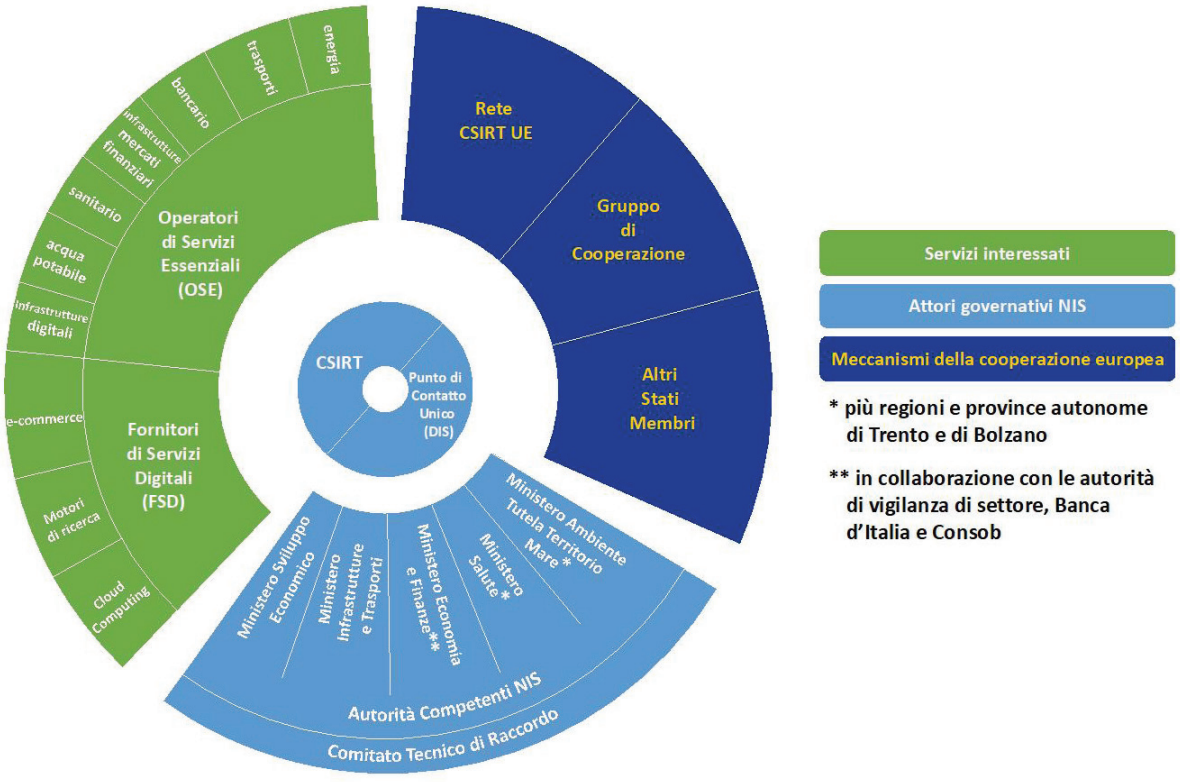

Fig.1 Assetto istituzionale in materia di sicurezza delle reti e dei sistemi informativi [3]

Il capo IV introduce anche un **obbligo di notifica** che vede gli OSE tenuti a comunicare, senza ingiustificato ritardo, al CSIRT italiano (ed all'autorità competente NIS) eventuali incidenti, allegando le informazioni necessarie per constatarne la portata e le ripercussioni sulla disponibilità del servizio. Le autorità competenti NIS, dunque i singoli ministeri, vegliano e guidano l'osservanza di tali obblighi e la loro effettiva attuazione (art.13).
Il Capo V prevede una disciplina analoga per i fornitori di servizi digitali. Anche i FSD hanno l'obbligo di adottare misure adeguate a prevenire e mitigare incidenti informatici, nonché di comunicare al CSIRT ed all'autorità competente l'occorrenza e la portata di questi (art.14).

3. *Autorità Nazionali Competenti e Punto di Contatto Unico*

Il decreto delinea e definisce un nuovo **assetto istituzionale per la gestione della sicurezza delle reti e dei sistemi informativi**. Il legislatore europeo ha lasciato un ampio margine di manovra anche per la predisposizione degli organi amministrativi, e l'art. 8 della direttiva si limita a disporre un generale obbligo in capo agli stati membri di designare una o più autorità nazionali competenti e un punto di contatto unico. L'Italia ha recepito la direttiva adottando un modello settoriale, diffuso e decentrato (fig.1).
L'art.7 del decreto indica come **autorità NIS** cinque ministeri, ognuno responsabile per il settore rientrante nella propria sfera di competenza, rispettivamente:

- Ministero dello sviluppo economico per i settori energetico e delle infrastrutture e servizi digitali;
- Ministero delle infrastrutture e dei trasporti per il settore trasporti;
- Ministero dell'economia e delle finanze per i settori bancario e dei mercati finanziari;
- Per ciò che attiene il settore sanitario si ha che Ministero della salute è l'autorità NIS per quel che riguarda l'attività di assistenza sanitaria ai sensi dell'art. 3, comma 1 lettera a) del D.lgs. n. 38/2014 e le Regioni e Province autonome di Trento e Bolzano per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati sul territorio[1];
- Ministero dell'ambiente e le Regioni e Province autonome di Trento e Bolzano per la fornitura e distribuzione di acqua potabile[2].

