Auditor, kijk ook naar de industriële systemen!

Innovatie in de audit: controle van en met de IT

Ir. Ronald Heil MSc CISSP CISA, Jip Hogenboom MSc CISSP, Martijn Sprengers MSc en Dennis Waalewijn MSc

Industriële bedrijven, en dus ook hun auditors, zijn tegenwoordig steeds meer of zelfs volledig afhankelijk van informatie afkomstig van digitale meters uit aangesloten IT-systemen. De beveiliging van deze systemen moet op orde zijn om de bedrijfscontinuïteit te kunnen waarborgen en om een juiste financiële jaarweergave te kunnen opstellen voor klanten met hun corebusiness in de procesindustrie. In de praktijk is er binnen industriële bedrijven echter weinig tot geen aandacht voor IT-beveiliging. Wat betekent dit voor de auditor?

R. Heil MSc CISSP CISA
is senior manager bij KPMG Advisory N.V.
heil.ronald@kpmg.nl

J. Hogenboom MSc CISSP
is senior consultant bij KPMG Advisory N.V.
hogenboom.jip@kpmg.nl

M.J. Sprengers MSc
is senior consultant bij KPMG Advisory N.V.
sprengers.martijn@kpmg.nl

D. Waalewijn MSc
is consultant bij KPMG Advisory N.V.
waalewijn.dennis@kpmg.nl

Inleiding

De jarenlange stabiele procestechnologie in industriële omgevingen is met een sneltreinvaart ingehaald door alle ontwikkelingen op het gebied van IT-technologie en daardoor is een raakvlak ontstaan tussen de industriële systemen en de kantooromgeving. Waar vroeger de productiedata van met smeer en roest besmeurde analoge tellers werden afgelezen en daarna op papier werden verstuurd, is de industrie nu afhankelijk van digitale meters, geautomatiseerde processen en een explosie aan informatie. Tegenwoordig zijn industriële bedrijven, en dus ook hun accountants, steeds meer (of zelfs al volledig) afhankelijk van informatie afkomstig van digitale meters uit aangesloten IT-systemen. Deze informatie, zoals de kwantiteit en kwaliteit van de producten, het productieresultaat of de uitstoot (van CO_2, NO_2, etc.), wordt tegenwoordig steeds vaker gebruikt om de bedrijfsvoering realtime aan te passen en/of te sturen.

De systemen die de productieprocessen aansturen en monitoren, worden ook wel Industrial Control Systems (ICS) genoemd. Dit zijn bijvoorbeeld de systemen die meten hoeveel olie door een pijpleiding loopt, een pomp automatisch aanzetten als de druk te hoog wordt of meetresultaten van verschillende sensoren combineren en deze data naar een ERP-systeem versturen zodat de nieuwe productieprocessen of benodigd onderhoud efficiënt gepland kunnen worden. Als de output van ICS-systemen incorrect is, worden er waarschijnlijk verkeerde prognoses gedaan voor de inkoop van grondstoffen, ontstaan er veiligheidsrisico's (de tank was toch leeg?) of worden aan de kant van verkoop onjuiste facturen verstuurd omdat het verbruik van grondstoffen en de levering van het eindproduct wezenlijk anders zijn dan het ERP-systeem laat zien. En het ERP-systeem is leidend, toch? Uiteindelijk zullen dan ook de jaarcijfers niet kloppen ten opzichte van de daadwerkelijke levering of productie, wat een aanzienlijk auditrisico met zich mee kan brengen bij nader onderzoek door overheid of milieu-inspectie of bijvoorbeeld bij ontdekking door de klanten zelf. Hierdoor kan ook de belastingbetaling aan de overheid incorrect zijn.

Ervan uitgaande dat de ICS-systemen correct zijn ingericht, dan is er toch geen auditrisico? Helaas, een van de meest actuele oorzaken van dit risico is een slecht ingerichte logische beveiliging (IT-systemen, netwerken, wachtwoorden, etc.) van de industriële omgeving. Een bijkomend effect van een slechte beveiliging van deze omgeving is dat de bedrijfscontinuïteit niet gewaarborgd

