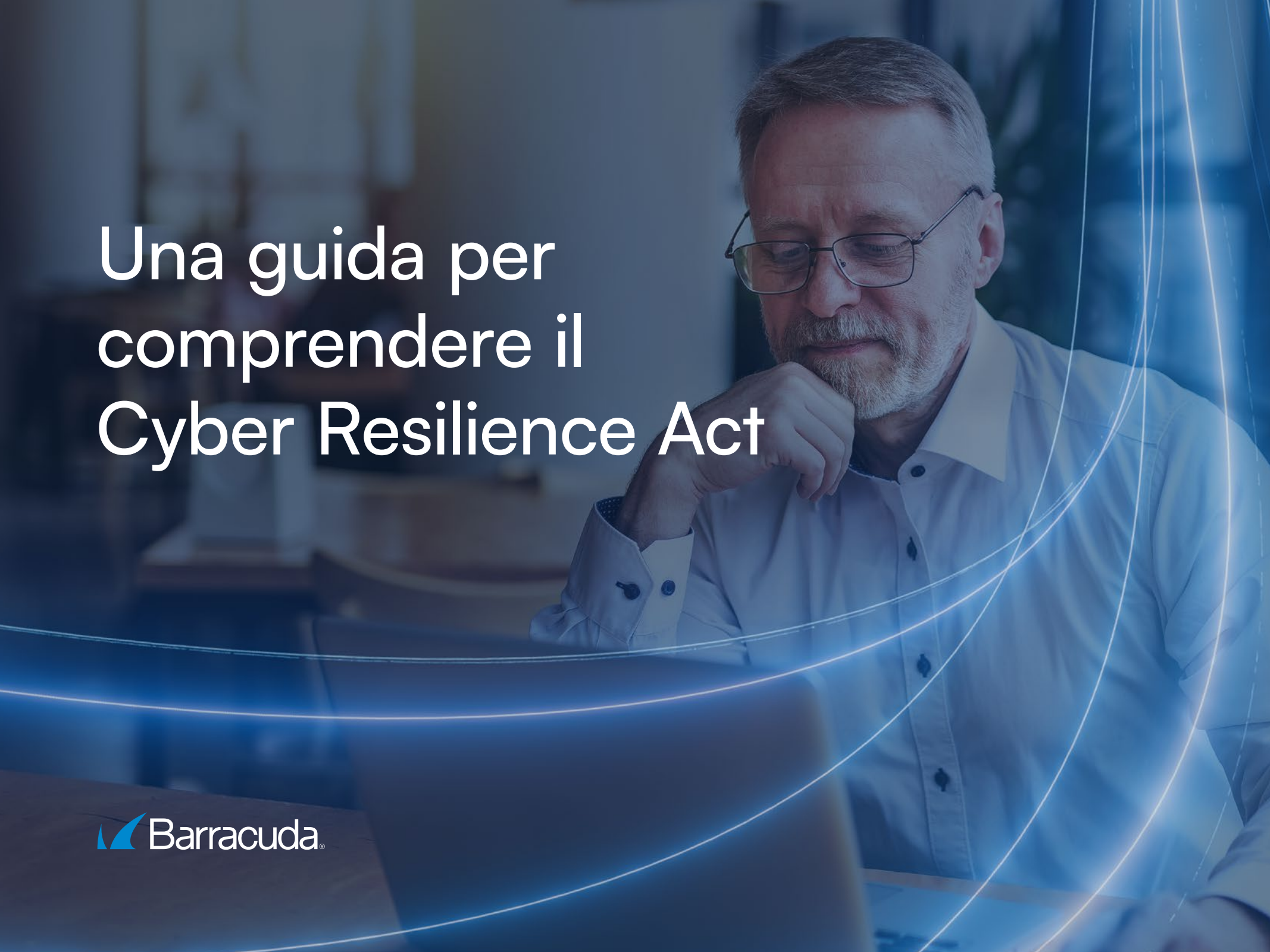

Una guida per comprendere il Cyber Resilience Act

Barracuda

Comprendere il Cyber Resilience Act (CRA) dell'Unione europea (UE) è essenziale per le organizzazioni che operano nell'UE. I produttori di prodotti digitali offerti in vendita nell'UE e gli importatori e distributori di tali prodotti sono soggetti al CRA. Questo e-book fornisce alcuni punti salienti del CRA per i produttori, ma non sostituisce né è destinato a essere una consulenza legale per la propria azienda.

