RISPOSTE DELLA COMMISSIONE EUROPEA

ALLA RELAZIONE SPECIALE DELLA CORTE DEI CONTI EUROPEA

Cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE: il livello di preparazione generale non è commisurato alle minacce

IT

IT

Indice

I. SINTESI DELLE RISPOSTE DELLA COMMISSIONE 2

a) Introduzione generale 2

b) Posizione della Commissione sulle principali osservazioni e raccomandazioni della Corte 2

c) Ultimi sviluppi di rilievo e prossime tappe 3

II. RISPOSTE DELLA COMMISSIONE ALLE PRINCIPALI OSSERVAZIONI DELLA CORTE DEI CONTI 3

1. Livelli di maturità degli EUIBA per quanto riguarda la cibersicurezza 3

2. Meccanismi di cooperazione degli EUIBA 4

3. Condivisione di informazioni su incidenti significativi o vulnerabilità 5

III. RISPOSTE DELLA COMMISSIONE ALLE CONCLUSIONI E RACCOMANDAZIONI DELLA CORTE 5

Raccomandazione 1 – Migliorare la preparazione alla cibersicurezza di tutti gli EUIBA mediante norme comuni vincolanti e maggiori risorse per la CERT-UE 5

Raccomandazione 2 – Promuovere ulteriori sinergie tra gli EUIBA in determinati settori 6

Raccomandazione 3 – Aumentare l'attenzione della CERT-UE e dell'ENISA sugli EUIBA meno maturi 7

Il presente documento contiene le riposte della Commissione europea alle osservazioni che figurano nella relazione speciale della Corte dei conti dell'Unione europea, conformemente all'articolo 259 del regolamento finanziario e pubblicate unitamente alla relazione speciale.

I. SINTESI DELLE RISPOSTE DELLA COMMISSIONE

a) Introduzione generale

La cibersicurezza ha assunto un ruolo politico e operativo prioritario per la Commissione europea. La crisi COVID-19 ha aumentato la dipendenza dai servizi digitali (cloud computing, dispositivi mobili, intelligenza artificiale); negli ultimi due anni si è inoltre assistito a una transizione su vasta scala verso il lavoro da casa. Per questi motivi anche la criminalità informatica e il ciberspionaggio, vale a dire le due principali minacce per istituzioni, organi e agenzie dell'Unione europea (EUIBA), hanno di fatto trasferito online gran parte delle loro attività. Consapevole di tale tendenza, la Commissione ha dato prova di una leadership coerente e risoluta in materia di cibersicurezza. Il regolamento sulla cibersicurezza, entrato in vigore nel 2019, ha conferito all'ENISA un mandato permanente, di più ampia portata. Il regolamento ha anche stabilito una cooperazione formale tra l'ENISA e la CERT-UE (la squadra di pronto intervento informatico a sostegno di tutti gli EUIBA). Nel 2020 la Commissione ha proposto il rafforzamento della direttiva sulla sicurezza delle reti e dell'informazione, la cui adozione in sede legislativa è prossima.

La strategia 2020 in materia di cibersicurezza contiene inoltre tre azioni riguardanti la sicurezza informatica degli EUIBA. Nel testo si annuncia un regolamento sulla sicurezza dell'informazione nelle istituzioni, negli organismi e nelle agenzie dell'UE, un regolamento su norme comuni in materia di cibersicurezza per le istituzioni, gli organi e gli organismi dell'UE e l'intenzione di fornire una nuova base giuridica per la CERT-UE al fine di consolidarne il mandato e i finanziamenti affinché disponga di risorse adeguate a far fronte al moltiplicarsi di minacce, rischi e incidenti.

Il lavoro di preparazione di tali proposte è in fase avanzata. Sebbene il collegio non abbia ancora provveduto ad adottarle, si prevede che lo farà nel primo trimestre del 2022. In questa fase preparatoria la discussione interistituzionale verte su questioni importanti quali la base giuridica delle proposte e la capacità di bilancio di tutti gli EUIBA per soddisfare il fabbisogno tanto in termini di copertura finanziaria delle proprie esigenze di cibersicurezza, quanto di reperimento delle risorse necessarie per sostenere la CERT-UE, il bilancio e in particolare l'organico.