wordt, gegevens door hackers via het internet kunnen worden aangepast en zogenaamde safetysystemen (kritische beveiligingssystemen) niet meer naar behoren functioneren (bijvoorbeeld als de druk in een pijpleiding te hoog oploopt), wat erg gevaarlijke situaties kan opleveren voor het personeel en de omgeving, met kans op grote branden, explosies, milieuvervuiling en verlies van levens. Wat bedrijfsleiders in de industrie zich vaak niet realiseren is dat de bovengenoemde voorbeelden van audit- en bedrijfsrisico's zich zelfs al in de vroege aanbesteding en constructie van nieuwe fabrieken kunnen manifesteren, zoals in de supply chain van (deel)componenten die worden gebruikt in de industriële omgeving. Het is van belang dat de beveiliging van deze systemen (en de supply chain) op orde is voor de bedrijfscontinuïteit en voor het kunnen opstellen van een juiste financiële jaarweergave van klanten met hun corebusiness in de procesindustrie.

Wat is ICS/SCADA?

Een Industrial Control System is een complex systeem van allerlei soorten computers, actuatoren, sensoren, verbindingen en protocollen, met als doel de (industriële) processen dag en nacht op een gecontroleerde wijze draaiende te houden. Een eenvoudig voorbeeld van een kleinschalig ICS-systeem is een zwembad waar verschillende componenten (zoals temperatuur- en druksensoren en pompen) gebruikt worden om de waterstromen op gang te houden, de temperatuur zo aangenaam mogelijk te houden maar ook het zwembad veilig te houden. Via een centraal dashboard kunnen dan bijvoorbeeld de huidige temperatuur van het water, het chloorgehalte en het waterniveau bewaakt worden. Op basis van de meetresultaten van de sensoren kunnen vervolgens handmatige of geautomatiseerde acties ondernomen worden, zoals het verhogen van de temperatuur, het toevoegen of verminderen van chloor en het aanzetten van een pomp.

Hetzelfde principe wordt gebruikt in een fabriek, maar dan op een veel grotere schaal met grotere consequenties bij falen. Binnen een industriële omgeving worden alle processen met behulp van Supervisory Control And Data Acquisition (SCADA)-systemen zo veel mogelijk geautomatiseerd bewaakt en aangestuurd op basis van gegevens die door de (soms wel miljoenen) sensoren worden waargenomen en gerapporteerd. In plaats van één dashboard zijn er vaak tientallen monitoren waarop operators dag en nacht de huidige status centraal kunnen bijhouden en vanzelfsprekend kunnen ingrijpen in het geval van een afwijking of calamiteit.

Een productieketen binnen een industrieel proces kan uit de volgende componenten bestaan:

- sensoren die bijvoorbeeld temperatuur, druk en luchtkwaliteit meten;
- controllers die fysieke componenten aansturen op basis van de output van sensoren of handmatige acties (bijvoorbeeld het openen van kleppen);
- centrale systemen waarvandaan de controllers kunnen worden aangestuurd;
- databases waarin de productie- en meetgegevens worden opgeslagen;
- Process Information (PI)-server die de bovengenoemde productie- en meetgegevens beschikbaar maakt voor financiële en operationele managementrapportages. Het is feitelijk de enige plek waar achteraf (in detail) te zien valt wat er heeft plaatsgevonden.

Binnen industriële omgevingen wordt van oudsher veel aandacht besteed aan HSE: Health (gezondheid), Safety (veiligheid) en Environment (omgeving). De processen en componenten zijn dan ook vaak zo geconfigureerd en geïmplementeerd dat de risico's voor de gezondheid, veiligheid en omgeving zo veel mogelijk zijn gereduceerd. Hiertoe zijn bij grotere fabrieken vaak geautomatiseerde veiligheidssystemen geïmplementeerd die in het geval van een noodsituatie zorgen voor een gecontroleerde 'shutdown' van alle processen zodat bijvoorbeeld het risico op een ontploffing in het geval van een hoge druk of chemische verbindingen in een leiding of vat gemitigeerd wordt. Interessant daarbij is dat de mens bijna nooit de mogelijkheid heeft om in deze processen in te grijpen: zodra de computer vindt dat de situatie onveilig is (of wordt), grijpt deze direct in.

Hoe werkt een ICS/SCADA-component aan de binnenkant? Verrassend genoeg zijn de ICS/SCADA-leveranciers de afgelopen jaren (en met een sneltreinvaart) steeds meer reguliere IT-componenten gaan gebruiken in hun producten en diensten. Een ICS/SCADA-component is dus eigenlijk niet anders dan een laptop of televisie, maar dan betrouwbaarder (althans, dat zou zo moeten zijn) en dus ook veel duurder (soms zelfs een factor 100).

