Sicurezza Digitale, l'Unione europea mette al riparo le istituzioni dal rischio cyber

di Alessia Palladino - pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale, 28 febbraio 2024

Lo scorso 13 dicembre 2023 è stato emanato il Regolamento Ue/2023/2841, che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione. Il Regolamento istituisce un quadro interno di gestione, governance e controllo dei rischi per la cibersicurezza, per assicurare la continuità operativa e la gestione delle crisi.

La tecnologia si conferma ormai, anche in ambito europeo, un apparato indispensabile per favorire un'amministrazione europea aperta, efficace ed indipendente.

Se il progressivo processo di digitalizzazione delle amministrazioni, d'insieme con il ricorso a strumenti ICT e cloud costituiscono aspetti ormai ricorrenti nelle attività istituzionali, l'evoluzione tecnologica e la crescente interconnessione dei sistemi digitali **amplificano i rischi per la cibersicurezza**, rendendo le istituzioni pubbliche **più vulnerabili** alle minacce e agli incidenti informatici.

Per raggiungere un livello comune elevato di *cibersicurezza* e realizzare un sistema di gestione efficace dei rischi e della continuità operativa, lo scorso 13 dicembre 2023 è stato emanato il **Regolamento Ue/2023/2841**, che stabilisce misure per un **livello comune elevato di cibersicurezza** nelle istituzioni, negli organi e negli organismi dell'Unione.

Il Regolamento europeo è entrato pienamente in vigore il 7 gennaio 2024, ed **istituisce un quadro interno di gestione, governance e controllo dei rischi per la cibersicurezza** per assicurare la continuità operativa e la gestione delle crisi.

A tal fine, ciascun soggetto dell'Unione dovrà adottare misure tecniche, operative e organizzative adeguate e proporzionate.

Il Regolamento sulla cibersicurezza è stato **presentato congiuntamente a una Proposta di Regolamento sulla sicurezza delle informazioni,** che stabilisce norme e norme minime in materia di sicurezza delle informazioni per tutte le istituzioni, gli organi, gli uffici e le agenzie dell'UE e con gli Stati membri, sulla base di pratiche e misure standardizzate per proteggere i flussi di informazioni.

Come precisato dal Commissario europeo per il Bilancio e l'amministrazione, **Johannes Hahn**, "*Il regolamento rafforza la cibersicurezza dei soggetti dell'Unione e allinea l'amministrazione dell'UE alle norme imposte agli Stati membri, come la direttiva relativa a livelli comuni elevati di cibersicurezza in tutta l'Unione, nota anche come NIS 2. La rapida adozione del regolamento dimostra l'impegno dell'UE per il conseguimento di tali obiettivi. Invito ora i colegislatori ad*

avviare rapidamente i negoziati per il regolamento parallelo sulla sicurezza delle informazioni".

Lo **sviluppo di una governance istituzionale coordinata** per fronteggiare le insidie del rischio cyber **costituisce un presupposto fondamentale**. Secondo il Commissario Hahn, *"Poiché le minacce informatiche stanno diventando sempre più pervasive e gli aggressori informatici sono più sofisticati, il conseguimento di un elevato livello comune di cibersicurezza in tutti i soggetti dell'Unione è fondamentale per garantire un'amministrazione pubblica dell'UE aperta, efficiente, sicura e resiliente".*

A tal fine, **il Regolamento fornisce interessanti innovazioni per la governance istituzionale,** dedicandovi i Capi III, IV e V.

Il **Capo IV** mira a fornire una **serie completa di norme** sull'organizzazione, il funzionamento e l'operatività del **CERT-UE**, la squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione Europea.

Il CERT-UE è stato rinominato "***Servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione***", e contribuisce (allineandosi ai ruoli delineati nella **Direttiva (UE)/2022/2555**) alla cooperazione e lo scambio di informazioni con la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (*the Computer Security Incident Response Teams* – **CSIRT**).

Inoltre, in linea con la **Raccomandazione 2017/1584/Ue** della Commissione europea, il Servizio dovrebbe **cooperare con l'ENISA** secondo le forme di **cooperazione strutturata** di cui al **Regolamento 2019/881/Ue**, per evitare la duplicazione delle attività.

Per contribuire a un livello comune elevato di cibersicurezza nell'Unione, infine, il CERT-UE dovrebbe condividere con gli omologhi degli Stati membri informazioni specifiche sugli incidenti.

Oltre a conferire maggiori compiti e un ruolo più ampio al CERT-UE, per assicurare un efficace coordinamento ed **instaurare un livello comune elevato di cibersicurezza** tra i soggetti dell'Unione, **il Capo III istituisce** il **Comitato interistituzionale per la cibersicurezza** (*Interinstitutional Cybersecurity Board* – ***IICB***).

Ai sensi dell'articolo 10, paragrafo 3, del Regolamento, l'IICB è composto da un rappresentante designato da ciascuno dei seguenti soggetti:

- il Parlamento europeo;
- il Consiglio europeo;
- il Consiglio dell'Unione europea;
- la Commissione;
- la Corte di giustizia dell'Unione europea;
- la Banca centrale europea;
- la Corte dei conti;

- il Servizio europeo per l'azione esterna;
- il Comitato economico e sociale europeo;
- il Comitato europeo delle regioni;
- la Banca europea per gli investimenti;
- il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca;
- l'ENISA;
- il Garante europeo della protezione dei dati (GEPD);
- l'Agenzia dell'Unione europea per il programma spaziale;
- tre rappresentanti designati dalla rete delle agenzie dell'Unione (EUAN) su proposta del suo comitato consultivo TIC.

Come precisato dal **Considerando n. 23**, l'IICB (il cui effettivo funzionamento dovrebbe essere ulteriormente disciplinato da un regolamento interno) svolge funzioni di controllo, vigilanza e indirizzo, anche nei confronti del CERT-UE. Inoltre, dovrebbe svolgere un ruolo propulsivo volto a sostenere l'attuazione del Regolamento, adottando raccomandazioni ed incentivando l'intervento dei soggetti interessati.

L'IICB dovrebbe altresì garantire la rappresentanza delle istituzioni dell'Unione e includere rappresentanti degli organi e degli organismi dell'Unione attraverso la rete delle agenzie dell'Unione europea (EU Agencies Network – EUAN).

In conclusione, il nuovo Regolamento sulla cybersicurezza offre l'occasione per riflettere sull'importanza della cooperazione, quale misura fondamentale di carattere organizzativo per ridurre il rischio cyber.