Il livello di preparazione in materia di cibersicurezza degli EUIBA è caratterizzato da diversi gradi di maturità. Molti di essi hanno conseguito ottimi risultati in termini di preparazione contro le minacce informatiche e dovrebbero continuare a svolgere un ruolo di guida, stimolando e favorendo i progressi e ulteriori miglioramenti in tutto il panorama della cibersicurezza. Per conseguire progressi misurabili, è importante prendere atto dei diversi gradi di maturità degli EUIBA, e stabilire le priorità rivolgendo le azioni di miglioramento in primo luogo agli EUIBA la cui esposizione al rischio è più elevata in ragione delle lacune individuate.

b) Posizione della Commissione sulle principali osservazioni e raccomandazioni della Corte

La Commissione accoglie con favore la relazione della Corte dei Conti sulla cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE. Prende atto che la relazione sottolinea l'importanza di quadri giuridici comuni a tutti gli EUIBA in materia di sicurezza delle informazioni e cibersicurezza al fine di aumentare il livello generale di cibersicurezza. La Commissione rileva che le principali osservazioni e raccomandazioni della Corte non riguardano la cibersicurezza operativa interna della

Commissione in sé, bensì il ruolo politico della Commissione nel formulare proposte legislative volte ad accrescere la maturità informatica degli EUIBA.

I futuri regolamenti sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'UE e sulle norme comuni in materia di cibersicurezza per le istituzioni, gli organi e gli organismi dell'UE stabiliranno le norme comuni finalizzate al raggiungimento di livelli elevati di sicurezza delle informazioni e di cibersicurezza, ma la loro attuazione nel contesto organizzativo e operativo dei singoli EUIBA (in particolare in relazione ai rispettivi profili di minaccia e di rischio) rimane di autonoma competenza di questi ultimi. La proposta di regolamento in materia di cibersicurezza prevederà meccanismi di conformità adeguati e commisurati all'obiettivo e all'ambito di applicazione delle nuove norme, fatta salva l'autonomia delle istituzioni, degli organi e delle agenzie.

La Commissione esercita attualmente la presidenza del sottogruppo per la cibersicurezza del comitato interistituzionale per la trasformazione digitale (ICDT), una carica con avvicendamento a rotazione (per un periodo massimo di due anni). Va osservato che il lavoro del sottogruppo non beneficia di risorse specifiche: tutte le azioni sono svolte dai partecipanti con la massima diligenza possibile e a titolo volontario.

La Commissione condivide il principio generale di rafforzare le risorse e il mandato della CERT-UE.

In questo senso, la Commissione aderisce alle principali osservazioni e raccomandazioni contenute nella relazione. La posizione della Commissione è esposta più diffusamente nelle osservazioni supplementari di cui alla sezione III. Per quanto riguarda le raccomandazioni, la Commissione accoglie la raccomandazione 1, lettere a), b), c), d), e), f) e g), e la raccomandazione 2, lettere a), b) e c).

c) Ultimi sviluppi di rilievo e prossime tappe

È stata completata la consultazione formale a livello dei direttori generali degli EUIBA in merito alle proposte consolidate dei due regolamenti (sulla sicurezza delle informazioni e sulla cibersicurezza) ed è in corso la valutazione dei riscontri ricevuti, preliminare al completamento del pacchetto e all'adozione da parte del collegio nel primo trimestre del 2022.

II. RISPOSTE DELLA COMMISSIONE ALLE PRINCIPALI OSSERVAZIONI DELLA CORTE DEI CONTI

1. Livelli di maturità degli EUIBA per quanto riguarda la cibersicurezza

La Commissione riconosce che nell'esaminare il livello della spesa per la cibersicurezza sostenuta dagli EUIBA è importante tenere conto delle minacce e dei rischi.

Analogamente, per quanto attiene all'aspetto risorse umane, vi sono molteplici fattori che influenzano la stabilità dell'organico degli EUIBA. Uno di questi è la crescente complessità del

mercato dal quale attingere gli esperti specializzati in cibersicurezza. In molti casi le norme applicabili alle risorse umane non sono adeguate ai profili specializzati (in termini di assunzione, crescita professionale, formazione). Inoltre la diffusa pressione esercitata dall'autorità di bilancio sui livelli degli organici di tutti gli EUIBA fa sì che settori emergenti e altamente prioritari rimangano sottodimensionati, in particolare nel caso dei servizi operativi interni.

Il riferimento ai progressi in materia di governance e gestione dei rischi dovrebbe tenere conto del fatto che attualmente il monitoraggio della conformità sta passando dalla fase pilota a quella della sua piena introduzione. È pertanto normale che il grado di copertura raggiunto finora sia piuttosto limitato. Il progetto di conformità rappresenta la fase successiva di un processo di miglioramento della maturità informatica a lungo termine, iniziato con la definizione di una metodologia comune di gestione dei rischi, la messa a punto di strumenti comuni, l'introduzione della gestione delle vulnerabilità e il monitoraggio, la verifica e la convalida dell'inventario delle risorse. In questo percorso ancora lungo sono stati compiuti progressi nonostante la complessità della base di risorse della Commissione, che conta oltre 1 000 sistemi informatici gestiti da più di 50 tra direzioni generali e agenzie esecutive.

