COMUFFICIO
Fondata nel 1945

Agli Associati Comufficio
Loro sedi

Milano, 27 agosto 2025

Oggetto: Cyber Resilience Act

Dal 2026 le aziende dovranno segnalare incidenti e vulnerabilità, in base a scadenze differenziate per prodotti normali, importanti e critici. Gli obblighi coinvolgeranno anche certificazioni e gestione dei rischi.
Il presente documento rappresenta una breve sintesi del provvedimento, per il quale chiediamo di esprimere interesse per un eventuale corso di approfondimento analitico, segnalando a:
segreteria@comufficio.it

Il recente Regolamento UE 2024/2847(**Cyber Resilience Act**) mira a garantire "che i prodotti con componenti digitali – per esempio, i prodotti relativi all'Internet delle Cose (Internet of Things – IoT) – siano resi sicuri lungo l'intera catena di approvvigionamento e per tutto il ciclo di vita". Il Regolamento si occupa, quindi, della **sicurezza informatica dei prodotti** e NON delle organizzazioni. Tale Regolamento diventa complemento sia del Cyber Security Act, sia di NIS2, che "non contemplano direttamente requisiti obbligatori per la sicurezza dei prodotti con elementi digitali".

Vediamo alcuni dettagli, riguardanti la classificazione dei prodotti:

- **prodotti normali**: "qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immessi separatamente sul mercato. Le misure minime da adottare e il relativo processo di gestione delle vulnerabilità fanno riferimento a quanto contenuto nell'allegato 1 del Regolamento;
- **prodotti importanti**: sono prodotti (analiticamente descritti nell'art. 7 All. 3 del Regolamento) di sicurezza informatica e prodotti i cui malfunzionamenti possono impattare su altri sistemi informatici o sulle persone. Entro 11/12/2025 la Commissione fornirà ulteriori indicazioni sulle descrizioni di tali prodotti;
- **prodotti critici**: definiscono un numero limitato di prodotti (descritti nell'art.8, allegato 49, alcuni dei quali già certificati secondo i Common Criteria -ISO/IEC 15408). Questi prodotti devono applicare le misure dell'allegato 1 ed essere certificati con livello di affidabilità almeno "sostanziale", in coerenza con le disposizioni del Cybersecurity Act (regolamento UE 2019/881).

Indicazioni per i fabbricanti

In generale, i **fabbricanti devono valutare il rischio relativo alla cybersicurezza dei prodotti**, sia in termini tecnici sia di processo, includendo le attività di manutenzione, assistenza e gestione della vulnerabilità. L'assistenza deve essere garantita per almeno 5 anni (art. 13).
Il Regolamento fornisce, inoltre, **indicazioni** sulla documentazione tecnica (art. 13 e 31, Allegato VII), sul tracciamento dei prodotti (art. 13), sulle istruzioni per gli utilizzatori (Allegato II), sui punti di contatto (art. 13), sul richiamo dei prodotti (art. 13), sulla redazione delle dichiarazioni di conformità UE (art. 28 e Allegato V) e sulla marcatura CE (art. 29 e 30).
L'articolo 14, come per altre normative, obbliga i fabbricanti a notificare al CSIRT (l'Agenzia per la cybersicurezza nazionale) gli incidenti determinati dallo sfruttamento di vulnerabilità dei prodotti. L'articolo 15, inoltre, prevede che fabbricanti e persone possano segnalare vulnerabilità al CSIRT (elemento sicuramente molto interessante).

Altri richiami

Il Regolamento si occupa, all'interno degli artt. 24 e 25 anche dei software liberi e open source e del processo di certificazione (art. 32) che li riguarda.

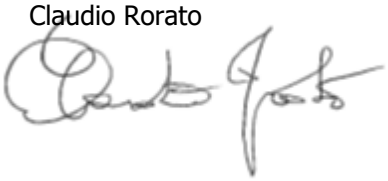
La certificazione (artt. 35-51) fa riferimento all'istituzione dell'autorità di notifica che, a sua volta, deve approvare gli organismi di notifica (organismi di certificazione sono già presenti per ISO 9001, ISO /IEC 27001 et similia).

All'articolo 32 si fa, inoltre, specifico riferimento al mondo delle micro e PMI, per le quali si raccomanda di fare attenzione alle loro specifiche esigenze in termini di tariffe e procedure di valutazione della conformità. Anche l'articolo 33 si occupa di questi segmenti aziendali, prevedendo misure di sostegno che riguardano la formazione e la comunicazione.

La Commissione Europea ha il potere di modificare alcuni dei punti sin qui illustrati ma devono ancora essere messi a punto i canali e le modalità di aggiornamento.
https://www.agendadigitale.eu/sicurezza/cyber-resilience-act-la-sicurezza-diventa-obbligatoria-cosa-cambia-per-le-aziende/

Con i migliori saluti.

Il Direttore Generale
Claudio Rorato



Associazione Nazionale Aziende Produttrici, Importatrici e Distributrici di prodotti e servizi per l'I.C.T.
Codice Fiscale 01796460150 - Partita IVA 09556140151
Via Sangro, 13/A 20132 Milano - Tel.02/28381307 - Fax 02/2841032
segreteria@comufficio.it – www.comufficio.it