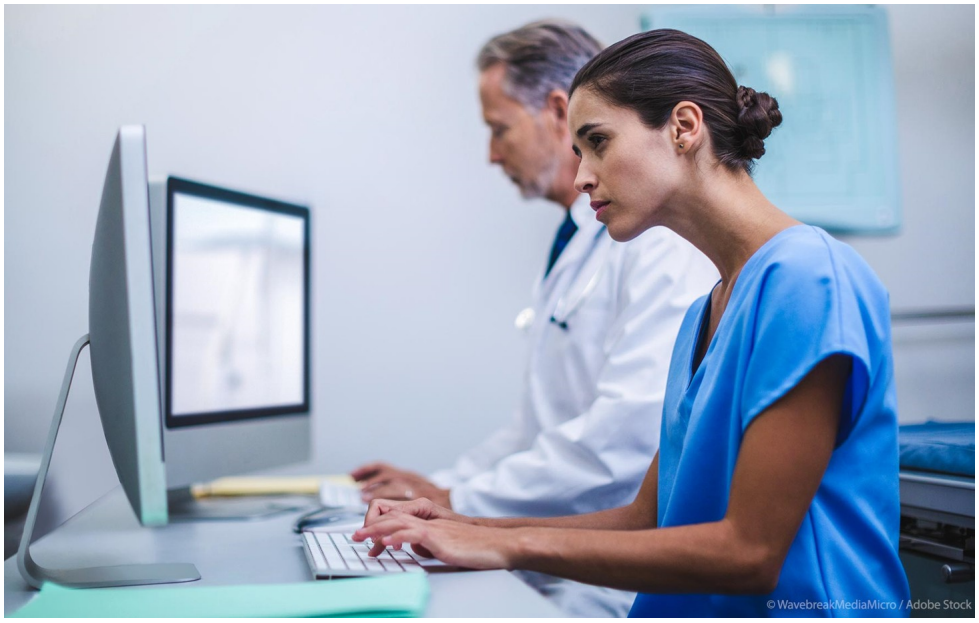
Scritto da Red.
Giovedì 10 Novembre 2022 13:31



STRASBURGO – Giovedì, i deputati hanno approvato norme che impongono ai Paesi dell'Ue di adottare misure di vigilanza e di applicazione più severe e di armonizzare le sanzioni.

La legislazione, già concordata tra i deputati e il Consiglio nel maggio scorso, stabilirà obblighi più severi in materia di cibersicurezza per quanto riguarda la gestione del rischio, gli obblighi di segnalazione e la condivisione delle informazioni. I requisiti riguardano, tra l'altro, la risposta agli incidenti, la sicurezza della catena di approvvigionamento, la crittografia e la divulgazione delle vulnerabilità.

Il testo legislativo è stato adottato con 577 voti favorevoli, 6 contrari e 31 astensioni.

Un numero maggiore di entità e settori dovrà adottare misure per proteggersi. I "settori essenziali", come quelli dell'energia, dei trasporti, delle banche, della sanità, delle infrastrutture digitali, della pubblica amministrazione e dello spazio, saranno coperti dalle nuove disposizioni in materia di sicurezza.

Durante i negoziati, i deputati hanno insistito sulla necessità di regole chiare per le aziende e sono riusciti a includere il maggior numero possibile di enti governativi e pubblici nel campo di applicazione della direttiva.

Le nuove norme proteggeranno anche i cosiddetti "settori importanti" come i servizi postali, la gestione dei rifiuti, i prodotti chimici, gli alimenti, la produzione di dispositivi medici, l'elettronica, i macchinari, i veicoli a motore e i fornitori di servizi digitali. Tutte le medie e grandi imprese dei settori selezionati dovranno rispettare le nuove regole.

Il testo stabilisce inoltre un quadro per una migliore cooperazione e condivisione delle informazioni tra le diverse autorità e gli Stati membri e crea una banca dati europea sulle vulnerabilità.

Citazione

"Il ransomware e le altre minacce informatiche hanno predato l'Europa per troppo tempo. Dobbiamo agire per rendere le nostre imprese, i nostri governi e la nostra società più resistenti alle operazioni informatiche ostili", ha dichiarato il relatore Bart Groothuis (Renew, NL).

"Questa direttiva europea aiuterà circa 160.000 enti a rafforzare la propria sicurezza e a rendere l'Europa un luogo sicuro in cui vivere e lavorare. Inoltre, consentirà di condividere le informazioni con il settore privato e con i partner di tutto il mondo. Se veniamo attaccati su scala industriale, dobbiamo rispondere su scala industriale", ha dichiarato.

"Questa è la migliore legislazione sulla sicurezza informatica che il Continente abbia mai visto, perché offre all'Europa una gestione proattiva degli incidenti informatici e orientata al servizio", ha aggiunto.

Prossime tappe

Dopo l'approvazione del Parlamento, anche il Consiglio deve adottare formalmente la legge prima che venga pubblicata nella Gazzetta Ufficiale dell'Ue e entri cosi in vigore.

Contesto

La direttiva sulla sicurezza delle reti e dell'informazione (Nis) è stato il primo atto legislativo a livello europeo sulla sicurezza informatica, con l'obiettivo specifico di raggiungere un elevato livello comune di sicurezza informatica in tutti gli Stati membri. Se da un lato ha aumentato le capacità degli Stati membri in materia di sicurezza informatica, dall'altro la sua attuazione si è rivelata difficile, causando una frammentazione a diversi livelli nel mercato interno.

Per rispondere alle crescenti minacce poste dalla digitalizzazione e all'aumento degli attacchi informatici, la Commissione ha presentato una proposta per sostituire la direttiva Nis e rafforzare così i requisiti di sicurezza, affrontare la sicurezza delle catene di approvvigionamento, semplificare gli obblighi di segnalazione e introdurre misure di vigilanza più rigorose e requisiti di applicazione più severi, comprese sanzioni armonizzate in tutta l'Ue.