 TEKST Yvonne van Osch | **FOTO'S** Shutterstock, Laurens Hekkink

Cybersecurity centraal

10 vragen (en antwoorden) over de nieuwe Machineverordening

Over krap twee jaar wordt de Europese Machineverordening 2023/1230 van kracht. Het duurt nog even, toch is het zaak om nu alvast voor te sorteren. Laurens Hekkink, adviseur Informatiebeveiliging en Privacy bij CertificeringsAdvies Nederland, geeft antwoord op tien vragen over de betekenis en impact van de nieuwe verordening.

1. Wat houdt de Europese Machineverordening in?
"Op 20 januari 2027 vervalt de Machinerichtlijn 2006/42/EG die we kennen in de industrie. Daarvoor in de plaats komt de Europese Machineverordening 2023/1230. Deze verordening introduceert aangescherpte veiligheidseisen voor machines en de componenten daarvoor."

2. Waarvoor is de Machineverordening nodig?
"De verordening is nodig in verband met de toegenomen gevaren van cybercriminaliteit. Door het veel grotere gebruik van digitale technologie en gekoppelde

Waar het bij de nieuwe Europese Machineverordening om gaat, is dat je laat zien al het mogelijke te hebben gedaan om de veiligheid te waarborgen van je mensen, je klanten en je productieproces.

toepassingen bij operationele processen in de industrie is het aantal potentiële toegangspunten voor cybercriminelen sterk uitgebreid. Een Europese verordening geeft de mogelijkheid om een nieuwe standaard op te leggen die geldt voor alle EU-lidstaten."

3. Wat zijn de voornaamste veranderingen?
"Een belangrijke verandering is dat nu ook software tot de veiligheidscomponenten van machines en installaties gerekend wordt. Behalve om verplichte beveiliging tegen fysieke gevaren van machines zoals beknelling, lawaai en dergelijke, gaat het nu dus ook om maatregelen tegen cyberrisico's. De verordening is bovendien – anders dan bij de Machinerichtlijn, die naar nationale wetgeving werd omgezet – direct voor de hele EU van kracht."

4. Welke cyberrisico's zijn er in de bulksector?
"Je moet vooral denken aan malware, ransomware en spyware, dus schadelijke software die via een lek in een netwerk of apparaat naar binnen kan komen. Waren hackers voorheen vooral geïnteresseerd in financiële instellingen, nu deze hun beveiliging op orde hebben, zie je de risico's verschuiven. In feite is elk bedrijf dat van digitale netwerken gebruikmaakt kwetsbaar."

Laurens Hekkink werkt als adviseur informatiebeveiliging bij CertificeringsAdvies Nederland in Den Bosch. "Wie zich druk moeten maken over de nieuwe Europese Machineverordening? Bouwers van machines en componenten natuurlijk, maar ook verkopers en gebruikers van die machines."

HEY OPERATOR, WHERE'S YOUR CRANE?

Hoe ingrijpend cybercriminaliteit kan zijn, bewezen cyberonderzoekers Maggi en Balduzzi in 2018 in de Italiaanse regio Lombardije. Met bijna kinderlijk gemak namen de twee op diverse bouwlocaties de controle over hijskranen over. Afstandsbedieningen op radiofrequentie, veel gebruikt in constructie, productie en transport, bleken de zwakste schakel in veiligheidskritische IoT-toepassingen (Internet of Things). Analyses lieten zien dat er op verschillende niveaus beveiligingsfuncties ontbraken en leveranciers obscure eigen protocollen gebruikten in plaats van standaarden. Het onderstreepte het belang van de internationale regelgeving die er nu is. De onderzoekers deelden hun bevindingen in een YouTube-filmpje met de titel Attacking Industrial Remote Controllers. *Hey operator, where's your crane?*

De nieuwe Europese Machineverordening 2023/1230 introduceert aangescherpte veiligheidseisen voor machines en de componenten daarvoor.

5. Wat is het doel van cybercriminelen?
"Het doel is meestal geld. Criminelen versleutelen na een aanval je computersystemen en eisen losgeld voor herstel. Dit is bijvoorbeeld een paar jaar geleden gebeurd bij één van de transportbedrijven voor Albert Heijn, met lege kaasschappen tot gevolg. Behalve om geld kan het gaan om het verkrijgen van gevoelige informatie, zoals klantgegevens, bedrijfsstrategieën of technische data, om deze te verkopen of te exploiteren. Soms richten aanvallers zich op het domweg verstoren van productieprocessen. Dan heb je het over sabotage of pesterij."

6. Waar komen criminelen vandaan?
"In verreweg de meeste gevallen heb je te maken met een criminele organisatie. Bij gespecialiseerde, innoverende bedrijven kan het gaan om spionage in opdracht van een concurrent. Je kunt ook te maken krijgen met een wat wij noemen 'statelijke actor'. Dan moet je denken aan fysieke spionage door hooggekwalificeerde werknemers uit het buitenland, meestal Rusland of China, die gegevens komen stelen. Chipfabrikant ASML heeft het dit jaar voor de derde keer mee moeten maken. Een enkele keer is sprake van een bedreiging van binnenuit, bijvoorbeeld een werknemer of ex-werknemer die nog een appeltje met de baas te schillen had."