Echter, doordat er steeds meer IT wordt geïntroduceerd in deze industriële omgevingen, ontstaat er ook een nieuw risico: informatiebeveiliging (Security). Binnen verschillende bedrijven met een industriële omgeving is sinds enkele jaren de S van Security aan het rijtje HSE toegevoegd, om daarmee te komen tot HSSE. Dit is niet voor niks, want security heeft een directe impact op de gezondheid, de veiligheid en de omgeving!

Hoewel noodprocedures en veiligheids-protocollen (HSE) in industriële omgevingen vaak van zeer hoog niveau zijn, is er weinig tot geen aandacht voor IT-beveiliging

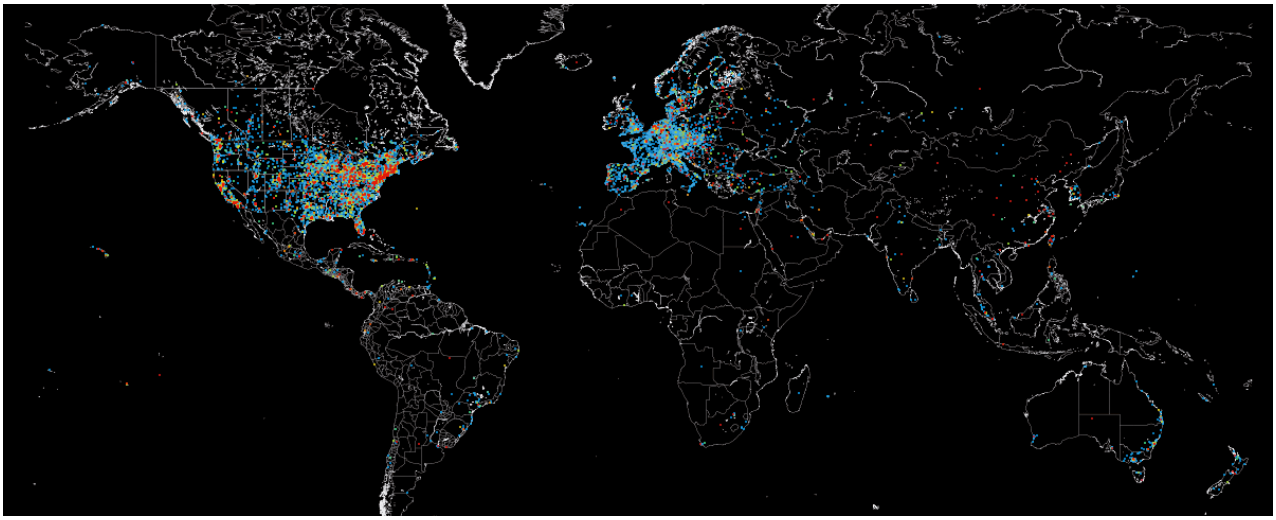
Wij zien hier een opvallende tegenstelling. Hoewel noodprocedures en veiligheidsprotocollen (HSE) in industriële omgevingen vaak van zeer hoog niveau zijn, is er weinig tot zeg maar gerust geen aandacht voor IT-beveiliging (Security) en bijbehorende processen die in het normale bedrijfsleven heel gewoon zijn (zoals access management, patch management, etc.). Boorplatformen beschikken bijvoorbeeld over Fire and Gas (FIS/GAS)- of Emergency Shutdown (ESD)-systemen die automatisch het proces en de onderliggende infrastructuur stilleggen als er vuur, gas of een te hoge druk gedetecteerd wordt. Kijk je in dezelfde omgeving naar de IT-beveiliging, dan is er sprake van een heel andere, bijna onvoorstelbare, onveilige situatie. Sommige systemen zijn zelfs zonder nadenken gekoppeld aan het internet, waardoor bijna iedereen ze op afstand kan manipuleren. Het is opvallend dat in een omgeving waarin veiligheid boven aan de agenda staat, de IT-beveiliging vaak achterblijft. De paradox hier is dat juist die zwakheden in de IT-omgeving eenvoudig misbruikt kunnen worden om de processen te verstoren en aan te passen en zelfs de safetysystemen buiten werking te zetten. De veiligheid (safety) wordt dus juist ondermijnd door een gebrek aan security.

