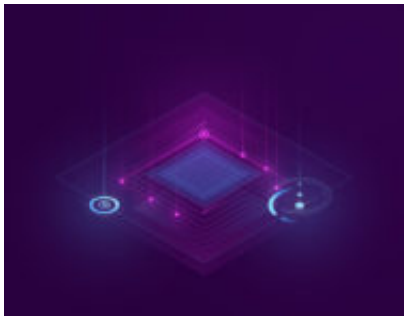
La Direttiva NIS e il DDL Sicurezza Cibernetica: un piccolo confronto

Author : Federica Maria Calì

Date : 24 Settembre 2019



Vista la crescente dipendenza della vita quotidiana e delle economie dalle tecnologie digitali, i cittadini sono sempre più esposti a gravi incidenti informatici. Per far fronte alle sfide crescenti, l'Unione Europea ha intensificato le sue attività nel settore della sicurezza informatica, promuovendo un **ecosistema cibernetico sicuro** e affidabile.

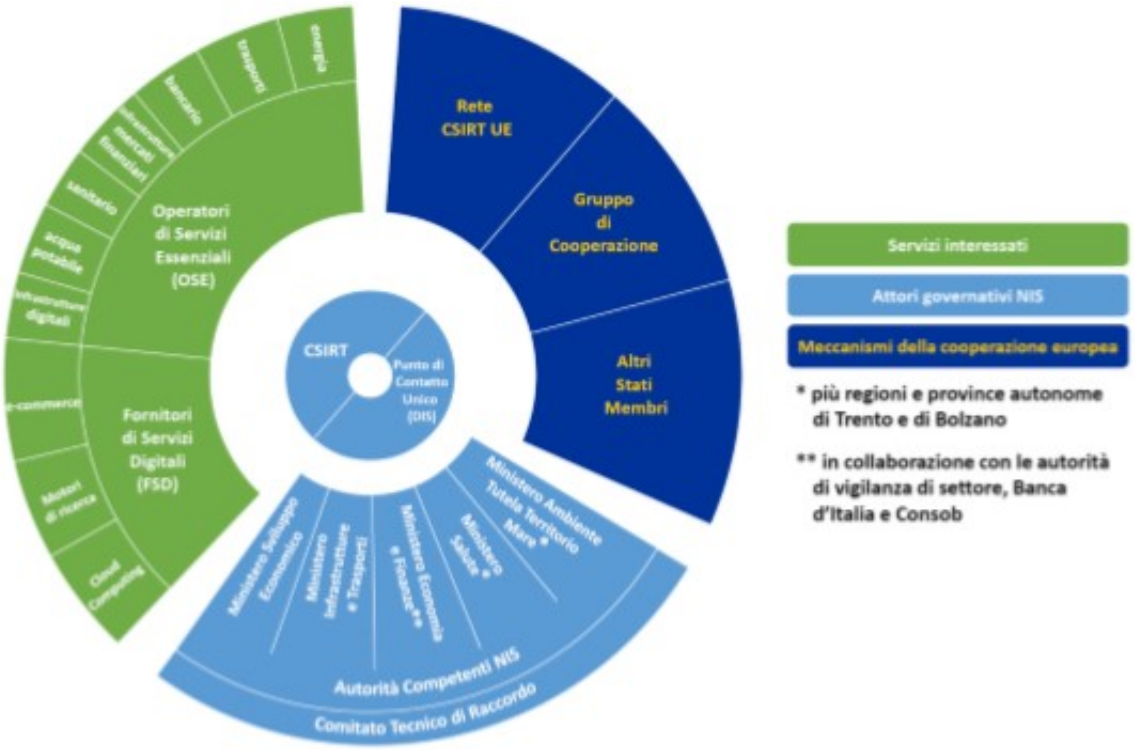
Nel 2016 infatti l'Unione ha adottato le sue prime misure nel settore della cybersicurezza attraverso la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio sulla sicurezza delle reti e dei sistemi informativi, la così detta **Direttiva NIS** (*Network and Information Security*). Questa è stata recepita dall'Italia con il decreto legislativo n.65/2018 pubblicato sulla Gazzetta Ufficiale il 9 giugno ed effettivo dal 24 giugno.

