AUDIT MAGAZINE

ARTIKELEN | 1 JULI 2020

INDUSTRIE 4.0: DE RISICO'S EN AANBEVELINGEN

Auteur: Jouke Albeda MSc RE CISSP
Beeld: Adobe Stock - Marcos Mayer
Leestijd: 5 min

UIT DE IT-AUDITOR
Dit artikel is eerder gepubliceerd op deauditor.nl

Door de opkomst van nieuwe technologieën ontwikkelt zich een nieuwe vorm van industriële productie, aangeduid als 'smart manufacturing' of 'Industrie 4.0'.

Het gebruik van deze nieuwe technologieën brengt vooruitgang, maar creëert ook nieuwe risico's. De uitdagingen die de introductie van deze technologieën met zich meebrengt zijn in heel Europa aan de orde. Daarom heeft het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) in november 2018 een onderzoeksrapport gepubliceerd met aanbevelingen en maatregelen voor de beveiliging van Industrie 4.0. Het rapport draagt de titel *Good practices for Security of Internet of Things in the context of Smart Manufacturing*.[1] Het is een nuttig en praktisch bruikbaar rapport voor de auditor.

Nieuwe technologieën

De opkomst van nieuwe technologieën zoals internet of things (IoT), artificial intelligence (AI), machine learning (ML) en robotic process automation (RPA) brengt nieuwe risico's met zich mee. De EU-brede problematiek van een explosief

groeiende hoeveelheid data die wordt verwerkt heeft ENISA in november 2017 getriggerd een beveiligingsrichtlijn (Baseline Security Recommendation for IoT) op te stellen.[2] Het doel was om bedrijven te helpen de risico's van deze nieuwe technologieën te beheersen. Enkele jaren verder zien we dat deze technologieën zich verder doorzetten. Zo begint de digitale accountant onderdeel van de accountantscontrole te worden, gebruikt de politie kunstmatige intelligentie om oude politiezaken te onderzoeken, wordt blockchain steeds meer gebruikt door verzekeraars en banken en implementeert BMW smart manufacturing in hun logistieke proces.

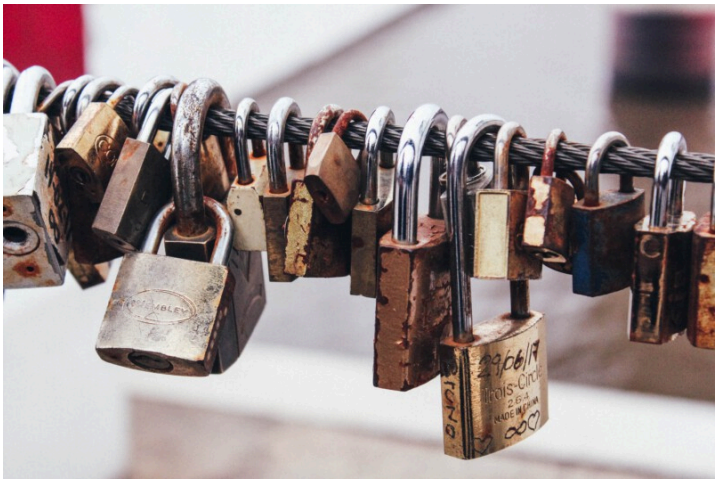
Het doorzetten van de trend 'Industry 4.0' vormde voor ENISA de aanleiding voor een vervolgonderzoek. Het is een uitgebreide literatuurstudie waarbij gebruik is gemaakt van meer dan vijftig wereldwijd gebruikte standaarden, frameworks en initiatieven van onder andere ISO, IEC en NIST. Het rapport geeft voor alle aanbevolen maatregelen verwijzingen naar die standaarden, zodat je inzicht krijgt in de overlappingen. Ook zijn de ontwikkelingen in wet- en regelgeving meegenomen en wordt specifiek verwezen naar de AVG. Zodoende neemt deze 'good practice'-maatregelen mee die nodig zijn om te voldoen aan meerdere standaarden, frameworks en wet- en regelgeving.

De toenemende automatisering en onderlinge communicatie tussen apparaten en systemen zorgen ook voor nieuwe kansen voor auditors

Industrie 4.0 en smart manufacturing

Industrie 4.0 is een recent ontstane aanduiding voor de nieuwe 'slimme' industriële productie met inzet van de genoemde nieuwe technieken zoals IoT, AI en ML. Door integratie van informatietechnologie (IT) en operationele technologie (OT) vindt er verdere automatisering plaats in de industriële wereld zoals we deze kennen. Het gebruik van deze opkomende technologieën en het gebruik van sensoren en verbonden apparaten, laten systemen nog efficiënter en effectiever functioneren. Ook kunnen deze technologieën zelf beslissingen nemen op basis van beschikbare informatie. Deze innovaties leiden tot smart manufacturing, kortom, slimmere industriële productie. Apparaten communiceren onderling en kunnen de productiviteit verhogen en de productiekwaliteit verbeteren.

Uiteraard brengen de nieuwe technologieën nieuwe risico's met zich mee. Tegelijkertijd zorgen de toenemende automatisering en onderlinge communicatie tussen apparaten en systemen ook voor nieuwe kansen voor auditors. Er komen namelijk meer geautomatiseerde controles en er ontstaan meer data over cruciale stappen binnen industriële processen. Voor de auditor is een nieuwe rol weggelegd als degene die deze controles evalueert en de gedetailleerde procesdata analyseert. In deze rol geeft de auditor zekerheid dat het bedrijf het industriële proces onder controle heeft.