Hoe kunnen deze risico's zich materialiseren?

Zoals eerder beschreven kunnen productiegegevens worden gewijzigd door middel van manipulatie van gegevens binnen het proces zelf, tijdens het verzamelen en transporteren van gegevens, direct in de centrale database of direct op de PI-server. Als we dit combineren met onze eerdere opmerking dat de IT-beveiliging van al deze onderdelen over het algemeen niet op het juiste niveau is (lees slecht), dan is het vrij eenvoudig om in te zien dat uiteindelijk de meet- en productiegegevens eenvoudig incorrect kunnen worden geïnterpreteerd, simpel omdat ze gewoon niet meer kloppen. Aangezien deze gegevens de basis zijn voor de jaarrekeningcontrole bij industriële klanten (immers, alle bedrijfsprocessen rondom de fabriek zijn afhankelijk van deze gegevens en resulteren uiteindelijk in een financieel getal), is de integriteit hiervan uiterst essentieel.

Op basis van onze ervaringen met het uitvoeren van security reviews van industriële omgevingen zien wij de volgende veelvoorkomende zwakheden:

- *Het gebruik van onveilige (of verouderde) software zoals Windows XP.* Het komt vaak voor dat nieuwe software- of besturingssystemen niet werken met de software van de



Figuur 1. **Voorbeeld van ShodanHQ inzake op internet aangesloten onbeveiligde industriële systemen.**

ICS/SCADA-leverancier (of de leverancier claimt dat het niet werkt). Daarnaast is het bijna onmogelijk de systemen te herstarten om een nieuwe patch te installeren zonder dat dit impact heeft op de productieprocessen. Het komt dus nog regelmatig voor dat een splinternieuwe fabriek in 2015 opgeleverd wordt met Windows XP als besturingssysteem op de ICS-componenten, terwijl Windows XP al jaren niet meer ondersteund wordt door Microsoft. De omgeving is dus eigenlijk al lek (vanuit beveiligingsoogpunt) voordat deze formeel wordt overgedragen aan de klant.

- *Het gebruik van zwakke wachtwoorden voor accounts met vergaande rechten.* Door onvoldoende 'security awareness' worden er vaak zwakke wachtwoorden geconfigureerd omdat deze gemakkelijker te onthouden zijn.
- *Onveilig geconfigureerde systemen die resulteren in kwetsbaarheden.* De systemen worden vaak eenmalig geconfigureerd bij de oplevering van de omgeving. Aangezien de focus ligt op de beschikbaarheid en functionaliteit, worden beveiligingsrisico's vaak niet opgelost.
- *Onveilige segregatie van het netwerk, remote toegang en inadequate controle op derde partijen.* Om eventuele problemen op afstand te kunnen oplossen worden er vaak verbindingen aangelegd met leveranciers. Het probleem is dat er in de afspraken tussen de afnemer en de leveranciers vaak geen eisen aan de beveiliging worden opgenomen. Eenzelfde situatie doet zich voor bij onderaannemers die bijvoorbeeld pure zuurstof leveren aan de fabriek. Bij grote fabrieken staat zo'n onderaannemer zelf ook met een minifabriekje op het terrein. Tussen de systemen van beide zit heel vaak een verbinding zodat de processen optimaal op elkaar zijn afgestemd, maar helaas is 99 van de 100 keer deze verbinding onbeveiligd.

Waar de meeste geautomatiseerde aanvallen in het ICS-domein (die in het nieuws komen) gericht zijn op het uitvoeren van een zogenaamde Denial of Service (DoS)-aanval, oftewel het tijdelijk maar vaak ook permanent verstoren van de productie (denk aan Stuxnet, zie [Lang11]), is het belangrijk te weten dat de verkregen toegang ook gemakkelijk misbruikt had kunnen worden om meet- en productiegegevens direct te manipuleren.

Nu kan een organisatie zich afvragen waarom zij het doel zou zijn van een aanvaller. Dat een organisatie denkt dat zij niet 'belangrijk' genoeg is om te worden aangevallen is echter niet relevant – dit is volledig aan de aanvaller om te bepalen. Helaas geldt (in tegenstelling tot het bedrijfsleven) dat bijna alle industriële omgevingen wel interessant zijn voor iemand, om uiteenlopende redenen, zoals spionage, concurrentie, diefstal van intellectueel eigendom, milieuactivisme of hobbyisme.