Il CRA è entrato in vigore nel dicembre 2024, concedendo alle organizzazioni un po' di tempo per raggiungere la conformità. Ecco alcune date importanti da sapere:

- 11 settembre 2026 — I produttori devono iniziare a segnalare gravi incidenti di sicurezza informatica e vulnerabilità attivamente sfruttate.
- 11 dicembre 2027 — Tutti i prodotti nuovi e quelli esistenti «sostanzialmente modificati» immessi sul mercato a partire da questa data devono essere conformi al CRA.

La legge è concepita per fornire un insieme più uniforme di requisiti di sicurezza per tutti i prodotti con elementi digitali venduti nell'UE e per offrire a consumatori e aziende maggiori informazioni sulla sicurezza di questi prodotti prima dell'acquisto. La legge mira a correggere ciò che l'UE descrive come il «livello inadeguato» di sicurezza informatica riscontrato in molti prodotti, inclusa la mancanza di aggiornamenti di sicurezza.

Il CRA integra il Digital Operational Resilience Act (DORA) e la Direttiva sulla sicurezza delle reti e delle informazioni 2 (NIS2):

- DORA si concentra sul miglioramento della resilienza cibernetica dell'industria finanziaria, mentre NIS2 si applica a un insieme più ampio di entità che forniscono servizi essenziali in settori chiave.
- Sia DORA che NIS2 specificano requisiti di sicurezza informatica, comprese le misure di sicurezza della catena di approvvigionamento, con l'obiettivo di aumentare la resilienza delle aziende regolamentate, dato l'impatto che le loro offerte hanno su altre persone.
- Il CRA si applica a livello di prodotto, fornendo il quadro obbligatorio per i prodotti sicuri con elementi digitali. Quando il cliente di tali prodotti è regolamentato da DORA o NIS2, l'utilizzo di hardware e software conformi al CRA può aiutare queste entità a rispettare i loro obblighi.

NIS2 e DORA non rientrano nell'ambito di questo e-book. Per ulteriori dettagli, consultare Comprendere DORA: una guida al Digital Operational Resilience Act e Orientarsi nella NIS2: una guida alle imminenti normative europee sulla sicurezza informatica.

Perché il CRA è importante?

Il CRA copre tutti i prodotti che contengono «elementi digitali», il che significa che questo regolamento copre sia l'hardware che il software collegati a un dispositivo o a una rete, oltre alle soluzioni integrate di elaborazione dei dati a distanza di tali prodotti (cioè i servizi cloud). La Commissione Europea afferma: «Il regolamento si applica a tutti i prodotti collegati direttamente o indirettamente a un altro dispositivo o rete, ad eccezione di esclusioni specifiche, come alcuni prodotti di servizi o software open-source che sono già coperti da norme esistenti, come nel caso dei dispositivi medici, dell'aviazione e delle automobili».[1] I prodotti non conformi non potranno essere venduti nell'UE. Le organizzazioni sorprese a farlo saranno soggette a multe. Proprio come il Regolamento generale sulla protezione dei dati (GDPR) ha cambiato radicalmente il modo in cui le aziende gestiscono le informazioni personali, il CRA ha il potenziale per avere un effetto simile sul modo in cui i produttori realizzano, vendono e supportano i loro prodotti con elementi digitali offerti sul mercato dell'UE.

Il CRA affronta un problema crescente legato ai prodotti tecnologici moderni che raccolgono, elaborano, condividono e archiviano i dati degli utenti, spesso senza alcuna sicurezza o con una sicurezza debole, mettendo a rischio tali dati. Con l'invecchiamento di questi prodotti, le soluzioni di sicurezza disponibili possono diventare obsolete. C'è poca supervisione su come, quando o se gli aggiornamenti di sicurezza vengono forniti agli utenti. Il CRA si propone di aumentare la sicurezza dei prodotti con elementi digitali e di garantire che tali prodotti rimangano sicuri durante tutto il loro ciclo di vita. La legge garantirà inoltre maggiore trasparenza agli utenti, che avranno una migliore comprensione della sicurezza dei prodotti con elementi digitali e di come ciò potrebbe influire sui loro dati.

