Risposte del capo del comitato direttivo del CERT-UE, del CERT-UE e dell'ENISA alla relazione speciale della Corte dei conti europea sulla cibersicurezza delle istituzioni, degli organi e delle agenzie dell'Unione

1. Sintesi

Alla luce del continuo evolvere delle minacce informatiche, la cibersicurezza ha assunto un'importanza e una criticità di prim'ordine per le istituzioni, gli organi e le agenzie dell'Unione, che negli ultimi anni si sono rivelati un bersaglio sempre più frequente di ciberattacchi altamente sofisticati. Nel contesto dei rispettivi mandati, l'ENISA e il CERT-UE possono entrambi offrire un valido sostegno alla cibersicurezza di istituzioni, organi e agenzie dell'Unione a vari livelli. La proposta della Commissione Europea di un regolamento per stabilire misure volte al raggiungimento di un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e nelle agenzie dell'Unione è uno strumento chiave in questo contesto, fortemente sostenuto dall'ENISA, dal CERT-UE e dal capo del comitato direttivo del CERT-UE.

A questo scopo, l'ENISA, il CERT-UE e il capo del comitato direttivo del CERT-UE accolgono con favore la relazione speciale della Corte dei conti europea sulla cibersicurezza delle istituzioni, degli organi e delle agenzie dell'Unione, che arriva in un momento estremamente opportuno per valutare il livello di preparazione degli stessi nel loro complesso. La relazione sottolinea chiaramente il ruolo centrale che l'ENISA e il CERT-UE possono svolgere in questo ambito. La relazione, inoltre, delinea la necessità di impiegare ulteriori risorse e intraprendere azioni concrete mirate al miglioramento in materia di sicurezza informatica delle istituzioni, degli organi e delle agenzie dell'Unione.

Con questa comprensione, l'ENISA, il CERT-UE e il capo del comitato direttivo del CERT-UE sostengono le osservazioni e le raccomandazioni principali presenti nella relazione, che risultano in linea con le proposte legislative della Commissione europea nelle aree della cibersicurezza e della sicurezza delle informazioni nelle istituzioni, negli organi e nelle agenzie dell'UE.

I commenti presentati nella sezione seguente vogliono fornire ulteriori chiarimenti su alcune aree della relazione, soprattutto per quanto concerne le attività già svolte dall'ENISA e/o dal CERT-UE e

sulle azioni da loro previste, in particolare per lo sviluppo di capacità di cibersicurezza nelle istituzioni, gli organi e le agenzie dell'Unione. In merito alle raccomandazioni, l'ENISA e il CERT-UE accettano la raccomandazione 3 (Concentrare maggiormente l'interesse del CERT-UE e dell'ENISA sulle istituzioni, sugli organi e sulle agenzie dell'Unione meno maturi), a loro appositamente indirizzata.

2. Osservazioni principali

L'ENISA e il CERT-UE supportano le osservazioni principali della Corte dei conti. Detto questo, vengono di seguito presentati alcuni chiarimenti, soprattutto in merito alle azioni già intraprese dall'ENISA e/o dal CERT-UE e ai piani già stabiliti per le attività future.

Paragrafo 49

In merito alla richiesta formale inviata dal comitato consultivo sulle tecnologie dell'informazione e della comunicazione (ICTAC) al capo del comitato direttivo del CERT-UE sul diritto di voto nel comitato, desideriamo chiarire quanto segue:

Dato l'enorme impegno che avrebbe comportato una revisione dell'attuale accordo interistituzionale e dato che il lavoro in corso sul «Regolamento relativo a un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e nelle agenzie dell'Unione» affronta il tema della rappresentazione delle agenzie decentrate, si è concordato di risolvere formalmente la questione, in una prospettiva a lungo termine, attraverso il regolamento stesso. Fino a quel momento, come confermato dal capo del comitato direttivo, si continuerà a fare ricorso alle pratiche correnti e i rappresentanti dell'ICTAC saranno ancora invitati a dare voce alle proprie opinioni, che verranno considerate per quanto possibile e con equità.

