COMMISSIONE
EUROPEA

Bruxelles, 4.10.2017
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Sfruttare al meglio le reti e i sistemi informativi – verso l'efficace attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

IT

Introduzione

La direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi nell'Unione (di seguito "la direttiva NIS" o "la direttiva")[1] adottata il 6 luglio 2016 è la prima legislazione orizzontale dell'UE ad affrontare le sfide in materia di cibersicurezza, che ha davvero rivoluzionato la resilienza e la cooperazione in termini di cibersicurezza in Europa.

La direttiva ha tre obiettivi principali:

- migliorare le capacità nazionali di cibersicurezza;
- rafforzare la cooperazione a livello dell'UE;
- promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e i fornitori di servizi digitali.

La direttiva NIS costituisce una pietra angolare nella risposta dell'UE alle crescenti minacce e sfide cibernetiche che accompagnano la digitalizzazione della nostra vita economica e sociale; la sua attuazione è pertanto una parte essenziale del pacchetto sulla cibersicurezza presentato il 13 settembre 2017. L'efficacia della risposta dell'UE è inibita fino al pieno recepimento della direttiva NIS in tutti gli Stati membri dell'Unione, fattore riconosciuto come punto critico anche nella comunicazione del 2016 della Commissione "Rafforzare il sistema di resilienza informatica"[2].

La novità della direttiva NIS e l'urgenza di far fronte al panorama in rapida evoluzione delle ciberminacce richiedono di porre particolare attenzione alle sfide che tutti gli attori si trovano di fronte nel garantire il recepimento tempestivo e riuscito della direttiva. In vista del termine di recepimento del 9 maggio 2018 e del termine per l'identificazione degli operatori di servizi essenziali del 9 novembre 2018, la Commissione sostiene da tempo il processo di recepimento da parte degli Stati membri e il lavoro da questi svolto a tal fine nel gruppo di cooperazione.

La presente comunicazione, con il relativo allegato, si basa sui lavori preparatori e sulle analisi della Commissione riguardanti l'attuazione della direttiva NIS fino ad ora, sul contributo dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) e sulle discussioni tenute con gli Stati membri nella fase di recepimento della direttiva, in particolare in sede di gruppo di cooperazione[3]. La presente comunicazione integra i considerevoli sforzi profusi finora, in particolare attraverso:

- l'intenso lavoro del gruppo di cooperazione, che ha convenuto un piano di lavoro concentrato soprattutto sul recepimento della direttiva NIS, in particolare sull'identificazione degli operatori di servizi essenziali e sui loro obblighi di sicurezza e di notifica degli incidenti. Sebbene la direttiva preveda la discrezionalità nel

[1] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. La direttiva è entrata in vigore l'8 agosto 2016.
[2] COM(2016) 410 final.
[3] Meccanismo di cooperazione strategica tra gli Stati membri nell'ambito della direttiva NIS, articolo 11.

recepimento delle disposizioni riguardanti gli operatori di servizi essenziali, gli Stati membri hanno riconosciuto l'importanza di un approccio armonizzato al riguardo[4];

- l'istituzione e l'operatività in tempi brevi della rete composta dai gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) in conformità all'articolo 12, paragrafo 1, della direttiva. Nel frattempo detta rete ha iniziato a gettare le fondamenta per una cooperazione operativa strutturata a livello europeo.

Per i livelli sia strategico che operativo rappresentati da tali due strutture, il pieno coinvolgimento di tutti gli Stati membri è essenziale al fine di raggiungere l'obiettivo di un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

La presente comunicazione con il relativo allegato rafforzerà le iniziative in tal senso raccogliendo e confrontando le migliori pratiche provenienti dagli Stati membri che sono pertinenti ai fini dell'attuazione della direttiva, fornendo ulteriori orientamenti sul modo in cui la direttiva dovrebbe essere attuata e proponendo spiegazioni più dettagliate su disposizioni specifiche. L'obiettivo generale è sostenere gli Stati membri nel raggiungere un'attuazione efficace e armonizzata della direttiva NIS in tutta l'UE.

