De volgende uitdaging van de IT-auditor

Operationele Technologie

16 juni 2020

Stan van Bommel

Dankzij de Industrial Internet of Things (IIoT) speelt IT een steeds grotere rol binnen de Operationele Technologie (OT). Nieuwe technologieën zoals artificial intelligence, cloud computing en big data doen hun intrede en hebben direct impact op de monitoring en besturing van industriële processen. [ENIS18] Het zorgt niet alleen voor meer efficiency, maar creëert ook nieuwe risico's. Dit wekt de interesse van hackers én de overheid. Deze bijdrage geeft aan hoe de IT-auditor hierop kan aansluiten.

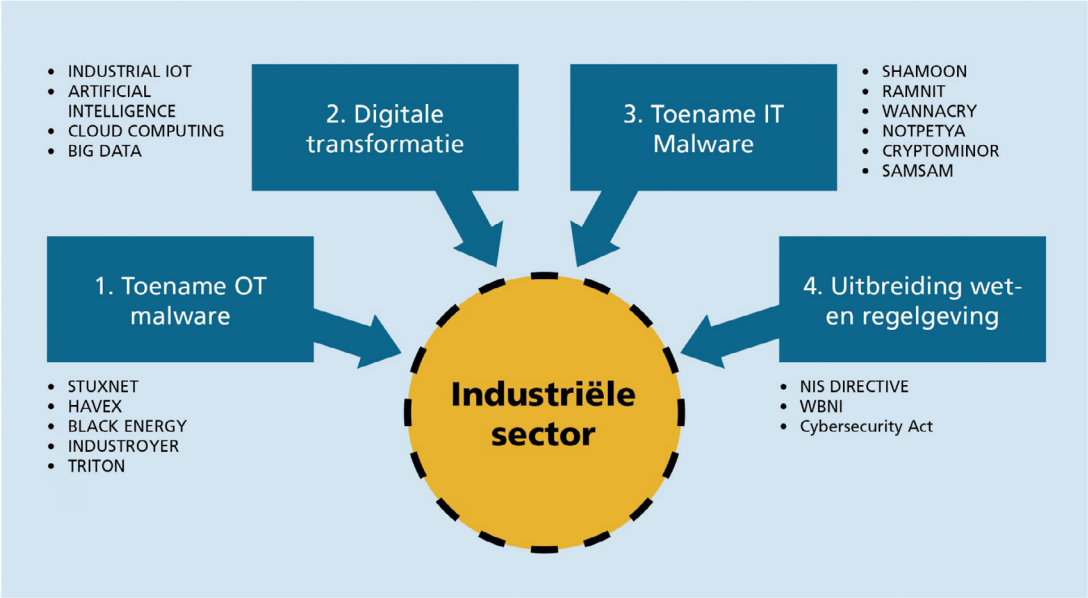
Door de opkomst van nieuwe technologieën vindt een toename van de automatiseringsgraad plaats. Deze 'vierde industriële revolutie' stelt de OT voor de grootste uitdaging ooit. De wijze waarop de beheersing van fysieke processen en machines plaatsvindt, verandert snel. De revolutie kenmerkt zich door de toepassing van IIoT-apparaten en doordat organisaties zich transformeren tot ICT-bedrijven. Dit biedt unieke kansen voor organisaties, maar wekt ook de interesse van hackers. Een veilige samenwerking van IT met OT is dan ook essentieel. De IT-auditor heeft als uitdaging om tijdig aan te haken bij de ontwikkelingen in het OT-domein, kennis over OT-omgevingen op te doen, en de specifieke beveiligingsrisico's die hierbij spelen in beeld te krijgen. [ALBE19]

De volgende ontwikkelingen zijn *drivers* voor de IT-auditor om nu ook binnen het OT-domein actief te worden.
Binnen het vakgebied van OT vinden op dit moment vier belangrijke ontwikkelingen plaats, te weten:

- **Toename OT-malware.** Het is nog maar tien jaar geleden dat Stuxnet de security-wereld op zijn kop zette. [WIJSM16] Dit was de eerste gerichte cyberaanval die op OT plaatsvond. Sindsdien lukt het statelijke actoren regelmatig om (delen van) vitale infrastructuren van landen stil te leggen.
- **Digitale Transformatie.** Ten tweede innoveert de industrie snel en doen nieuwe technieken hun intrede. De huidige OT-omgevingen zijn niet meer te vergelijken met die van een paar jaar terug. OT en IT vloeien steeds meer in elkaar over.