[1] Cyber Resilience Act | Modellare il futuro digitale dell'Europa

Barracuda

Obblighi CRA per i produttori

Il CRA introduce requisiti obbligatori di sicurezza informatica per i produttori che regolano la pianificazione, la progettazione, lo sviluppo, la produzione, la consegna, la documentazione e la manutenzione di tali prodotti. Questi obblighi devono essere soddisfatti in ogni fase della catena del valore.

Ai sensi del CRA, i prodotti possono essere classificati come standard (livello più basso), «importanti» (con più obblighi) — suddivisi in due sottocategorie: importante di classe I e importante di classe II — e «critici» (con il livello più alto di rischio e quindi di obblighi).

Per gli articoli standard, i produttori sono tenuti a progettare, fabbricare e testare beni e servizi per garantire la conformità ai «requisiti di sicurezza essenziali» specificati nell'Allegato I del CRA, documentare la valutazione e mantenere la documentazione tecnica a disposizione delle autorità di sorveglianza di mercato. A questo livello, i produttori possono fare affidamento su una valutazione interna della conformità (autovalutazione).

In generale, circa il 90% dei prodotti hardware e software dovrebbe rientrare in questa categoria standard, permettendo ai produttori di auto-testare e creare una dichiarazione di conformità prima di applicare il marchio CE che i prodotti conformi riceveranno.

Alcuni prodotti con elementi digitali, come browser web, firewall e sistemi operativi, rientrano nella categoria «Importante», altri addirittura nella categoria «Critico». Devono ancora soddisfare i requisiti tecnici di cui all'Allegato I, ma possono essere soggetti a un processo di valutazione della conformità più rigoroso, inclusa la valutazione/certificazione da parte di terzi prima di essere venduti nell'UE.

Oltre agli obblighi al momento della vendita, il CRA richiede anche ai produttori di fornire la gestione delle vulnerabilità e le patch di sicurezza come descritto di seguito.

Obblighi di segnalazione sulla sicurezza

Le vulnerabilità di sicurezza attivamente sfruttate e la segnalazione di incidenti gravi ai sensi del CRA entreranno in vigore l'11 settembre 2026.

Gli obblighi di segnalazione sono stringenti. I produttori dovranno fornire un avviso di «allerta precoce» ai regolatori entro 24 ore dalla presa di coscienza del problema. Entro 72 ore dalla scoperta di una vulnerabilità sfruttata, i produttori dovranno fornire informazioni generali sul prodotto interessato, una descrizione generale della vulnerabilità sfruttata e qualsiasi azione di mitigazione intrapresa dal produttore e che gli utenti possano adottare, oltre a indicare la sensibilità del problema. Entro 14 giorni dalla disponibilità delle misure di mitigazione, il produttore ha ulteriori obblighi di divulgazione sotto forma di un rapporto finale.

Gli obblighi di segnalazione includono anche l'informare gli utenti interessati e consigliarli su come mitigare l'esposizione.

I produttori dovrebbero familiarizzare con questi requisiti di segnalazione e sviluppare processi per rispettarli entro settembre Data di inizio 2026.

Obblighi di supporto tecnico

Il supporto alla sicurezza informatica, inteso come fornitura di aggiornamenti di sicurezza, è anch'esso un tema importante nel CRA e deve essere pianificato per coprire l'intero ciclo di vita del prodotto. I produttori devono specificare in anticipo il periodo di supporto per i prodotti con elementi digitali. In generale, le aziende che immettono sul mercato dell'UE prodotti con elementi digitali devono sostenerli per almeno cinque anni, a meno che la vita prevista del prodotto non sia inferiore a cinque anni; in tal caso, il supporto deve durare per la vita prevista del prodotto. Per i prodotti che generalmente hanno una durata superiore ai cinque anni (esempi: schede madri, router di rete, modem, switch e sistemi operativi), il periodo di assistenza dovrebbe essere più lungo. Gli aggiornamenti di sicurezza resi disponibili durante il periodo di supporto devono essere disponibili agli utenti per il periodo di supporto più lungo o per 10 anni.

Come verrà applicata la conformità?

La mancata conformità può comportare sanzioni, sia finanziarie — multe fino a 15 milioni di euro o il 2,5% del fatturato globale totale — sia non finanziarie. I regolatori potrebbero costringere un'azienda a richiamare prodotti non conformi.

Barracuda

Sei passaggi verso la conformità per i produttori

Di seguito sono riportati i passaggi fondamentali che i produttori devono seguire per avviare il processo di conformità ed essere pronti per il CRA quando sarà pienamente in vigore. I numerosi allegati del CRA forniscono dettagli su ciò che ci si aspetta da ogni passaggio.

