COMMISSIONE
EUROPEA

Bruxelles, 13.9.2017
COM(2017) 478 final

RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

sulla valutazione dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA)

1. INTRODUZIONE

1.1 INFORMAZIONI SULL'ENISA

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) è stata originariamente istituita nel 2004 e il suo mandato è stato rinnovato periodicamente. L'attuale mandato dell'ENISA è stabilito dal regolamento (UE) n. 526/2013[1] (di seguito: il "regolamento ENISA") che scadrà il 19 giugno 2020.

Il mandato dell'ENISA è di contribuire a garantire un elevato livello di sicurezza delle reti e dell'informazione nell'Unione. Il regolamento ENISA descrive gli obiettivi specifici dell'agenzia, stabilendo che essa:

- sviluppa e mantiene un elevato livello di competenza;
- assiste le istituzioni, gli organi e gli organismi dell'Unione nell'elaborazione delle politiche in materia di sicurezza delle reti e dell'informazione;
- assiste le istituzioni, gli organi e gli organismi dell'Unione e gli Stati membri nell'attuazione delle politiche necessarie a soddisfare le prescrizioni legali e regolamentari in materia di sicurezza delle reti e dell'informazione previste dagli atti giuridici vigenti e futuri dell'Unione, contribuendo in tal modo al corretto funzionamento del mercato interno;
- assiste l'Unione e gli Stati membri per migliorare e per rafforzare la loro capacità e la loro preparazione a prevenire, rilevare e reagire ai problemi e agli incidenti legati alla sicurezza delle reti e dell'informazione;
- impiega la sua competenza per stimolare un'ampia cooperazione tra attori del settore pubblico e del settore privato.

Inoltre, con la direttiva (UE) 2016/1148[2] recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (di seguito: la "direttiva NIS"), i colegislatori dell'UE hanno deciso di attribuire compiti importanti all'ENISA nell'attuazione della normativa. In particolare, l'agenzia assicura le funzioni di segretariato della rete CSIRT (istituita per promuovere una collaborazione operativa rapida ed efficace tra gli Stati membri) ed è inoltre chiamata ad assistere il gruppo di cooperazione per la cooperazione strategica nell'esecuzione dei suoi compiti. Infine la direttiva NIS prevede che l'ENISA assista gli Stati membri e la Commissione mettendo a disposizione le proprie competenze e fornendo consulenze, nonché agevolando lo scambio di buone pratiche.

L'agenzia ha sede in Grecia: la sede amministrativa è a Heraklion (Creta) e il centro operativo ad Atene. Il personale dell'agenzia conta 84 dipendenti e il suo bilancio operativo annuale è di 11,25 milioni di EUR. Ne è a capo un direttore esecutivo ed è gestita da un consiglio di amministrazione, un comitato esecutivo e dal gruppo permanente di parti interessate. Una rete informale di funzionari nazionali di collegamento facilita il coinvolgimento degli Stati membri.

---

[1] http://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1495472820549&uri=CELEX%3A32013R0526

[2] http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

1.2 FINALITÀ DELLA RELAZIONE

L'articolo 32 del regolamento ENISA impone alla Commissione di procedere a una valutazione dell'agenzia entro il 20 giugno 2018, "*per esaminare, in particolare, l'impatto, l'efficacia e l'efficienza dell'Agenzia e le sue metodologie di lavoro*" e per valutare l'eventuale necessità di una proroga dell'attuale mandato.

Nella comunicazione del 2016 "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza"[3], la Commissione ha annunciato che intendeva anticipare la valutazione e il riesame dell'ENISA, e ciò alla luce dei notevoli cambiamenti intervenuti nel panorama della cibersicurezza dal 2013, quando è stato adottato l'attuale regolamento ENISA, e del livello di maturità raggiunto a livello politico, di mercato e tecnologico. La Commissione ha osservato in particolare che il riesame dell'ENISA sarebbe l'occasione per un possibile miglioramento delle competenze e delle capacità dell'agenzia di aiutare gli Stati membri in modo sostenibile ad acquisire ciberresilienza.

Questa visione è stata ulteriormente confermata nelle conclusioni del Consiglio[4] del 2016, che hanno riconosciuto che "*le vulnerabilità e le minacce informatiche continuano a evolversi e a intensificarsi. Ciò richiederà una cooperazione costante e più stretta, in particolare nella gestione degli incidenti transfrontalieri e su vasta scala in materia di cibersicurezza*". Le conclusioni hanno ribadito che "*il regolamento ENISA è uno degli elementi centrali del quadro per la ciberresilienza dell'UE*".