- **Toename IT-malware**. De digitale transformatie biedt hackers nieuwe kansen, waardoor IT-gerelateerde criminaliteit doordringt in de OT-omgevingen. Recent voerde een hacker bijvoorbeeld een ransomware-aanval uit op een aardgasfabriek in de Verenigde Staten. De hacker kreeg via de IT-omgeving toegang tot de OT en versleutelde vervolgens in beide omgevingen data. De fabriek lag twee dagen stil. [CISA20]
- **Uitbreiding wet- en regelgeving**. De ontwikkelingen wekken ook de interesse van de overheid met als gevolg dat steeds meer aanbieders van essentiële diensten (AED's) moeten voldoen aan de Wet beveiliging netwerk- en informatiesystemen (Wbni), waardoor ze zelfs onder toezicht valt van de bevoegde autoriteit voor de sector waar de organisatie toe behoort.[1] Een AED levert een essentiële dienst als de continuïteit hiervan van vitaal belang is voor de Nederlandse samenleving.

Afbeelding 1 geeft deze drivers schematisch weer en de volgende paragrafen geven een nadere toelichting.

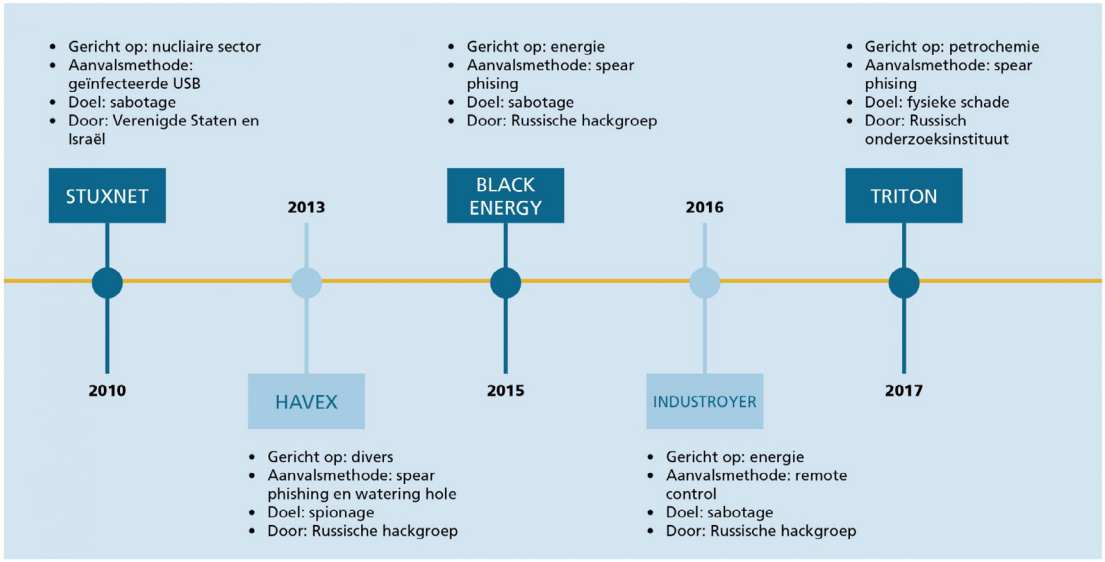


Tabel 1: Drivers voor de IT-auditor

Driver 1: Toename OT-malware

Essentiële diensten zoals de levering van water en energie, moeten te allen tijde beschikbaar zijn. Van oorsprong richtten de ontwerpen van traditionele OT-omgevingen zich dan ook op fysieke dreigingen. Maatregelen om vroegtijdig potentiële cybersecurity-incidenten te detecteren en tijdig te reageren, kregen hierdoor minder aandacht. Lange tijd leek aandacht voor deze digitale weerbaarheid niet nodig te zijn. Het keerpunt kwam in 2010, toen specifieke malware gericht op OT-omgevingen aanzienlijke schade veroorzaakte in het nucleaire programma van Iran. Stuxnet was hiermee de eerste cyberaanval door een statelijke actor op een OT-omgeving, die brede bekendheid kreeg. De wereld kreeg een indruk hoe toekomstige aanvallen er uit zouden komen te zien. Nieuwe cyberaanvallen door statelijke actoren en hieraan gelieerde actoren volgden