La presente comunicazione sarà ulteriormente integrata dall'imminente regolamento di esecuzione della Commissione concernente l'ulteriore specificazione degli elementi e dei parametri relativi agli obblighi di sicurezza e di notifica degli incidenti imposti ai fornitori di servizi digitali, adottato a norma dell'articolo 16, paragrafo 8, della direttiva NIS. Il regolamento di esecuzione faciliterà l'attuazione della direttiva in relazione agli obblighi riguardanti i fornitori di servizi digitali[5].

La presente comunicazione espone le conclusioni fondamentali dell'analisi delle questioni che sono considerate punti di riferimento importanti e potenziali fonti di ispirazione dal punto di vista del recepimento nel diritto nazionale. In tale contesto l'attenzione è rivolta principalmente alle disposizioni relative alle capacità e agli obblighi degli Stati membri per quanto riguarda i soggetti che rientrano nell'ambito di applicazione della direttiva. L'allegato presenta un esame più dettagliato dei settori in cui la Commissione ravvisa il valore maggiore nel fornire orientamenti pratici per il recepimento; quest'esame si articola nella spiegazione e interpretazione di determinate disposizioni della direttiva e nella presentazione di migliori pratiche e dell'esperienza maturata con la direttiva fino ad ora.

[4] Il gruppo di cooperazione sta attualmente lavorando a documenti orientativi di riferimento che riguardano tra gli altri aspetti: i criteri che definiscono la criticità di un operatore a norma dell'articolo 5, paragrafo 2, della direttiva; le circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti in base all'articolo 14, paragrafo 7, della direttiva; gli obblighi di sicurezza per gli operatori di servizi essenziali, in linea con l'articolo 14, paragrafi 1 e 2.

[5] La bozza del regolamento di esecuzione è disponibile per consultazione pubblica all'indirizzo https://ec.europa.eu/info/law/better-regulation/have-your-say_en.

Verso l'efficace attuazione della direttiva NIS

L'obiettivo della direttiva NIS è raggiungere un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'UE. Questo presuppone il miglioramento della sicurezza di internet e delle reti e dei sistemi informativi privati su cui si fonda il funzionamento della nostra società e della nostra economia. Il primo elemento importante a tal riguardo è la preparazione degli Stati membri, che dovrebbe essere garantita dalla predisposizione di strategie nazionali di cibersicurezza, come descritto nella direttiva, dal lavoro dei CSIRT e da quello delle autorità nazionali competenti.

Portata generale delle strategie nazionali

È importante che gli Stati membri colgano l'opportunità del recepimento della direttiva NIS per esaminare la loro strategia nazionale di cibersicurezza alla luce delle lacune, delle migliori pratiche e delle nuove sfide trattate nell'allegato.

Benché la direttiva si concentri comprensibilmente sulle imprese e sui servizi di particolare importanza critica, è la cibersicurezza dell'economia e della società nel complesso che deve essere affrontata da una prospettiva d'insieme e in modo coerente, vista la sempre maggiore dipendenza dalle TIC. L'adozione di strategie nazionali di portata generale che vanno oltre i requisiti minimi della direttiva (contemplando altri settori e servizi oltre a quelli elencati rispettivamente negli allegati II e III della direttiva) aumenterebbe pertanto il livello complessivo di sicurezza delle reti e dei sistemi informativi.

Visto che la cibersicurezza è ancora un settore dell'ordine pubblico relativamente nuovo e in rapida espansione, nella maggior parte dei casi sono necessari nuovi investimenti, anche se la situazione complessiva delle finanze pubbliche richiede tagli e risparmi. Prendere decisioni ambiziose volte ad assicurare le adeguate risorse finanziarie e umane indispensabili per l'efficace attuazione delle strategie nazionali, compresa l'assegnazione di risorse sufficienti alle autorità nazionali competenti e ai CSIRT, è pertanto fondamentale per il raggiungimento degli obiettivi della direttiva.