I risultati della valutazione dell'ENISA sono confluiti nella valutazione d'impatto che accompagna la proposta di regolamento del Parlamento europeo e del Consiglio relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) 526/2013, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (''regolamento sulla cibersicurezza'').

Ai sensi dell'articolo 32 del regolamento ENISA la Commissione trasmette la relazione di valutazione, unitamente alle proprie conclusioni, al Parlamento europeo, al Consiglio e al consiglio di amministrazione. Questa relazione di sintesi è accompagnata dal documento di lavoro dei servizi della Commissione sulla valutazione dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (SWD(2017) 502).

2. PRINCIPALI RISULTATI DELLA VALUTAZIONE

In conformità agli orientamenti della Commissione per legiferare meglio[5], la valutazione ha esaminato l'efficienza, l'efficacia, la coerenza, la pertinenza e il valore aggiunto europeo dell'agenzia, tenendo conto della performance, della governance, della struttura organizzativa interna e dei metodi di lavoro.

L'analisi ha tenuto conto anche degli sviluppi del contesto in cui opera attualmente l'agenzia, in particolare per quanto riguarda: il nuovo quadro normativo e politico dell'UE (ad esempio, la direttiva NIS, il riesame della strategia dell'UE per la cibersicurezza); l'evoluzione delle esigenze della comunità dei portatori di interessi

[3] Comunicazione della Commissione "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza" (COM(2016) 0410 final).

[4] Conclusioni del Consiglio "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza" del 15 novembre 2016.

[5] COM(2015) 215 final e SWD(2015) 111 final; http://ec.europa.eu/smart-regulation/guidelines/docs/swd_br_guidelines_en.pdf

dell'agenzia; la complementarità e le sinergie possibili con il lavoro condotto da altre istituzioni, organi e organismi dell'UE e nazionali, come il Gruppo di intervento per la sicurezza informatica in caso di incidente delle istituzioni, organi e organismi dell'UE (CERT-UE) e il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol.

Per valutare il funzionamento dell'agenzia:

- la Commissione ha richiesto uno studio indipendente, svolto da novembre 2016 a luglio 2017, che, insieme all'analisi interna effettuata dalla Commissione, costituisce la fonte principale di valutazione;
- le attività dello studio includevano ricerche a tavolino, la raccolta e l'analisi di dati, comprese indagini presso i portatori di interessi, interviste approfondite con soggetti chiave nel settore della cibersicurezza, un seminario con i portatori di interessi e, l'analisi comparativa, un esercizio di posizionamento dell'agenzia e un'analisi SWOT (punti di forza, debolezze, opportunità e minacce);
- la Commissione ha inoltre svolto una consultazione pubblica online della durata di 12 settimane, che verteva sia sulla valutazione *ex post* sia sul futuro dell'ENISA, nonché consultazioni mirate con i principali portatori di interessi.

Le principali conclusioni della valutazione, in base ai criteri di valutazione, possono essere sintetizzate come segue.

1. **Pertinenza:** tenuto conto degli sviluppi tecnologici e dell'evoluzione dei rischi e dell'esigenza significativa di una maggiore sicurezza delle reti e dell'informazione all'interno dell'UE, gli obiettivi dell'ENISA si sono dimostrati pertinenti. Infatti gli Stati membri e gli organi dell'UE fanno affidamento sulle competenze nel settore dell'evoluzione della sicurezza delle reti e dell'informazione. È inoltre necessario creare capacità negli Stati membri per capire e rispondere alle minacce e promuovere la cooperazione dei portatori di interessi nei vari ambiti tematici e nelle varie istituzioni. La sicurezza delle reti e dell'informazione continua a essere una priorità politica fondamentale dell'UE alla quale l'ENISA dovrebbe rispondere. Tuttavia la concezione dell'ENISA come agenzia dell'Unione europea con un mandato a tempo determinato: i) non consente la pianificazione a lungo termine e l'assistenza sostenibile agli Stati membri e alle istituzioni dell'UE nel contesto di rapida evoluzione delle minacce alla cibersicurezza; ii) può comportare un vuoto giuridico, in quanto le disposizioni della direttiva NIS che affidano compiti all'ENISA sono di natura permanente.