dan ook snel. Na Stuxnet zijn de vijf bekendste: Havex (Dragon Fly), Black Energy, Industroyer (Crashoverride) en Triton (Trisis). [ROCC18] Zie afbeelding 2 voor meer uitleg (in een aantal gevallen zijn de vermelde aanvalsmethode of aanvaller gebaseerd op vermoedens).



Tabel 2: OT-malware (Bron: [ROCC18])

Het Cybersecuritybeeld Nederland 2019 geeft aan dat door de veranderende geopolitieke verhoudingen de dreiging van sabotage en spionage verder toeneemt naarmate Nederland onderdeel wordt van, of betrokken raakt bij, geopolitieke conflicten. [NCSC19] In dit kader is Nederland vanwege het lidmaatschap en de vestigingsplaats van internationale instituties een interessant doelwit. Andere redenen zijn de Nederlandse rechtszaak over het neerhalen van vlucht MH17 met een luchtdoelraket en de cruciale rol die Nederland speelde bij de Stuxnet-aanval. [MODD19] Het lijkt erop dat het dus niet wachten is óf Nederland digitaal aangevallen wordt, maar wannéér.

In het algemeen is de kans op een cyberaanval op een OT-domein de afgelopen jaren flink gestegen. Veel OT-domeinen bevatten systemen van twintig jaar of ouder die hier in hun ontwerp geen rekening mee hielden, omdat niet kon worden voorzien dat ze ooit met de buitenwereld verbonden zouden worden. Het tegen moderne aanvalstechnieken weerbaar maken van deze legacy-omgevingen vraagt daarom bijzondere aandacht van de IT-auditor. De IT-auditor kan zijn/haar opdrachtgever zekerheid verschaffen door onder meer de volgende vragen te onderzoeken:

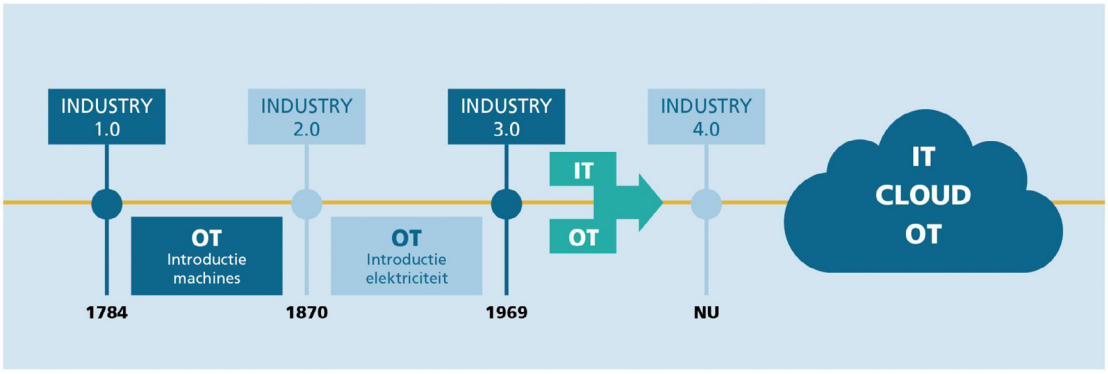
- Worden de koppelingen tussen het IT- en het OT-domein voldoende beheerst?
- Worden patches weloverwogen uitgevoerd? Worden alternatieve mitigerende maatregelen ingevoerd indien patches niet mogelijk zijn?
- Signaleren pentesters risico's en worden de gevonden issues tijdig opgelost?
- Vindt er logging en monitoring op de OT-omgeving plaats om cyberaanvallen te detecteren en wordt indien nodig adequaat op meldingen gereageerd?
- Houdt het *security management* rekening met de dreiging van OT-malware?