De ‘good practices’

Zoals gezegd, heeft het vervolgonderzoek van de ENISA geleid tot een document met good practices. Het document beschrijft de vernieuwde industriële IoT (met Industrie 4.0 en smart manufacturing), geeft voorbeelden van uitdagingen in de beveiliging waar we mee te maken krijgen en komt op gestructureerde wijze uit op de verschillende middelen/assets die (kunnen) meespelen in smart manufacturing. Ook komen verschillende voorbeelden van dreigingsscenario’s aan bod. Via een uitgebreide dreigingen-en risicoanalyse komt ENISA vervolgens tot een set aanbevolen maatregelen.

Deze maatregelen zijn geordend naar de volgende drie gebieden:

- *Beleid en procedures*
  Binnen organisaties is voldoende aandacht nodig, van voldoende niveau, voor cybersecurity. Dit moet geregeld worden in beleid en procedures. Ontwerp- en beheerrichtlijnen zijn hier onderdeel van.
- *Organisatorische maatregelen*
  Binnen de organisatie moet de governance op orde zijn en moeten beveiligingsprincipes worden vastgesteld. Bepaald moet worden wat de regels zijn en waar de verantwoordelijkheden liggen: hoe om te gaan met cybersecurity-incidenten, met kwetsbaarheden en hoe wordt de veiligheid gewaarborgd?
- *Technische maatregelen*
  Belangrijk in het technologisch domein zijn de technische maatregelen. Hierbij worden beveiligingsmaatregelen aangevuld met gerelateerde maatregelen, zoals maatregelen ten behoeve van infrastructuur en continuïteit.

De maatregelen zijn meer principle-based dan rule-based beschreven. Het document geeft dus geen recept voor een blinde implementatie van te nemen maatregelen, maar beschrijft zo concreet mogelijk de onderliggende principes.

Deze good practice geeft de auditor houvast op het gebied van risico’s en maatregelen die van groot belang kunnen zijn voor de betreffende onderneming

Wet- en regelgeving

Door de komst van de AVG is de beveiliging van eventuele persoonsgegevens een extra aandachtspunt bij het verwerken van grote hoeveelheden data. Naast de AVG die in de EU geldt, zie je ook wereldwijd meer aandacht voor cybersecurity. In de Verenigde Staten is in 2017 bijvoorbeeld de ‘US IoT Cybersecurity Improvement Act’ geïntroduceerd.[3] Bij het opstellen van regelgeving wordt dan ook gekeken naar nationale en internationale standaarden, zoals die van NIST en ISO.

Ook bij de AVG is er een zekere overlapping met nationale en internationale standaarden. Het voldoen aan een breed scala aan standaarden, zoals geïncorporeerd in de good practices van ENISA, helpt je om snel, soms ook direct, te voldoen aan huidige wet- en regelgeving en wet- en regelgeving die gaat komen. De ENISA heeft in de studie gebruikgemaakt van meer dan vijftig standaarden, initiatieven en frameworks van onder andere ISO, IEC en NIST. Het ENISA-rapport verwijst bij elke voorgestelde maatregel naar de relevante standaarden. Hierdoor kun je als gebruiker van het rapport de overlappingen vanuit compliance-oogpunt zelf bepalen. Omdat de AVG enkele specifieke eisen stelt zijn deze apart meegenomen in het rapport.

Relevantie voor de auditor

De auditor kan verschillende rollen vervullen, waaronder de audit-, de advies-, de quality assurance- en de implementatierol. Voor alle rollen kan dit document zeer waardevol zijn, zeker in een omgeving die gebruikmaakt van IoT. In de implementatie-rol – voor het implementeren van de good practice zelf – zijn de gestructureerde aanpak en de

definiëring van middelen, dreigingen, risico's en maatregelen te gebruiken in de eigen risicoanalyse en kunnen ze uitdagen tot een uitgebreidere analyse. Door de algemeen geformuleerde maatregelen in het rapport te concretiseren voor de specifieke situatie ontstaat een veilige IoT-productieomgeving. Vanuit een quality-assurancerol kan de auditor de structuur heel mooi gebruiken om bij een implementatie-project waarbij gebruik is gemaakt van smart manufacturing te toetsen of de juiste risico's op de juiste manier worden afgedekt.

Ook is het document bruikbaar om vanuit een auditrol de risicoanalyse en de beveiligingsmaatregelen te toetsen. Deze good practice geeft de auditor houvast op het gebied van risico's en maatregelen die van groot belang kunnen zijn voor de betreffende onderneming. Kortom, het rapport is een welkome en veelzijdig bruikbare handreiking voor de auditor!

Noten

1. www.enisa.europa.eu (geraadpleegd op 14 januari 2019).
2. www.enisa.europa.eu (geraadpleegd op 14 januari 2019).
3. www.leidenlawblog.nl (geraadpleegd op 14 januari 2019).

Over
Jouke Albeda is IT-auditor en ondersteunt vanuit zijn bedrijf Contrisity klanten op het gebied van audit, risk en compliance. Daarvoor werkte hij als risk- en compliancemanager bij Datacenter.com en bij EY en BDO in de externe (IT-)auditpraktijk.

Tags: IT-audit

Bron url: https://auditmagazine.nl/artikelen/industrie-4-0-de-risicos-en-aanbevelingen/