La direttiva è volta a migliorare le difese delle **infrastrutture critiche** degli Stati membri, puntando su *intelligence* e prevenzione per raggiungere un adeguato livello di sicurezza cibernetica e di resilienza dei sistemi critici nazionali. L'obiettivo è quello di creare misure volte a garantire un elevato livello comune di sicurezza delle reti e delle informazioni che sia uniforme in tutta l'Unione europea. Ciò, attraverso l'adozione di misure tecniche e organizzative che consentano di ridurre i rischi e l'impatto degli incidenti informatici.
In quest'ottica, la Direttiva si sviluppa su **tre piani:**

- promuovere la cultura della gestione del rischio e della segnalazione degli incidenti tra i principali attori economici, in particolare tra gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali, così come tra i fornitori di servizi digitali;
- migliorare le capacità nazionali in materia di sicurezza cibernetica;
- rafforzare la cooperazione in questo settore a livello nazionale e in ambito europeo.

L'applicazione della direttiva NIS riguarda principalmente le aziende che verranno identificate come Operatori di servizi essenziali **(OSE)** o Fornitori di servizi digitali **(FSD)**.

Tanto gli OSE che gli FSD sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio. Hanno inoltre l'obbligo di notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante,rispettivamente sulla continuità e sulla fornitura del servizio, al *Computer Security Incident Response Team* **(CSIRT)** italiano, informandone anche l'Autorità competente NIS di riferimento.



I soggetti giuridici non identificati come OSE e che non sono FSD possono inoltrare al CSIRT notifiche volontarie degli incidenti che abbiano un impatto rilevante sulla continuità dei servizi da loro erogati. Ciò poiché l'intento della Direttiva NIS e del relativo decreto di recepimento è quello di favorire la più ampia **diffusione di una consapevole cultura nel campo della cybersecurity** e di un conseguente accrescimento dei relativi livelli di sicurezza, anche attraverso un maggiore scambio di informazioni.

Il decreto 65/2018 resta molto fedele al testo della direttiva europea e identifica **otto settori** di intervento: energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile, infrastrutture digitali, servizi digitali (quali motori di ricerca, servizi *cloud* e piattaforme di commercio elettronico).

Si prevede, inoltre, l'istituzione presso la Presidenza del Consiglio dei Ministri di un unico Computer Security Incident Response Team, detto CSIRT italiano, che andrà a sostituire, fondendoli, gli attuali CERT Nazionale (operante presso il Ministero dello Sviluppo Economico) e CERT-PA (operante presso l'Agenzia per l'Italia Digitale).

Gli **operatori di servizi essenziali** dovranno adottare misure tecnico-organizzative “adeguate” alla gestione dei rischi e alla prevenzione degli incidenti informatici. Il decreto specifica che nell’adottare tali misure gli operatori dovranno tenere in debita considerazione le linee guida che sono state recentemente predisposte dal Gruppo di Cooperazione. Le autorità competenti NIS potranno inoltre imporre l’adozione di misure di sicurezza specifiche, sentiti gli operatori di servizi essenziali.

Analoghi obblighi in materia di sicurezza sono previsti a carico dei **fornitori di servizi digitali**, i quali dovranno adottare misure tecniche-organizzative per la gestione dei rischi e per la riduzione dell’impatto di eventuali incidenti informatici.

Per l’adozione di tali misure i soggetti coinvolti possono utilizzare *framework* come quello elaborato dal NIST U.S. (l’Istituto Nazionale degli Standard e della Tecnologia), o la certificazione ISO 27001, quali soluzioni di *best practice*, allo scopo di valutare il loro livello di sicurezza IT e impostare obiettivi per migliorare le procedure utilizzate per proteggere i dati sensibili. I livelli del *Cybersecurity framework* (parziale, consapevole del rischio informatico, replicabile e adattivo) spiegano quanto deve essere profonda l’implementazione della sicurezza informatica e con riferimento alle categorie e sottocategorie, è possibile stabilire dove siano le lacune e scegliere i piani d’azione più adeguati per colmarle. La ISO 27001 adotta un approccio più ampio poichè la sua metodologia si basa sul **ciclo *Plan-Do-Check-Act* (PDCA)**, ovvero costruire un sistema di gestione che non solo progetta e implementa la cyber security, ma mantiene e migliora anche l’intero sistema di gestione delle informazioni.