2. Meccanismi di cooperazione degli EUIBA

Grazie alla sua partecipazione a pieno titolo alla rete dei CSIRT istituita dalla direttiva NIS, la CERT-UE rappresenta una straordinaria esperienza di successo nella promozione della cooperazione non solo tra gli EUIBA, ma anche a livello europeo. In questo senso la CERT-UE costituisce un caso esemplare di come sia possibile migliorare tanto la cooperazione quanto i servizi di cibersicurezza. Dalle osservazioni della Corte sulla CERT-UE emerge con chiarezza l'eccezionale lavoro svolto da quest'ultima a dispetto di un panorama di minacce informatiche sempre più aggressive e delle risorse cronicamente sottodimensionate.

Nel quadro dell'attuale accordo interistituzionale (AII), le agenzie decentrate e le imprese comuni dell'UE sono ufficialmente rappresentate dall'ENISA in seno al comitato direttivo della CERT-UE. Inoltre le loro posizioni sono espresse nelle riunioni del comitato direttivo da un rappresentante del comitato consultivo TIC (ICTAC) autorizzato a partecipare a tali riunioni per assistere l'ENISA nel suo ruolo di rappresentanza delle agenzie, ma senza farne parte e senza diritto di voto. La proposta di regolamento affronterà la questione dell'adeguata rappresentanza delle agenzie presso il comitato direttivo della CERT-UE completandone la composizione con un massimo di tre rappresentanti designati dalla rete delle agenzie dell'UE (EUAN) su proposta del suo comitato consultivo TIC.

La partecipazione al sottogruppo sulla cibersicurezza dell'ICDT avviene con la massima diligenza possibile secondo il livello di impegno stabilito dall'istituzione, dall'organo o dall'agenzia dell'UE. Nel processo di preparazione del nuovo contratto quadro sulla cibersicurezza si sta affrontando il tema del miglioramento della condivisione delle informazioni sugli appalti, elemento importante nell'ambito della task force 2 del sottogruppo sulla cibersicurezza.

Per quanto riguarda gli strumenti comuni per servizi quali la posta elettronica e la videoconferenza, esiste già la possibilità di applicare alla posta elettronica criptata il sistema SECEM-2 introdotto dalla Commissione per tutti gli EUIBA, legato alla gestione efficace di chiavi e certificati crittografici. È inoltre in fase di sviluppo il SECABC, uno strumento che consente la crittografia della posta elettronica tra le istituzioni, con l'intento di renderlo accessibile a tutti gli EUIBA interessati a partire dal 2022. Il sistema di videoconferenze sicure per i servizi di SNC è già stato realizzato e può essere esteso ad altri EUIBA su base ad hoc mediante la gestione delle identità dei partecipanti alle riunioni. Nella proposta di regolamento sulla sicurezza delle informazioni si affronterà anche la

condivisione delle informazioni sensibili (in particolare prevedendo un'etichettatura e una marcatura comuni).

3. Condivisione di informazioni su incidenti significativi o vulnerabilità

Il progetto di regolamento sulla cibersicurezza, conformemente alla proposta avanzata dalla Commissione nella direttiva NIS 2[1], affronta anche il fatto che non tutti gli EUIBA notifichino alla CERT-UE gli incidenti significativi o le vulnerabilità . Il livello di attuazione dipenderà dalle risorse supplementari destinate allo scopo dagli EUIBA autonomi. A causa dell'autonomia istituzionale degli EUIBA, la possibilità di imporre l'invio di tali notifiche rimane limitata anche nell'ambito della proposta di regolamento attualmente prevista. La proposta di regolamento in materia di cibersicurezza prevederà meccanismi di conformità adeguati e commisurati all'obiettivo e all'ambito di applicazione delle nuove norme, fatta salva l'autonomia delle istituzioni, degli organi e delle agenzie.

III. RISPOSTE DELLA COMMISSIONE ALLE CONCLUSIONI E RACCOMANDAZIONI DELLA CORTE

Raccomandazione 1 – Migliorare la preparazione alla cibersicurezza di tutti gli EUIBA mediante norme comuni vincolanti e maggiori risorse per la CERT-UE

Nel testo della proposta di regolamento saranno incluse misure specifiche volte a rafforzare ulteriormente il livello comune di cibersicurezza. Tali misure si tradurranno in piani di cibersicurezza definiti e attuati a livello degli EUIBA nell'ambito del loro quadro di governance della cibersicurezza.

