



Helft maakbedrijven vreest dit jaar voor cyberaanval

27 april 2021, 10:00

Marie-France Rousseau

De helft van de maakbedrijven in ons land vreest voor een cyberaanval in de komende twaalf maanden. Dat blijkt uit de eerste studie over cyberveiligheid in de maakindustrie in ons land. Zevenenzeventig bedrijven namen deel. De studie werd uitgevoerd door technologiefederatie Agoria in samenwerking met Howest, UGent en kenniscentrum Sirris.

In België zijn er zo'n vijfduizend industriële maakbedrijven. Daarvan heeft een goeie zestig procent de stap gezet naar Industrie 4.0, een trend van automatisering en gegevensuitwisseling die gebruikt wordt bij industriële fabricagetechnieken. Maakbedrijven investeren toenemend in slimme operationele technologieën, geconnecteerde machines en robots om hun productieprocessen te verbeteren. Dit industrieel 'Internet of Things' komt echter ook steeds meer in het vizier van cybercriminelen.

In een internationale bevraging van Fortinet geven achteenvijftig procent van de grote industriële bedrijven aan dat ze het afgelopen jaar te maken kregen met een veiligheidsinbreuk op hun systemen voor operationele technologie (OT). Deze operationele technologie omvat alle hardware en software die fysieke toestellen en processen controleren en beheren. Hoe is het gesteld met de cyberveiligheid van maakbedrijven in België? Om dit te achterhalen, organiseerden Agoria, Howest, UGent en Sirris eind 2020 een diepgaande bevraging onder zevenenzeventig Belgische maakbedrijven.

In de studie is vastgesteld dat er bij de Belgische maakbedrijven te weinig bewustzijn en kennis is over cybersecurity en de risico's die de convergentie tussen IT en operationele technologie (OT) met zich meebrengt. Daardoor is er maar zelden een veiligheidsbeleid rond operationele technologie. Is het er wel, dan is het vaak niet geïntegreerd in het IT-veiligheidsbeleid of is het eraan ondergeschikt.

Danny Goderis, Chief Digital Officer van Agoria: "Het was even schrikken toen we vaststelden dat dertig procent van de kritische hardwarecomponenten en bijhorende besturingssystemen meer dan tien jaar oud zijn. Bovendien voeren bedrijven nauwelijks updates uit. Hierdoor ligt de productieomgeving te grabbel voor cybercriminelen. Als het dan fout loopt, blijkt dat slechts één op vier van de respondenten beschikt over een goed rampenplan dat zowel de omgeving van de IT als de OT (operationele technologie) afdekt."

Enkele van de meest opmerkelijke cijfers:

- 50% van de bedrijven vreest dat hun bedrijf het komende jaar slachtoffer wordt van een cyberaanval.
- 48% van de respondenten zegt niet over interne kennis te beschikken als ze geconfronteerd worden met een cyberaanval.
- 40% van de bevroegde bedrijven schenkt geen aandacht aan cybersecurity bij industriële aankopen.
- 77% test de beveiliging van de operationele technologie nooit.
- 32% van de bedrijven scant hun netwerk op kwetsbaarheden.
- 31% van de respondenten heeft geen idee over de grootteorde van de leeftijdscategorie van de oudste PLC's (programmable logic controllers of programmeerbare logische sturing).
- 35% werkt met PLC's van tien jaar of ouder.
- 34% heeft een beleid dat zowel IT als operationele technologie (OT) dekt.
- 55% van de respondenten geeft aan geen standaarden te gebruiken of te overwegen met betrekking tot cybersecurity van de operationele technologie.
- 48% voert zelden tot nooit updates uit.

Maar 10 procent van de ondervraagden toont wel hoe het moet. Deze kopgroep van best scorende bedrijven:

- heeft een beveiligingsbeleid voor IT en operationele technologie (OT).
- test regelmatig de beveiliging.
- creëert bewustzijn rond veiligheid door minstens jaarlijks activiteiten te organiseren.
- updatet regelmatig de systemen.
- schenkt aandacht aan cybersecurity bij de aanschaf van industriële apparatuur.
- hanteert een minimale vorm van segmentatie.
- beschikt intern over een minimale cyberveiligheidsexpertise, waarop ze een beroep doet bij een cyberaanval.

[Agoria](#), [Howest](#), [UGent](#) en [Sirris](#) roepen nu alle maakbedrijven op om deze kopgroep te vervoegen.

Meer informatie

Het volledige rapport van de studie en een whitepaper met tien gedetailleerde aanbevelingen om aan de slag te gaan, kan worden gedownload op <https://www.agoria.be/nl/studie-Cybersecurity-in-de-maakindustrie>.

Authors



Marie-France Rousseau