Tornando alla Direttiva NIS, in ossequio a quanto richiesto dall’articolo 7, il decreto di recepimento prevede l’adozione di una strategia nazionale di sicurezza cibernetica da parte del Presidente del Consiglio dei Ministri. La strategia dovrà prevedere in particolare le **misure di preparazione, risposta e recupero dei servizi** a seguito di incidenti informatici, la definizione di un piano di valutazione dei rischi informatici e programmi di formazione e sensibilizzazione in materia di sicurezza informatica.

Così nel mese di luglio 2019 il nostro Paese ha visto, da un lato, la realizzazione e la diffusione delle *Linee guida per* gli OSE in ambito NIS e, dall’altro, lo *“Schema di disegno di legge in materia di perimetro di sicurezza nazionale cibernetica*”. Tutti questi interventi legislativi sembrerebbero tessere di un mosaico che si colloca in maniera coerente con l’evoluzione che ormai da tempo si sta ravvisando nello scenario nazionale e internazionale in tema di cyber security e sicurezza delle informazioni.

Il Consiglio dei Ministri ha infatti approvato proprio qualche giorno fa un disegno di legge in materia di **perimetro di sicurezza nazionale cibernetica** per "*assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l’esercizio di una funzione o servizio essenziale dello Stato per il mantenimento di attività civili, sociali o economiche fondamentali e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale".*

A questo scopo, **il disegno di legge prevede:**

1. la definizione delle finalità del perimetro e delle modalità di individuazione dei soggetti pubblici e privati che ne fanno parte, nonché delle rispettive reti, dei sistemi informativi e dei servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica per i quali si applicano le misure di sicurezza e le procedure introdotte;
2. l'istituzione di un meccanismo teso ad assicurare un *procurement* più sicuro per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi ICT destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti;
3. l'individuazione delle competenze del Ministero dello sviluppo economico – per i soggetti privati inclusi nel perimetro – e dell'Agenzia per l'Italia Digitale (AgID) – per le amministrazioni pubbliche;
4. l'istituzione di un sistema di vigilanza e controllo sul rispetto degli obblighi introdotti;
5. lo svolgimento delle attività di ispezione e verifica da parte delle strutture specializzate in tema di protezione di reti e sistemi nonché, per quanto riguarda la prevenzione e il contrasto del crimine informatico, delle Amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti.

Le **conseguenze** dell' approvazione di questa legge saranno numerose: questo infatti potrebbe rappresentare il primo vero momento di diffusione delle buone pratiche di *security by design* e *by default*. Alla aziende, alle PA si chiederà un nuovo sforzo di **cambio di mentalità** e un forte impegno nello studio di soluzioni sostenibili e intelligenti per promuovere il progresso, la tecnologia, lo sviluppo e la sicurezza.

In tale ottica e con gli attuali scenari presenti, l'asse della sicurezza si sta spostando da un punto di vista solo fisico ad un **approccio olistico** alla cybersecurity.

La sicurezza fisica delle infrastrutture è fondamentale ma anche la sicurezza cibernetica non deve essere sottovalutata.

Un problema della cybersecurity è che questa non ha **confini** spaziali e temporali. Se devo compiere un furto fisico devo necessariamente farlo sul posto; viene fatto una sola volta e da una sola entità. Un furto informatico, invece, può attuarsi da qualsiasi posto nel mondo - anche più volte –, possono esserci diversi attaccanti ed è possibile compiere, nello stesso tempo, più furti nei confronti di più soggetti.

A cura di **Federica Calì** e **Stefano Gorla**