Paragrafo 66

A fine 2021, l'ENISA ha stabilito un piano d'azione per lo svolgimento di esercitazioni di cibersicurezza che coinvolgono in modo specifico istituzioni, organi e agenzie dell'Unione. Il conseguente piano d'azione relativo alle formazioni per le istituzioni, gli organi e le agenzie dell'Unione verrà presentato nel primo trimestre del 2022.

Casella 3

Sebbene non esplicitamente menzionato tra i risultati operativi, l'ENISA ha fornito supporto operativo e ha collaborato con diverse istituzioni, organi e agenzie dell'Unione su richiesta di questi ultimi. Per esempio, nel 2018, in relazione all'obiettivo 2.2. Supportare l'attuazione delle politiche nell'Unione europea:

- la Banca centrale europea ha richiesto supporto nello sviluppo del quadro di riferimento per i test dei red team dell'Eurosistema;
- l'Agenzia dell'Unione europea per la sicurezza aerea ha richiesto supporto per lo sviluppo degli obiettivi del centro europeo per la cibersicurezza nell'aviazione (ECCSA), per aumentare la consapevolezza in materia di cibersicurezza e per implementare la direttiva NIS a livello settoriale;
- l'Agenzia dell'Unione europea per le ferrovie ha richiesto supporto nell'implementazione della direttiva NIS nel settore ferroviario, in particolare per lo sviluppo di un centro di condivisione e di analisi delle informazioni (ISAC) per gestori dell'infrastruttura e imprese ferroviarie, nonché per lo sviluppo delle capacità (organizzazione di sessioni di formazione e informazione);
- l'ENISA ha supportato l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) nel miglioramento delle proprie competenze in materia di cibersicurezza e continuità operativa. In particolare, l'ENISA ha messo a disposizione le proprie competenze per l'organizzazione di esercitazioni e lo sviluppo di scenari, oltre a offrire all'eu-LISA una versione completamente sviluppata della piattaforma ENISA CEP con l'obiettivo di organizzare un'esercitazione per valutare la preparazione di uno dei sistemi informatici vitali per l'Unione europea.

Inoltre, dal 2019 l'ENISA collabora attivamente con istituzioni, organi e agenzie dell'Unione (per esempio ERA, EMSA, AESA, ACER), nell'ambito dell'applicazione della direttiva NIS, allo sviluppo di conoscenze settoriali, allo svolgimento di attività volte ad aumentare la consapevolezza in materia di cibersicurezza e a iniziative settoriali.

Paragrafo 71

L'ENISA ha sviluppato nel 2021 e presenterà nel 2022 una formazione specializzata dal titolo «How to Build an Awareness Program & Using table Top Exercises» indirizzata in modo specifico alle istituzioni, agli organi e alle agenzie dell'Unione. Nel contesto della loro cooperazione strutturata, nel 2022 l'ENISA e il CERT-UE forniranno congiuntamente anche alle istituzioni, agli organi e alle agenzie dell'Unione.

Paragrafo 72

Va notato che le esercitazioni di cibersicurezza dell'ENISA hanno obiettivi ampi e un pubblico eterogeneo, che comprende anche le istituzioni, gli organi e le agenzie dell'Unione. Questo approccio consente di affrontare le diverse necessità delle istituzioni, degli organi e delle agenzie dell'Unione, che possono beneficiare enormemente di tali esercitazioni svolte con rappresentanti degli Stati membri. Va notato inoltre che l'ENISA coinvolge il personale tecnico delle istituzioni, degli organi e delle agenzie dell'Unione nelle esercitazioni Cyber Europe fin dal 2016, sotto la guida del CERT-UE che ne è il principale preparatore. In continuazione di questi impegni, l'ENISA prevede, nella propria strategia per le esercitazioni 2022, sotto le attività per lo sviluppo di capacità, un nuovo prodotto per le esercitazioni che verrà fornito con il sostegno del CERT-UE e che consentirà alle istituzioni, agli organi e alle agenzie dell'UE di imparare a condurre esercitazioni basate sull'autovalutazione.

3. Conclusioni e raccomandazioni

L'ENISA e il CERT-UE accettano la raccomandazione 3 (Concentrare maggiormente l'interesse del CERT-UE e dell'ENISA sulle istituzioni, sugli organi e sulle agenzie dell'Unione meno maturi), indirizzato appositamente a queste due entità.