2. **Efficacia:** in generale l'ENISA ha raggiunto i propri obiettivi ed eseguito i propri compiti. Essa ha contribuito ad aumentare la sicurezza delle reti e dell'informazione mediante le sue attività principali (sviluppo della capacità, offerte di consulenza, creazione di comunità e sostegno alle politiche). L'agenzia ha inoltre mostrato di avere potenziale di miglioramento in ciascuna di esse. La valutazione ha concluso che l'ENISA ha creato efficacemente forti relazioni basate sulla fiducia con i portatori di interessi, in particolare con gli Stati membri e le comunità di CSIRT. Gli interventi nell'ambito dello sviluppo della capacità sono stati considerati efficaci, in particolare per gli Stati membri che dispongono di minori risorse. La promozione di una vasta cooperazione è stata uno degli elementi di spicco e i portatori di interessi hanno ampiamente concordato sul fatto che l'ENISA abbia avuto un ruolo positivo nel mettere in contatto le persone.

Tuttavia l'ENISA ha avuto difficoltà ad incidere profondamente nel vasto settore della sicurezza delle reti e dell'informazione. Ciò è stato anche dovuto al fatto che l'agenzia disponeva di risorse umane e finanziarie piuttosto limitate per adempiere a un mandato molto ampio. Dalla valutazione è inoltre emerso che l'ENISA ha soddisfatto parzialmente l'obiettivo di fornire competenze a causa dei problemi legati all'assunzione di esperti (cfr. anche la successiva sezione "Efficienza").

3. **Efficienza:** nonostante il modesto bilancio – uno dei più bassi tra le agenzie dell'UE – l'ENISA è stata in grado di contribuire a obiettivi mirati, dimostrando in generale un uso efficiente delle risorse. La valutazione ha concluso che i processi erano in generale efficienti e una chiara definizione delle responsabilità all'interno dell'organizzazione ha portato a una buona esecuzione dei lavori. Una delle sfide principali per l'efficienza dell'agenzia riguarda le difficoltà dell'ENISA di assumere e trattenere esperti altamente qualificati. Le conclusioni indicano che ciò può essere spiegato da una combinazione di fattori, tra cui la difficoltà generale in tutto il settore pubblico a competere con il settore privato nel tentativo di assumere esperti altamente specializzati, il principale tipo di contratto (a tempo determinato) che l'agenzia poteva offrire e il livello di attrattiva piuttosto basso dell'ubicazione dell'ENISA, ad esempio a causa delle difficoltà incontrate dai coniugi a trovare lavoro. Nonostante la suddivisione della sede tra Atene e Heraklion richieda un ulteriore impegno di coordinamento e generi costi aggiuntivi, il trasferimento ad Atene nel 2013 delle principali attività operative ha aumentato l'efficienza operativa dell'agenzia.

4. **Coerenza:** le attività dell'ENISA sono state generalmente coerenti con le politiche e le attività dei suoi portatori di interessi, a livello nazionale e dell'UE, ma è necessario un approccio più coordinato in materia di cibersicurezza a livello dell'UE. Il potenziale di cooperazione tra l'ENISA e gli altri organismi dell'UE non è stato interamente sfruttato. L'evoluzione del quadro giuridico e politico dell'UE rende oggi l'attuale mandato meno coerente.

5. **Valore aggiunto europeo:** il valore aggiunto dell'ENISA è consistito principalmente nella capacità dell'agenzia di migliorare la cooperazione, soprattutto tra gli Stati membri ma anche con le pertinenti comunità di sicurezza delle reti e dell'informazione. A livello dell'UE non vi sono altri soggetti che sostengono la cooperazione di una tale varietà di portatori di interessi nel settore della sicurezza delle reti e dell'informazione. Il valore aggiunto offerto dall'agenzia è variato a seconda delle diverse esigenze e delle risorse dei suoi portatori di interessi (ad esempio, Stati membri grandi rispetto a quelli piccoli; Stati membri rispetto al settore industriale) e alla necessità dell'agenzia di stabilire una priorità tra le proprie attività in base al programma di lavoro. La valutazione ha concluso che un'eventuale chiusura dell'ENISA costituirebbe un'occasione persa per tutti gli Stati membri. Non sarebbe possibile garantire il medesimo livello di comunità e di cooperazione tra gli Stati membri nel campo della cibersicurezza senza un'agenzia dell'UE decentrata. La situazione sarebbe più frammentata se il vuoto lasciato dall'ENISA fosse colmato da cooperazioni bilaterali o regionali.