La Commissione accoglie la raccomandazione. Con riferimento alle sotto-raccomandazioni specifiche, la Commissione rileva quanto segue:

a) la Commissione accoglie la raccomandazione 1, lettera a). La proposta di regolamento conterrà disposizioni sulla governance e sui quadri di controllo istituiti al massimo livello di gestione esecutiva di ogni EUIBA al fine di garantire una gestione efficace e prudente di tutti i rischi di cibersicurezza;
b) la Commissione accoglie la raccomandazione 1, lettera b). La proposta di regolamento rafforzerà il riferimento all'approccio alla cibersicurezza basato sulla valutazione dei rischi, chiarendo che le azioni, i piani di sicurezza informatica e l'attuazione effettiva dei controlli essenziali dovrebbero tenere conto delle valutazioni effettuate;

[1] Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (COM(2020) 823 final).

c) la Commissione accoglie la raccomandazione 1, lettera c). I programmi di istruzione, sensibilizzazione e formazione in materia di cibersicurezza saranno citati nella proposta di regolamento come parte integrante degli elementi di base della cibersicurezza;
d) la Commissione accoglie la raccomandazione 1, lettera d). L'esperienza della Commissione dimostra che, per quanto essenziali, gli audit e le verifiche periodici non sono sufficienti ad accertare il compimento di progressi. Di conseguenza sono necessarie relazioni periodiche e trasparenza nell'ambito del quadro di governance della cibersicurezza di cui alla lettera a);
e) la Commissione accoglie la raccomandazione 1, lettera e). La proposta di regolamento conterrà disposizioni relative alla notifica, da parte degli EUIBA, di minacce, vulnerabilità e incidenti informatici significativi alla CERT-UE;
f) la Commissione accoglie la raccomandazione 1, lettera f). La Commissione sostiene la necessità di potenziare le risorse della CERT-UE. Nel testo della proposta di regolamento figureranno disposizioni relative all'organico e ai contributi finanziari degli EUIBA;
g) la Commissione accoglie la raccomandazione 1, lettera g). La proposta di regolamento prevederà meccanismi di conformità adeguati e commisurati all'obiettivo e all'ambito di applicazione delle disposizioni, nel rispetto dell'autonomia istituzionale degli EUIBA. Il contenuto del futuro regolamento dipende dall'esito della procedura legislativa ed è il risultato della decisione del legislatore dell'UE relativamente alla proposta formulata dalla Commissione.

Raccomandazione 2 – Promuovere ulteriori sinergie tra gli EUIBA in determinati settori

La Commissione, che attualmente presiede il sottogruppo sulla cibersicurezza del comitato interistituzionale per la trasformazione digitale (ICDT), accoglie le raccomandazioni che invitano a promuovere soluzioni per la condivisione uniforme e sicura delle informazioni sensibili, la condivisione sistematica di informazioni sui progetti in materia di cibersicurezza e quadri comuni per gli appalti e i contratti relativi ai servizi di cibersicurezza.

La Commissione accoglie la raccomandazione. Con riferimento alle sotto-raccomandazioni specifiche, la Commissione rileva quanto segue:

a) la Commissione accoglie la raccomandazione 2, lettera a). La Commissione sta presentando al sottogruppo dell'ICDT sulla cibersicurezza iniziative e servizi tecnici per promuovere e sostenere la creazione di strumenti comuni di condivisione delle informazioni sensibili, abilitandoli per servizi quali la posta elettronica e le videoconferenze. Si fa inoltre presente che le questioni della marcatura comune e delle norme comuni per la gestione delle informazioni sensibili non classificate saranno affrontate nella proposta di regolamento sulla sicurezza delle informazioni;
b) la Commissione accoglie la raccomandazione 2, lettera b). L'attuale task force nell'ambito del sottogruppo dell'ICDT sulla cibersicurezza sta esaminando la questione e ne curerà gli sviluppi. Il miglioramento della condivisione delle informazioni sugli appalti costituisce uno dei punti affrontati nella preparazione del nuovo contratto quadro sulla cibersicurezza;
c) la Commissione accoglie la raccomandazione 2, lettera c). Gli EUIBA hanno già accesso ai contratti quadro interistituzionali nel settore delle TIC gestiti dalla Commissione. La preparazione del nuovo contratto quadro sulla cibersicurezza sarà coordinata con il sottogruppo dell'ICDT sulla cibersicurezza.

Raccomandazione 3 – Aumentare l'attenzione della CERT-UE e dell'ENISA sugli EUIBA meno maturi

La raccomandazione è rivolta alla CERT-UE e all'ENISA.