Met betrekking tot logging, monitoring en detectie is een interessante ontwikkeling dat beveiligingsspecialisten in operationele technologie steeds vaker diensten aanbieden voor het 24×7 monitoren van industriële systemen. Deze diensten zijn vergelijkbaar met de Security Operations Centers (SOC's) uit de IT-wereld. [AUTO19]

Driver 2: Digitale transformatie

OT gebruikt Industrial Control Systems (ICS's) om de fysieke toestand van een systeem te bewaken of te wijzigen. ICS's kom je overal tegen: van distributie van elektriciteit tot vervoer van water via leidingen en personen via spoorwegen. Om data uit ICS's te kunnen gebruiken voor besluitvorming en het voorspellen van onderhoud, maken organisaties steeds vaker gebruik van IIoT-apparaten. Hierbij koppelen organisaties apparaten aan internet, en gebeuren monitoring en aansturing op afstand. Technologieën als artificial intelligence, cloud computing en big data doen hun intrede. De industriële sector sluit steeds meer aan op IT en de digitale transformatie is begonnen. Industry 4.0 is gestart (zie afbeelding 3). In dit kader kan de IT-auditor onder meer aan zijn/haar opdrachtgever zekerheid verschaffen door onder andere de volgende vragen te onderzoeken:

- Worden nieuwe technologieën *risk-based* geïmplementeerd? En wordt hierbij naar de keten van leveranciers en onderleveranciers gekeken?
- Worden er *security by design*-principes gehanteerd bij het implementeren van nieuwe OT-technologie?
- Zijn nieuwe OT-componenten veilig geïntegreerd met de bestaande OT-componenten?



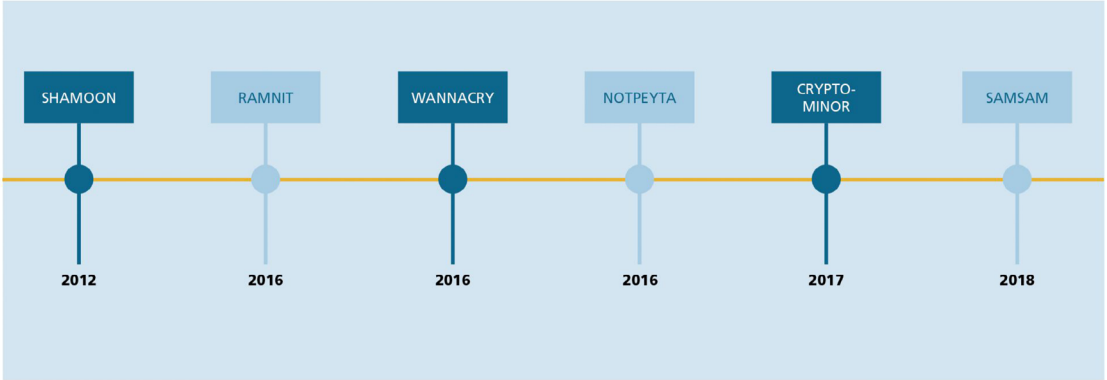
Tabel 3: De industriële revolutie: Industry 4.0

Driver 3: Toename IT-malware met impact op de industriële sector

Het aantal cyberaanvallen neemt niet alleen toe, maar verandert ook in opzet en complexiteit. Historisch gezien waren het statelijke actoren die specifieke aanvallen op OT-omgevingen uitvoerden, met het doel maatschappelijke ontwrichting te veroorzaken.