3. CONCLUSIONI E RACCOMANDAZIONI

La valutazione ha concluso che il regolamento ENISA ha affidato all'agenzia un ampio mandato – che permette una certa flessibilità, ma in alcuni casi non risulta

sufficientemente preciso e non consente all'agenzia di avere un impatto significativo – i cui obiettivi si sono dimostrati rilevanti nel corso del periodo 2013-2016. L'agenzia è riuscita a raggiungere un buon livello di efficienza e ha dimostrato il valore aggiunto dell'azione a livello dell'UE, in particolare mediante attività essenziali, quali le esercitazioni paneuropee di cibersicurezza, il sostegno alle comunità di CSIRT, le analisi sul panorama delle minacce. L'ENISA ha contribuito ad aumentare la sicurezza delle reti e dell'informazione in Europa, principalmente attraverso il sostegno alla cooperazione tra gli Stati membri e i portatori di interessi nel settore della sicurezza delle reti e dell'informazione, nonché attraverso le sue attività di sviluppo della comunità e delle capacità.

L'agenzia ha raggiunto questi risultati nonostante le varie sfide presentate nelle precedenti sezioni della relazione e nel documento di lavoro dei servizi della Commissione allegato. Una delle sfide principali è collegata alle risorse limitate, che non corrispondono all'ampio mandato dell'agenzia, in particolare alla luce dei nuovi compiti che le ha attribuito la direttiva NIS e la rapida evoluzione del panorama delle minacce. L'ENISA rimane inoltre l'unica agenzia dell'UE con un mandato a tempo determinato, nonostante, tra l'altro, i compiti legati alla direttiva NIS, come indicato sopra.

Il panorama delle minacce informatiche è in rapida evoluzione e nuove minacce emergono continuamente nella misura in cui l'Europa diventa sempre più dipendente dalle infrastrutture e dai servizi digitali, non solo mediante dispositivi connessi ma ormai anche con l'onnipresenza della connettività. L'internet degli oggetti crea nuove opportunità legate all'efficienza energetica, alla protezione dell'ambiente, alla mobilità connessa, al monitoraggio della salute in tempo reale e alle operazioni finanziarie fluide nell'economia e nella società digitali. Tuttavia queste spinte commerciali sono accompagnate da vulnerabilità e lacune di sicurezza che possono portare a perturbazioni del mercato unico digitale da parte di dispositivi compromessi.

La valutazione ha portato alla conclusione che il presente mandato non fornisce all'ENISA gli strumenti necessari a far fronte alle sfide alla cibersicurezza attuali e future.

Inoltre vi è adesso un rischio crescente di aumento della frammentazione a livello dell'UE a causa del numero di soggetti dell'UE nel settore della cibersicurezza e dell'insufficiente coordinamento tra loro. L'UE ha bisogno di un punto di riferimento per affrontare le nuove minacce orizzontali con un impatto su molteplici settori industriali e per soddisfare le esigenze della comunità della cibersicurezza, in particolare gli Stati membri, le istituzioni dell'UE e le imprese. La valutazione indica che è necessaria un'agenzia dell'UE organizzata su base transettoriale/orizzontale con un mandato forte.

La valutazione dimostra che, nonostante una serie di questioni complesse, se dotata di un mandato forte e di sufficienti risorse finanziarie e umane, l'ENISA è potenzialmente in grado di apportare un contributo all'aumento della cibersicurezza nell'UE.

Vi è inoltre una chiara necessità di cooperazione e coordinamento tra i diversi portatori di interessi. La necessità di un coordinatore a livello dell'UE per agevolare i flussi di informazioni, ridurre al minimo le lacune ed evitare la sovrapposizione dei ruoli e delle responsabilità si fa sempre più forte. L'ENISA, in qualità di agenzia decentrata dell'UE e di intermediario neutrale, è in grado di coordinare l'approccio dell'UE nei confronti delle minacce informatiche.

In virtù di ciò, la Commissione ha presentato una proposta per riformare l'ENISA, affidandole un mandato permanente che si basa sui principali punti di forza mostrati dall'agenzia e sui nuovi settori prioritari d'intervento, ad esempio quello della certificazione della cibersicurezza. Questo nuovo mandato dovrebbe riflettere il cambiamento della realtà e conferire all'agenzia il potere di fornire un sostegno adeguato al futuro dell'UE.