Auteur: Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technisch beveiliging, voor de toonaangevende vakbladen in Nederland en België. Ronald is te bereiken via: ronald@eygendaal.com

De Europese Machineverordening en Cybersecurity

De Machinerichtlijn, ingevoerd in 1995, bevordert vrije handel binnen de EU en waarborgt de veiligheid van machines voor bedrijven in de Europese Economische Ruimte (EER) die machines ontwerpen, bouwen of verkopen. Een CE-markering toont aan dat een machine voldoet aan de veiligheidsnormen. Op 20 januari 2027 treedt de nieuwe Machineverordening (EU) 2023/1230 in werking, met een sterke nadruk op cybersecurity. Deze verordening stelt strengere eisen aan verbonden machines, AI-systemen en veiligheidscomponenten om cyberrisico's, zoals aanvallen op industriële controlesystemen, te minimaliseren.

CE-markering en Machineverordening

De Machineverordening behoudt de verplichting om conformiteit aan te tonen en sluit aan bij andere EU-wetgeving, zoals de Cyber Resilience Act, die brede cybersecuritynormen stelt. De verordening richt zich op machines die door digitalisering fysieke of datagerelateerde schade kunnen veroorzaken, zoals complexe machines met mechanische, bouwkundige en geautomatiseerde componenten. Fabrikanten kunnen al vóór 2027 een EU-conformiteitsverklaring afgeven. Cybersecurity-eisen zijn vastgelegd in Bijlage III, met name in paragraaf 1.1.9 ("Bescherming tegen corruptie"), die vereist dat machines bestand zijn tegen kwaadwillige manipulatie.

Cybersecurity-eisen

De Machineverordening stelt specifieke eisen aan cybersecurity:

- Risicobeoordeling: fabrikanten moeten fysieke en cyberdreigingen analyseren, vooral bij AI-systemen met zelflerend gedrag.
- Beschermingsmaatregelen: machines moeten beveiligd zijn tegen netwerkaanvallen en softwaremanipulatie. Fabrikanten moeten cybersecurity waarborgen voor minimaal 10 jaar na marktintroductie, inclusief het loggen van cyberincidenten.
- CE-markering: digitale veiligheidscomponenten en software moeten voldoen aan cybersecurity-eisen, vooral in industriële netwerken waar kwetsbaarheden fysieke gevaren kunnen veroorzaken.
- Mens-machine-interactie: bij AI- of robotsystemen moet cybersecurity veilige interactie tussen mens en machine garanderen, in lijn met de EU AI Act.

Niet-naleving kan leiden tot boetes of marktverboden.

Impact op industrie, fabrikanten, gebruikers en IT

Met de nieuwe Machineverordening, de aankomende NIS2-richtlijn en de geplande Cyber Resilience Act is cybersecurity een wettelijke verplichting voor fabrikanten, integrators en exploitanten van machines. Fabrikanten moeten investeren in maatregelen zoals encryptie, toegangsbeheer en regelmatige software-updates. Dit verhoogt kosten, maar stimuleert innovatie in veilige technologieën en versterkt de concurrentiepositie op de EU-markt. Voor gebruikers en operators betekent dit veiligere apparatuur en minder risico op downtime door cyberincidenten.

Holistische Compliance

Hoewel er geen directe link is tussen machineveiligheid en informatiebeveiligingsnormen zoals ISO 27001 en IEC 62443, worden deze normen steeds relevanter voor digitale componenten van moderne machines. Zowel de Machineverordening als deze normen stellen eisen aan patchbeheer, kwetsbaarheidsbeheer en versiebeheer. Informatiebeveiliging helpt bij het beschermen van data die machines genereren of verwerken, wat cruciaal is voor verbonden systemen. Een geïntegreerde aanpak voorkomt tegenstrijdigheden in compliance en zorgt voor een samenhangend veiligheidsbeleid.