Autorità competenti NIS	Ambito di competenza
Ministero dello sviluppo economico	Settore dell'energia – Sottosettori energia elettrica, gas e petrolio
	Settore delle infrastrutture digitali
	Servizi digitali
Ministero delle infrastrutture e dei trasporti	Settore dei trasporti – Sottosettori trasporto aereo, trasporto ferroviario, trasporto per vie d'acqua e trasporto su strada
Ministero dell'economia e delle finanze in collaborazione con Banca d'Italia e Consob	Settore bancario
	Settore delle infrastrutture dei mercati finanziari
Ministero della salute, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità sanitarie territorialmente competenti)	Settore sanitario
Ministero dell'ambiente e della tutela del territorio e del mare, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità territorialmente competenti)	Settore della fornitura e distribuzione di acqua potabile

Le autorità competenti NIS sono responsabili dell'attuazione del decreto, e vigilano sulla sua applicazione esercitando le relative potestà ispettive e sanzionatorie. In particolare, esse possono richiedere agli OSE e FDS informazioni e dimostrazioni della corretta attuazione della policy di sicurezza informatica, anche mediante un audit che potrà essere svolto dalla autorità NIS o da un revisore abilitato. Le autorità NIS potranno, inoltre, emettere istruzioni vincolati o disporre di misure specifiche per risolvere eventuali carenze individuate (art. 13). Qualora venissero rilevate delle violazioni degli obblighi in materia di scurezza e notifica, le autorità NIS possono applicare sanzioni amministrative fino a € 150.000 (Art. 21). Le autorità NIS devono anche identificare tutti gli operatori di servizi essenziali attivi nel proprio settore di competenza e comunicare le liste al Ministero dello sviluppo economico che ha il compito di redigere un elenco complessivo entro il 9 novembre 2018.
La decisione di optare per un modello diffuso crea un assetto istituzionale più flessibile, dove le autorità competenti adottano provvedimenti specifici per rispondere alle necessità particolari dei singoli settori, senza mettere a rischio l'organicità del sistema. La nuova disciplina infatti prevede l'istituzione di organi catalizzatori come il **Comitato Tecnico di Raccordo** (art. 9), istituito da DPCM e composto dai delegati dei ministeri competenti e delle Regioni e Province autonome di Trento e Bolzano, con il compito di agevolare e coordinare il loro operato.

Quale **punto di contatto unico** invece, il decreto ha designato il **Dipartimento delle Informazioni per la Sicurezza (DIS)**. Tale decisione è in linea con la disciplina precedente (legge n.124/2007 e 133/2012, e DPCM 17/02/2017) che ha da sempre visto tale ufficio svolgere un ruolo significativo nell'architettura cyber nazionale. Il DIS è l'organo responsabile del coordinamento delle attività di ricerca finalizzate a rafforzare la protezione cibernetica e sicurezza informatica nazionale, e comprende presso i suoi uffici il Nucleo Sicurezza Cibernetica. Con la nomina di punto di contatto unico, il decreto estende le sue competenze conferendogli ulteriori mansioni di coordinamento. Il punto di contatto unico, come espresso nella direttiva europea (art. 8), svolge una funzione di collegamento per promuovere la cooperazione con le autorità degli altri stati membri, il gruppo di cooperazione e la rete CSIRT.

1 Questa frammentazione di competenze potrebbe generare, come già successo per il Fascicolo Sanitario Elettronico, una non omogeneità fra i diversi operatori con conseguente aumento di difficoltà e i rischi e ciò anche alla luce di quelli che saranno gli interscambi di informazione fra i diversi operatori sanitari nei prossimi anni.

2 In questo caso il legislatore conferisce la responsabilità congiunta al Ministero e alle Regioni.

Tra i suoi compiti, il DIS deve inviare con cadenza annuale al **Gruppo di Cooperazione**, formato da rappresentati degli stati membri, la CE e l'ENISA, una relazione sugli incidenti avvenuti contenente il numero e la natura di questi episodi e le azioni intraprese per gestirli. Inoltre, deve trasmettere ogni due anni, alla Commissione Europea, le informazioni necessarie per valutare lo stato d'attuazione della direttiva.

