Cyber Resilience Act (CRA): come l’affrontano due aziende del settore

10 Aprile 2025
Dalle 10 alle 11 CET

bluewind

drivesec

ARROW

Partecipa al Webinar Arrow Comes Home sulla Cyber Resilience Act (CRA) e scopri come la stanno affrontando due aziende del settore.

Come rendere sicuri i propri prodotti. L'approccio di Bluewind.

Per la marcatura CE, deve essere dimostrata la conformità ai requisiti essenziali elencati nella CRA.

La presunzione di conformità è data quando lo sviluppo ha seguito standard armonizzati o specifiche comuni che soddisfano un livello simile di sicurezza informatica. Poiché non esiste ancora una norma armonizzata per CRA, occorre scegliere la norma tecnica corretta e le tecnologie allo stato dell'arte che possono essere accettate. CRA promuove i principi del "Security by Design", che richiedono un approccio basato sul rischio (risk based approach).

Il processo di sviluppo del software (progettazione, sviluppo, testing, produzione, manutenzione) è quindi arricchito durante la fase di progettazione di un'analisi delle minacce (threat analysis) dalla quale si estraggono le esigenze in materia di minimizzazione dei rischi (la valutazione dei rischi deve essere fornita come documentazione tecnica). Durante lo sviluppo occorre prestare attenzione alla valutazione delle vulnerabilità anche per software open source e di terze parti, garantendo l'integrità e l'autenticità di ogni componente utilizzato. I test devono valutare la solidità e la sicurezza delle tecniche di attenuazione del rischio attuate. La manutenzione, che include il supporto per gli aggiornamenti di sicurezza e la gestione delle vulnerabilità, deve essere garantita per l'intera vita del prodotto.

Testing e monitoraggio della sicurezza dei propri prodotti. Le soluzioni Drivesec

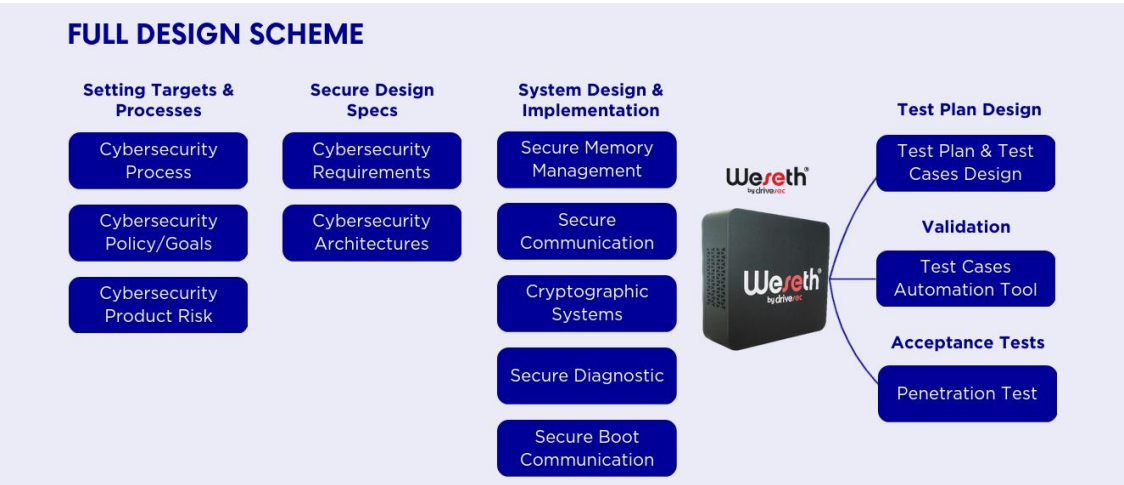
La valutazione della cybersecurity sta diventando un problema cruciale in tutti i settori dell'Internet of Things (IoT). Le normative richiedono ai produttori, ed ai loro fornitori, di considerare la resilienza alla cybersecurity come un requisito per i nuovi prodotti, di certificare l'applicazione delle migliori pratiche e di implementare un processo per monitorare la presenza di nuove vulnerabilità e minacce.

A differenza di molti altri ambiti, la cybersecurity non è una performance misurabile.

Per sua natura, la cybersecurity è un processo di gestione e mitigazione dei rischi a livelli accettabili, pertanto è un obiettivo in continua evoluzione.

Questo scenario crea la necessità di migliorare i processi e i metodi utilizzati per validare i requisiti di cybersecurity e testare la postura di sicurezza dei prodotti.

Drivesec propone un approccio innovativo che aumenta l'affidabilità, la velocità e la ripetibilità dei test di cybersecurity. Estende la copertura del perimetro testato, supporta l'automazione dei test e garantisce una corretta archiviazione delle conoscenze acquisite e delle lezioni apprese da una versione di prodotto ad una nuova. Per questo ha sviluppato WESETH®, una piattaforma per l'automazione dei test di cybersecurity che supporta le industrie nella capacità di monitorare efficacemente e da remoto la postura di sicurezza dei prodotti.



Registrati ora