1. Classificare i prodotti e condurre una valutazione del rischio informatico. Le organizzazioni possono avere prodotti in più categorie. Pertanto, è importante valutare ogni prodotto per determinare in quale categoria rientra: standard, importante o critico.

2. Preparare la documentazione tecnica. Esaminare l Allegato I del CRA e i requisiti della catena di approvvigionamento per tutti i prodotti e individuare eventuali lacune. Condurre e documentare una valutazione del rischio per ciascun prodotto secondo i criteri applicabili e individuare standard adeguati, specifiche comuni o schemi di certificazione.

3. Determinare l'approccio di valutazione della conformità di ciascun prodotto. Se necessario, coinvolgere una terza parte per questo esercizio.

4. Preparare una dichiarazione di conformità in linea con l'Allegato V/VI e completare la documentazione tecnica che copre il contenuto dell'Allegato VII. Successivamente il produttore deve applicare il marchio CE a un prodotto conforme, al suo imballaggio o alla documentazione. La marcatura CE indicherà la conformità dei prodotti con elementi digitali con il CRA, in modo che possano circolare liberamente all'interno dell'UE.

5. Preparare e fornire informazioni/istruzioni per l'utente come da Allegato II. La documentazione è una parte cruciale della conformità e il suo obiettivo è fornire trasparenza all'utente.

6. Monitorare e gestire le vulnerabilità. Il CRA richiede una partecipazione attiva e continua da parte dei produttori durante il periodo di copertura del supporto, che comprende la fornitura di assistenza per la sicurezza informatica, il monitoraggio di eventuali vulnerabilità, la segnalazione e la correzione, come gli aggiornamenti del software che affrontano i problemi di sicurezza.

Barracuda è attivamente impegnata nella conferma delle sue categorie di prodotto e nell'affrontare i prossimi passi. Forniremo informazioni sul Trust Center quando saranno disponibili.

PASSAGGIO 1
Classificare i prodotti e condurre una valutazione per ciascuno

PASSAGGIO 2
Preparare la documentazione tecnica

PASSAGGIO 3
Determinare l'approccio di valutazione della conformità

PASSAGGIO 4
Applicare la marcatura CE e redigere la dichiarazione di conformità

PASSAGGIO 5
Preparare e fornire istruzioni per l'utente

PASSAGGIO 6
Monitorare e gestire le vulnerabilità

Importante di classe I e importante di classe II

I prodotti importanti di classe I presentano un rischio di sicurezza informatica inferiore rispetto ai prodotti importanti di classe II. I produttori possono scegliere di autodichiarare la conformità se rispettano alcuni standard qualificati dell'UE/specifiche comuni/schemi di certificazione, purché siano disponibili e applicabili al prodotto. Altrimenti, potrebbero richiedere una verifica da parte di terzi.

Si ritiene che i prodotti importanti di classe II presentino un livello più elevato di rischio di sicurezza informatica e che sia necessaria la certificazione da parte di un ente terzo autorizzato.

Il CRA, il DORA e la NIS2 costituiscono un complesso insieme di normative sulla sicurezza informatica per le aziende che operano nell'UE. La propria azienda potrebbe essere soggetta a più di una di queste normative. Il Trust Center di Barracuda contiene diverse risorse per aiutare i clienti a comprendere il DORA, tra cui il nostro e-book Comprendere DORA: una guida al Digital Operational Resilience Act, e la NIS2, tra cui il nostro e-book Orientarsi nella NIS2: una guida alle imminenti normative europee sulla sicurezza informatica, per aiutare le aziende a rispettare i loro obblighi di conformità.

Informazioni su Barracuda

Barracuda è un'azienda leader globale nel settore della sicurezza informatica che offre una protezione completa contro le minacce complesse per le aziende di qualsiasi dimensione. La nostra piattaforma BarracudaONE basata sull'IA protegge e-mail, dati, applicazioni e reti con soluzioni innovative, XDR gestito e una dashboard centralizzata per massimizzare la protezione e rafforzare la resilienza informatica. Scelto da centinaia di migliaia di professionisti IT e provider di servizi gestiti in tutto il mondo, Barracuda offre difese potenti e facili da acquistare, implementare e utilizzare. Per maggiori informazioni, visitare it.barracuda.com.

Barracuda