Efficacia dell'attuazione e del controllo

La necessità di designare autorità nazionali competenti e punti di contatto unici, delineata nell'articolo 8 della direttiva, costituisce un elemento chiave al fine di garantire un'attuazione efficace della direttiva NIS e della cooperazione transfrontaliera. Al riguardo negli Stati membri sono emersi approcci sia centralizzati che decentrati. Quando gli Stati membri adottano un approccio più decentrato in termini di designazione delle autorità nazionali competenti, si è dimostrata essenziale la definizione di solidi accordi di cooperazione tra numerose autorità e il punto di contatto unico (*cfr. tabella 1 della sezione 3.2 dell'allegato*). Si aumenterebbe così l'efficacia dell'attuazione e si faciliterebbe il controllo del rispetto delle norme.

Attingere all'esperienza pregressa maturata con la protezione delle infrastrutture critiche informatizzate (CIIP) potrebbe contribuire a progettare un modello ottimale di governance per

gli Stati membri, garantendo sia un'efficace attuazione settoriale della direttiva NIS sia un approccio orizzontale coerente (*cfr. sezione 3.1 dell'allegato*).

Capacità rafforzata dei CSIRT nazionali

Senza CSIRT nazionali efficaci e dotati di risorse adeguate in tutta l'UE, come stabilito nell'articolo 9 della direttiva NIS, l'UE rimarrà troppo vulnerabile alle ciberminacce transfrontaliere. Gli Stati membri potrebbero pertanto prendere in considerazione l'estensione dell'ambito di applicazione dei CSIRT oltre i settori e i servizi inclusi nell'ambito di applicazione della direttiva (*cfr. sezione 3.3 dell'allegato*). Una scelta in tal senso consentirebbe ai CSIRT nazionali di fornire sostegno operativo in caso di ciberincidenti che si verificano presso imprese e organizzazioni che non rientrano nell'ambito di applicazione della direttiva ma che sono comunque importanti per la società e l'economia. Inoltre, gli Stati membri potrebbero usare appieno le opportunità di finanziamento supplementare offerte dal programma delle infrastrutture di servizi digitali (DSI) per la cibersicurezza del Meccanismo per collegare l'Europa (MCE), concepito per consolidare le capacità dei CSIRT nazionali e la cooperazione fra di essi (*cfr. sezione 3.5 dell'allegato*).

Coerenza del processo di identificazione degli operatori di servizi essenziali

In conformità all'articolo 5 della direttiva NIS, gli Stati membri sono tenuti a identificare entro il 9 novembre 2018 i soggetti che saranno considerati operatori di servizi essenziali. In relazione a tale compito gli Stati membri potrebbero prendere in considerazione l'ipotesi di usare sistematicamente le definizioni e gli orientamenti inclusi nella presente comunicazione al fine di garantire che tipi di soggetti simili che svolgono un ruolo simile nel mercato interno siano identificati sistematicamente come operatori di servizi essenziali negli altri Stati membri. Gli Stati membri potrebbero altresì prendere in considerazione un'estensione dell'ambito di applicazione della direttiva NIS alle amministrazioni pubbliche, visto il ruolo che rivestono per la società e per l'economia nel complesso (*cfr. sezioni 2.1 e 4.1.3 dell'allegato*).

Allineare al massimo gli approcci nazionali all'identificazione degli operatori di servizi essenziali, in particolare seguendo gli orientamenti elaborati dal gruppo di cooperazione (*cfr. sezione 4.1.2 dell'allegato*) sarebbe molto utile, poiché comporterebbe un'applicazione più armonizzata delle disposizioni della direttiva, riducendo così il rischio di frammentazione del mercato. Nei casi in cui gli operatori di servizi essenziali forniscano servizi essenziali in due o più Stati membri, è essenziale impegnarsi per raggiungere, nel contesto del processo di consultazione di cui all'articolo 5, paragrafo 4, un accordo tra gli Stati membri sull'identificazione coerente dei soggetti (*cfr. sezione 4.1.7 dell'allegato*), in quanto eviterebbe un diverso trattamento normativo dello stesso soggetto nelle diverse giurisdizioni degli Stati membri.