Sinds 2018 zien we de trend dat naast statelijke actoren en hieraan gelieerde actoren ook cybercriminelen vanuit een commercieel oogpunt ransomware-aanvallen uitvoeren binnen de industriële sector, zie afbeelding 4. [ROCC18] Een belangrijk aandachtspunt voor de IT-auditor is het bewaken van de optimale samenwerking tussen IT en OT. Naast de onderzoeksvragen van driver 1 kan de IT-auditor in dit kader zijn/haar opdrachtgever zekerheid verschaffen door onder meer de volgende vragen te onderzoeken:

- Is er een integraal beveiligingsbeleid met zowel aandacht voor IT als OT?
- Is er een overall architectuurontwerp met zowel aandacht voor IT als OT?
- Is er adequate monitoring op en detectie van IT-cyberaanvallen die impact kunnen hebben op de OT-omgeving?
- Houdt *security management* rekening met de dreiging van malware?
-



Tabel 4: IT-malwareaanvallen (na Stuxnet) op de industriële sector (Bron: [ROCC18])

Driver 4: Uitbreiding wet- en regelgeving

Bedrijfsleven en overheid werken nauw samen om de digitale weerbaarheid van essentiële diensten te borgen. Om dit mogelijk te maken, worden AED's steeds meer onder formeel toezicht van onder andere de Inspectie Leefomgeving en Transport en Agentschap Telecom gesteld. Om dit mogelijk te maken bracht Europa hiervoor de NIS Directive uit. Nederland vertaalde deze in 2018 naar de Wbni. De wet schrijft voor, dat aanbieders van vitale processen passende en evenredige technische en organisatorische maatregen moeten nemen om hun netwerk en informatiesystemen te beveiligen. Eventuele incidenten met aanzienlijke gevolgen moeten zij melden bij de overheid. De Wbni noemt deze verplichtingen de zorg- en meldplicht. Daarnaast trad op 27 juni 2019 de Europese 'Cybersecurity Act' (CSA) in werking met als doel dat de EU grensoverschrijdende cyberaanvallen beter het hoofd kan bieden. [VREE19] Hiermee komt vrijwillige certificering van producten, processen en diensten een stap dichterbij. Lidstaten hebben tot medio 2021 om de kaders uit te werken. In 2024 evalueert de Europese Commissie de Cybersecurity Act en bepaalt dan onder andere of certificering verplicht zal worden. In dit

kader kan de IT-auditor zijn/haar opdrachtgever zekerheid verschaffen door onder meer de volgende vragen te onderzoeken:

- Voldoet de organisatie aan de zorg- en meldplicht zoals opgenomen in de Wbni? Ook voor organisaties die (nog) niet onder deze wet vallen, is de zorgplicht een goed uitgangspunt voor de IT-auditor.
- Volgt de organisatie de ontwikkelingen rondom de Wbni en CSA en bereidt zij zich hier indien nodig op voor?
- Is de organisatie aangesloten op de informatievoorziening vanuit de overheid en industriële sector met betrekking tot actuele dreigingen?

Tot slot

Om een eerste indruk van de beveiliging van een OT-domein te verkrijgen, kan de IT-auditor de 'Checklist beveiliging van ICS/SCADA-systemen' van het NCSC gebruiken. [NCSC15] Deze checklist bevat een overzicht van organisatorische en technische good practices. Een vervolg op het verkregen inzicht is het formuleren van onderzoeksvragen. Deze bijdrage beschrijft vier drivers die voor de IT-auditor aanleiding kunnen zijn om nu actief te worden binnen het OT-domein. De drivers zijn de toename van OT-malware, de digitale transformatie , de toename van IT-malware en de uitbreiding van wet- en regelgeving. Per driver zijn meerdere mogelijke onderzoeksvragen geformuleerd die de IT-auditor kan onderzoeken. Hierbij zal de IT-auditor uiteraard een normenkader gebruiken. Een veel gebruikt normenkader binnen het IT-domein is de ISO27000-serie. Hoewel nieuwe OT-processen en systemen steeds meer richting ISO27000-normering verschuiven, is de IEC62443 een specifieke aanvulling voor het OT-domein op deze norm. IEC62443 bevat een uitgebreide normenset die zich richt op de continuïteit en de digitale weerbaarheid van organisaties. Uiteraard zijn er nog diverse andere good practices die de IT-auditor kan gebruiken. Door een verbreding van het IT-auditvakgebied naar het OT-domein, kan de IT-auditor een belangrijke bijdrage leveren aan de digitale weerbaarheid van organisaties in de industriële sector. Deze ontwikkeling biedt de IT-auditor unieke kansen. Wellicht is de tijd dan ook gekomen om de naam van de IT-auditor te evolueren naar IT/OT-auditor of cybersecurity-auditor.