7. Wie moeten zich druk maken over de Machineverordening?
"Bouwers van machines en componenten zoals sensoren en monitoren, maar ook verkopers en gebruikers. Op het moment dat iets misgaat, zijn de verantwoordelijkheden natuurlijk altijd extra interessant. Gaat het om een mechanisch defect aan de transportband of schudmachine, is er een probleem met de elektriciteit of is het de software van een monitor of besturingspaneel die hapert? Reken maar dat bedrijven zullen proberen de schade van een storing of defect op andere partijen af te wentelen. Verordeningen, ISO-normen en andere kwaliteitsinstrumenten dwingen je de risico's van alle processen door te lichten en verantwoordelijkheden af te bakenen."

8. Wat kun je doen tegen cybergevaren?
"Een heleboel kun je zelf doen. Denk bijvoorbeeld aan:
a) Regelmatige software- en beveiligingsupdates.
b) Een goede wachtwoorddiscipline. Onze online voetafdruk wordt steeds groter, je kunt nauwelijks meer contact met een bedrijf hebben of je moet inloggen. Stel dat hackers met een bruteforce-aanval - een soort geautomatiseerd giswerk gebaseerd op eerder gelekte wachtwoorden, de inloggegevens van één van je accounts achterhalen. Het eerste wat ze doen is dit op heel veel andere accounts testen. Gebruik

dus moeilijke wachtwoorden, neem niet hetzelfde wachtwoord voor verschillende accounts en vernieuw je wachtwoorden om de zoveel tijd.

c) In het verlengde hiervan: scheiden van netwerken. Laat de monitor van je installatie niet op hetzelfde netwerk draaien als bijvoorbeeld het mailverkeer van kantoorpersoneel, dat vaak veel contacten naar de buitenwereld heeft. Zo beperk je de risico's bij mogelijke netwerkaanvallen. Elk lijntje naar buiten kan een risico zijn.

d) Regelmatige back-ups. Wij raden altijd aan er drie te maken, op twee verschillende opslagplaatsen waarvan één op een andere locatie, bijvoorbeeld offline op een harde schijf. Je vermijdt dan bij een aanval niet alleen het risico om losgeld te moeten betalen voor herstel van je gegevens, je bent ook veilig in het geval dat een online back-upsysteem, zoals bij Microsoft, Amazon of Google, tegelijk met de aanval gecorrumpeerd raakt."

9. En ben je er dan uit?

"Nee, dit is een begin. Bij elk traject van nieuwe wetgeving komt veel kijken. Je moet de eisen begrijpen, risico's inventariseren, informatie inwinnen, opties voor maatregelen onderzoeken en afwegen, maatregelen implementeren, werknemers op de hoogte brengen en trainen, afspraken maken hoe om te gaan met informatie van klanten en leveranciers, eisen aan leveranciers opstellen, kwaliteit monitoren, evalueren, enzovoort. Als wij klanten hierin bijstaan, is de doorlooptijd - afhankelijk van de eigen kennis en inzet - gemiddeld zo'n negen tot twaalf maanden."

10. Waar staat de Machineverordening in het landschap van wetten en regels?

"Wetten, regels en normen kunnen vaak bij elkaar worden ingeprikt. Je had bijvoorbeeld al de Cyberbeveiligingswet (waarin per 2025 de Europese NIS2-richtlijn wordt geïmplementeerd) voor zogenoemde kritieke organisaties zoals transportbedrijven, chemiebedrijven en groothandels in levensmiddelen. Al die organisaties gebruiken ook machines waar ze op moeten kunnen vertrouwen, en daar bestaan sinds lang de verplichte CE-markeringen voor. En ben je als bedrijf reeds gecertificeerd voor de ISO 27001, die gaat over informatieveiligheid, dan heb je ook een deel van het werk voor de Machineverordening (en NIS2) al op orde, kortom: het grijpt in elkaar. Waar het bij de Machineverordening om gaat, is dat je kunt laten zien al het mogelijke te hebben gedaan om de veiligheid te waarborgen van je mensen, je klanten en je productieproces." BULK

ZOEK EEN PARTNER

Het is niet onmogelijk om als bedrijf zelf te bepalen hoe je aan de eisen van de Machineverordening 2023/1230 kunt voldoen. Toch is het waarschijnlijk handiger en veiliger daarvoor een adviseur in de arm te nemen. Kijk in hoeverre je terecht kunt bij een brancheverenigingen als FME (technologische industrie), GMV (machinebouwers agri en food), DMFI (food), Metaalunie (Bouw- product- en machinebouw) of FEDA (aandrijftechniek en automatisering). Anders zijn er diverse commerciële partners die zich aanbieden voor advies en begeleiding. Geschikte bureaus zouden behalve grote partijen als E-Wise en KPMG onder andere kunnen zijn Certificerings-Advies Nederland, Pilz, Kader, KienIA en NEN.

Praktische en actuele informatie rond de nieuwe Europese Machineverordening vind je ook op de website www.platform-machineverordening.nl. Zowel grote als kleine bedrijven kunnen via de website ontdekken welke stappen voor hen relevant zijn.