Presentazione alla Commissione di informazioni sull'identificazione degli operatori di servizi essenziali

In conformità all'articolo 5, paragrafo 7, gli Stati membri sono tenuti a fornire alla Commissione informazioni riguardanti le misure nazionali che consentono l'identificazione degli operatori di servizi essenziali, un elenco dei servizi essenziali, il numero di tali operatori identificati e l'importanza di tali operatori per il settore. Gli Stati membri sono inoltre tenuti a fornire le soglie, se esistenti, utilizzate nel processo di identificazione al fine di determinare il livello di fornitura pertinente o l'importanza dello specifico operatore ai fini del mantenimento di un livello sufficiente di fornitura. Gli Stati membri potrebbero altresì prendere in considerazione la possibilità di condividere con la Commissione l'elenco degli operatori di servizi essenziali identificati, se necessario in via riservata, poiché questo contribuirebbe a migliorare l'accuratezza e la qualità della valutazione della Commissione (*cfr. sezioni 4.1.5 e 4.1.6 dell'allegato*).

Approcci allineati concernenti gli obblighi di sicurezza e di notifica degli incidenti imposti agli operatori di servizi essenziali

In relazione agli obblighi di sicurezza e di notifica degli incidenti imposti agli operatori di servizi essenziali (articolo 14, paragrafi 1, 2 e 3), un approccio allineato al riguardo, finalizzato a facilitare la conformità di tali operatori in tutti gli Stati membri dell'UE, promuoverebbe nella massima misura possibile un effetto di mercato unico. Il punto di riferimento rimane il lavoro su un documento d'indirizzo in sede di gruppo di cooperazione (*cfr. sezioni 4.2 e 4.3 dell'allegato*).

In caso di ciberincidente su larga scala che colpisce diversi Stati membri è molto probabile che una notifica obbligatoria dell'incidente venga inviata da un operatore di servizi essenziali o da un fornitore di servizi digitali a norma dell'articolo 14, paragrafo 3, e dell'articolo 16, paragrafo 3, o, su base volontaria a norma dell'articolo 20, paragrafo 1, da un altro soggetto che non rientra nell'ambito di applicazione della direttiva. In linea con la raccomandazione della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala, gli Stati membri potrebbero prendere in considerazione l'allineamento dei rispettivi approcci nazionali in modo da poter fornire il prima possibile informazioni pertinenti basate su tali notifiche alle autorità competenti o al CSIRT degli Stati membri interessati. Informazioni accurate e utilizzabili sarebbero vitali per ridurre il numero di infezioni o per risolvere le vulnerabilità prima che vengano sfruttate.

In uno spirito di partenariato per trarre il massimo dalla direttiva NIS, la Commissione intende estendere il sostegno erogato nell'ambito del Meccanismo per collegare l'Europa a tutte le parti interessate nell'ambito di tali norme. Sebbene l'attenzione sia stata rivolta verso la creazione di capacità dei CSIRT e verso una piattaforma che favorisca una rapida ed efficace cooperazione operativa, rafforzando così la rete dei CSIRT, la Commissione valuterà ora il modo in cui i finanziamenti nell'ambito del Meccanismo per collegare l'Europa possano

andare anche a vantaggio delle autorità nazionali competenti, degli operatori di servizi essenziali e dei fornitori di servizi digitali.

Conclusioni

In vista dell'imminente termine per il recepimento della direttiva NIS nella legislazione nazionale entro il 9 maggio 2018, e in vista del termine per l'identificazione degli operatori di servizi essenziali entro il 9 novembre 2018, gli Stati membri dovrebbero adottare misure atte a garantire che le disposizioni e i modelli di cooperazione di cui alla direttiva NIS siano in grado di fornire i migliori strumenti possibili a livello dell'UE per raggiungere un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. La Commissione invita gli Stati membri a tenere conto in tale processo delle informazioni, degli orientamenti e delle raccomandazioni contenuti nella presente comunicazione.

La presente comunicazione potrebbe essere ulteriormente integrata da altre azioni, comprese quelle generate tramite il lavoro in corso in sede di gruppo di cooperazione.