



CRA: Cyber Resilience Act 2027



De Cyber Resilience Act (CRA) is een Europese cybersecuritywet die zich richt op het inherent verbeteren van de beveiliging van digitale producten en diensten. Hieronder vallen alle digitale hard- en software die in de tuinbouwsector worden ontwikkeld, geïmplementeerd, geïmporteerd en gedistribueerd.

1

Beveiligingseisen CRA

NIS2 & belangrijke data

2

3

Voor wie en welke
verplichtingen

Kwetsbaarheden &
meldplicht

4

Beoordelingsproces &
soorten producten

5

6

Risicomanagement

Leveranciersmanagement &
SLA's

7

8

Stappenplan

1. Beveiligingseisen

Secure-by-design:

Alle producten met digitale elementen moeten veilig worden ontworpen, ontwikkeld en geproduceerd. Dit vereist een risicogebaseerde aanpak vanaf de ontwerpfase van het product, waarbij het systeem wordt voorzien van veilige standaardinstellingen en minimale toegangsrechten.

Bijvoorbeeld: een klimaatcomputer of PLC die niet meer standaard met 'admin/admin' geleverd mag worden.

Updates & support:

Fabrikanten moeten minimaal een 5-jarige beveiligingsupdates leveren over hun producten en die updates moeten ondertekend en met een rollback-scherm worden geïnstalleerd. Updates moeten gebruiksvriendelijk te installeren zijn.

Bijvoorbeeld: een fabrikant die updates voor een apparaat die niet kan worden geïnstalleerd.



**Verdere inhoud exclusief
voor deelnemers
Cyberweerbaarheidscentrum
Greenport**

**Dit document bevat een versimpelde versie van de CxS richtlijnen*

2.1 Verschil met NIS2

Het verschil tussen NIS2 en CRA is dat NIS2 zich richt op het versterken van de cyberveiligheid van de belangrijkste infrastructuur en diensten. CRA richt zich op de verbetering van de cyberveiligheid van de productieve sector en de financiële markt.



**Verdere inhoud exclusief
voor deelnemers
Cyberweerbaarheidscentrum
Greenport**

**Dit document bevat een vereenvoudigde versie van de CRA-richtlijnen*