4. Cooperazione nazionale e comunitaria

Oltre al DIS con il ruolo di punto di contatto unico, la nuova disciplina istituisce vari organi e meccanismi per garantire la **cooperazione in materia di sicurezza delle reti e dei sistemi informativi** sia all'interno dello stato che in ambito comunitario. Uno dei canali essenziali è il meccanismo di notifica degli incidenti, di cui il **CSIRT italiano** ne costituisce l'epicentro. Il CSIRT, o **Computer Security Incident Response Team**, assorbe le funzioni del **Computer Emergency Response Team nazionale (CERT)** e del **CERT-PA** ed è disciplinato da DPCM entro il 9 novembre 2018. Il CSIRT ha compiti di natura prevalentemente tecnica: definisce le procedure per prevenire e gestire i rischi informatici; riceve le notifiche di incidente da parte degli OSE e le inoltra alle autorità competenti e al punto di contatto unico; e supporta il soggetto notificante fornendo le informazioni e l'exptertise per facilitare la gestione efficace dell'evento e la minimizzazione delle ripercussioni.
A livello nazionale, la centralizzazione e la decisione di fondere in un unico ufficio la prevenzione, risposta e recovery degli incidenti informatici rappresenta un punto di svolta importante. Da una parte, tale decisione riconosce l'interdipendenza tra i vari settori e dunque la necessità di un sistema di coordinazione efficace e di comunicazione veloce e capillare. Dall'altra, crea un'operatività maggiormente coesa tra settore pubblico e privato.

Il CSIRT italiano partecipa inoltre alla **rete CSIRT**, composta dagli omologhi computer response team dei paesi membri e dal CERT europeo, scambiando informazioni rilevanti riguardo agli incidenti informatici, fornendo sostegno agli stati membri, condividendo orientamenti e best practice e individuando forme di intervento combinato (art. 11). Come specificato dall'art. 12 della direttiva, la rete di CSIRT è costituita al fine di sviluppare fiducia tra gli stati membri e di promuovere una cooperazione operativa efficace. Occorre precisare che, come previsto comma 10 dell'art. 12, nelle sue attività di interscambio il CSIRT italiano preserva "la sicurezza e gli interessi economici dell'OSE, nonché la riservatezza delle informazioni fornite".

5. Cultura sicurezza e gestione del rischio

Tra i suoi obbiettivi, il decreto vuole diffondere una **cultura di sicurezza e gestione del rischio in ambito cyber** e di protezione delle reti. La nuova disciplina inquadra il tema della cyber-security come un requisito non solo del singolo ma dell'intera comunità, da cui deriva la necessità di introdurre sistemi di educazione e sensibilizzazione. In tal senso, il sistema di notifica degli incidenti (artt. 12; 14) che prevede un meccanismo di autodenuncia segnala il conferimento di grande responsabilità agli operatori e fornitori di servizi digitali. Inoltre, la notifica volontaria, che dà la possibilità di riportare incidenti rilevanti anche ai soggetti non direttamente classificati come OSE o FSD (art. 18), rappresenta la volontà del legislatore di promuovere un'effettiva campagna educativa per sviluppare consapevolezza e cultura del rischio, confermata dalle tante disposizioni che spingono i nuovi organi istituzionali competenti a svolgere attività di ricerca, sviluppo di best practice e promozione di training e altre iniziative formative. Tali attività vengono inoltre indicate quali elementi essenziali nell'ambito della strategia nazionale di sicurezza cibernetica (art. 6).

6. Quali sono i passi successivi?

Per rendere effettive e funzionanti le disposizioni del decreto sono necessari ulteriori interventi normativi e istituzionali. In attuazione della direttiva europea, l'art. 6 del decreto prevede l'adozione di una **strategia nazionale di sicurezza cibernetica** da parte del Presidente del Consiglio dei ministri e in collaborazione con il Comitato Interministeriale per la Sicurezza della Repubblica (CISR). In realtà, il Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico del 2013 e il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica del 2017, hanno già tracciato alcune linee guida per una strategia nazionale. Tuttavia, per ottemperare agli obblighi europei è necessaria l'adozione di un nuovo documento che contenga specifici elementi come l'identificazione di obbiettivi e priorità in ambito di sicurezza delle reti, il quadro di strumenti e strutture per conseguirli, un piano di valutazione dei rischi e le misure per migliorare la collaborazione tra settore pubblico e privato e per diffondere formazione e sensibilizzazione sulla cyber-security. Tale strategia deve essere trasmessa alla Commissione Europea entro tre mesi dalla sua adozione.

Un altro passaggio necessario per l'applicazione effettiva del decreto riguarda la redazione di una lista esaustiva degli OSE operanti sul territorio nazionale. L'identificazione degli operatori essenziali è carico delle autorità competenti NIS e dovrebbe essere finalizzata entro il 9 novembre 2018. Parallelamente, un **elenco intersettoriale di OSE** dovrebbe essere redatto e depositato presso il Ministero dello sviluppo economico.
Infine, sempre entro il 9 novembre 2018, il Presidente del Consiglio dei ministri è tenuto ad adottare un decreto per regolamentare l'organizzazione e il funzionamento del CSIRT, le cui funzioni, in attesa della disciplina richiesta, verranno svolte congiuntamente dal CERT nazionale e dal CERT-PA in collaborazione tra loro. ©

RIFERIMENTI

[1] Direttiva NIS 2016/1148 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148&from=IT
[2] D.Lgs. 8 maggio 2018, n. 65 http://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg
[3] La NIS in pillole (22 giugno 2018) https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cyber-la-nis-entra-in-vigore-litalia-si-rafforza-e-fa-rete-con-lue.html.