Noot

[1] De Wbni noemt voor de verschillende sectoren de volgende bevoegde autoriteiten: Energie, digitale infrastructuur: de minister van EZK. Bankwezen, infrastructuur voor de financiële markt: De Nederlandsche Bank. Vervoer, levering en distributie van drinkwater: de minister van I&W. Gezondheidszorg: de minister voor Medische Zorg.

Literatuur

[ALBE19] Albeda, J, I*ndustrie 4.0, de risico's en aanbevelingen*, 29-04-2019, https://www.deitauditor.nl/business-en-it/industrie-4-0-de-risicos-en-aanbevelingen/ geraadpleegd op 10 april 2020.

[AUTO19] Automatie | PMA, *Eerste SOC voor permanent monitoren OT-installaties op cyberincidenten*, 08-07-2019, https://automatie-pma.com/artikelen/eerste-soc-voor-permanent-monitoren-ot-installaties-op-cyberincidenten geraadpleegd op 10 april 2020.

[CISA20] Cybersecurity and Infrastructure Security Agency (CISA), Alert (AA20-049A): *Ransomware Impacting Pipeline Operations*, 18-02-2020, https://www.us-cert.gov/ncas/alerts/aa20-049a geraadpleegd op 10 april 2020.

[ENIS18] European Union Agency for Cybersecurity (ENISA), *Good Practices for Security of Internet of Things: in the context of Smart Manufacturing*, 19-11-2018, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot geraadpleegd op 10 april 2020.

[MODD19] Modderkolk, H en Zetter, K, *STUXNET: AIVD speelde cruciale rol bij sabotage kernprogramma Iran*, 02-09-2019, https://www.volkskrant.nl/nieuws-achtergrond/aivd-speelde-cruciale-rol-bij-sabotage-kernprogramma-iran~ba24df9f/?referer=https%3A%2F%2Fwww.google.com%2F geraadpleegd op 10 april 2020.

[NCSC19] Nationaal Cyber Security Centrum (NCSC), *Cybersecuritybeeld Nederland 2019*, 12-06-2019, https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019 geraadpleegd op 10 april 2020.

[NCSC15] Nationaal Cyber Security Centrum (NCSC), *Checklist beveiliging van ICS/SCADA*, 22-12-2015, https://www.ncsc.nl/documenten/publicaties/2019/mei/01/checklist-beveiliging-ics-scada geraadpleegd op 10 april 2020.

[ROCC18] Roccia, T, *TRITON: The Next Generation of ICS Malware*, 08-10-2018, https://www.slideshare.net/ThomasRoccia/triton-the-next-generation-of-ics-malware geraadpleegd op 10 april 2020.

[VREE19] Vreeburg, T, *De nieuwe EU Cybersecurity Act*, 08-09-2019, https://www.deitauditor.nl/business-en-it/norea-stuurt-mee/ geraadpleegd op 10 april 2020.

[WIJSM16] Wijsman, Th, *Stuxnet: de thriller*, 14-03-2016, https://www.deitauditor.nl/business-en-it/stuxnet-de-thriller/ geraadpleegd op 10 april 2020.

C.F. (Stan) van Bommel RE | specialistisch inspecteur Agentschap Telecom

Stan van Bommel vervult vanuit de Wet beveiliging netwerk- en informatiesystemen (Wbni) een toezichtsrol op de energiesector en organisaties die de digitale infrastructuur verzorgen. Hij heeft meerdere jaren ervaring als IT-auditor en Security Officer.