



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 de maakindustrie produceert, importeert en distribueert.

1

Beveiligingseisen CRA

2

NIS2 & belangrijke data

3

Voor wie & welke
verplichtingen

4

Kwetsbaarheden &
meldplicht

5

Beoordelingsproces &
soorten producten

6

Risicomanagement

7

Leveranciersmanagement &
SLA's

8

Stappenplan

1. Beveiligingseisen

Secure-by-design:

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 PLC die niet meer standaard met "admin/admin" geleverd mag worden.

Updates & support:

Fabrikanten moeten minimaal voor 5 jaar beveiligingsupdates leveren op aanvraag van de veiligheidsautoriteit (NEN, Dordtaland en andere) en de fabrikant moet de mogelijkheid bieden om updates te downloaden.



**Verdere inhoud exclusief
voor deelnemers
Cyberweerbaarheidscentrum
Maakindustrie ZH**



2.1 Verschil met NIS2

Het verschil met NIS2 is dat NIS2 zich richt op het beveiligen van de informatie van de onderneming, terwijl NIS1 zich richt op het beveiligen van de informatie van de overheid.



**Verdere inhoud exclusief
voor deelnemers
Cyberweerbaarheidscentrum
Maakindustrie ZH**

11 december 2024
beveiligingsmaatregelen

11 december 2024
aan de CMR

Dit document bevat vertrouwelijke informatie