Belangrijkste risico's

1. *Gebrek aan inzicht in risico's.* Omdat er te weinig kennis of bewustzijn is op dit vlak, weet men niet wat de risico's zijn of focust men op de verkeerde risico's.
2. *Remote shutdown.* Iemand kan op afstand de productieomgeving beïnvloeden en uitzetten.
3. *Ongeautoriseerde toegang tot Programmable Logic Controller (PLC).* Een PLC kun je beschouwen als een computer die het proces, de pompen en motoren, aanstuurt. De per proces verschillende aansturing heet 'ladder logic'. Het gaat om het veiligheidstrappensysteem waarbij bijvoorbeeld de installatie automatisch wordt teruggeschakeld als de druk te hoog wordt. Als criminelen die protocollen kunnen beïnvloeden, ontstaat een heel gevaarlijke situatie. Dit was bijvoorbeeld het geval bij Stuxnet, waarbij een centrifuge doelbewust werd oververhit.
4. *Dreigingen vanuit een derde partij.* Op productielocaties is het vaak een komen en gaan van allerlei externen (leveranciers, engineers, monteurs). Zij loggen met allerlei apparaten in en vormen zo een beveiligingsrisico.
5. *Auditrisico.* IT en de daaruit voortvloeiende beveiligingsrisico's zijn onoverkomelijk vervlochten geraakt met productieprocessen in fabrieken waardoor incorrecte jaarcijfers kunnen ontstaan.

Ketenbeveiliging begint bij de supply chain

De beveiliging van ICS begint niet wanneer de fabriek reeds in operatie is maar al veel eerder: bij de aanbesteding en implementatie van een nieuwe fabriek. Aangezien de industriële systeemcomponenten in een industriële omgeving een veelvoorkomend doel zijn voor cyberaanvallen, is het niet ondenkbaar dat deze componenten al voordat de fabriek is gebouwd en opgestart, worden gemanipuleerd. Met andere woorden, een aanvaller zou kunnen interfereren met de supply chain van deze componenten om zo mogelijk later schade aan het bedrijf te veroorzaken of financieel gewin te behalen (bijvoorbeeld door afpersing). Omdat deze dreigingen veelal plaatsvinden voordat een fabriek operationeel is, wordt dit vaak niet (direct) opgemerkt.

Een voorbeeld van een dreiging in de supply chain is dat een Programmable Logic Controller (PLC) in een opslagruimte (warehouse) wordt aangetast met malware met de functie om gemanipuleerde data te versturen. Je kunt je voorstellen dat het lastig (en soms bijna onmogelijk) is om

later vast te stellen dat dit het geval is, want de operators en het productieproces zien immers alleen deze data (waarvan ze denken dat die correct zijn). Zo kan een aanvaller bijvoorbeeld zeer effectief het productieproces inefficiënt laten verlopen.

Een ander voorbeeld van een dreiging betreft de situatie waarin wordt gewerkt met meerdere leveranciers, iets wat veel voorkomt in grote fabrieken. Een resultaat hiervan is dat op productielocaties talrijke externen (leveranciers, engineers, monteurs) komen met hun eigen apparatuur en computers (laptops) die zij op meerdere locaties van verschillende organisaties gebruiken. Zij bezoeken bijvoorbeeld een geïnfecteerde fabriek en gebruiken vervolgens de geïnfecteerde apparatuur in een andere fabriek. De malware die bestaat voor industriële omgevingen is al een tijdje slim genoeg om te 'springen' van de ene locatie naar de andere en tegelijkertijd onzichtbaar te blijven. Daarnaast gaan deze derde partijen veelal onvoorzichtig om met 'beheer op afstand', wat ook extra beveiligingsrisico's met zich meebrengt.

Uit deze voorbeelden komt naar voren dat vanuit het oogpunt van de supply chain en derde partijen het dus ook van vitaal belang is om voldoende mitigerende maatregelen te treffen om de integriteit (en continuïteit) te waarborgen.

Bepaal wat het geïdentificeerde risico betekent voor je audit

IT en de daaruit voortvloeiende beveiligingsrisico's zijn onoverkomelijk vervlochten geraakt met de productieprocessen in industriële omgevingen. Wanneer deze risico's niet voldoende gemitigeerd worden, kunnen incorrecte jaarcijfers ontstaan en moet de accountant zich afvragen of zijn verklaring over de jaarrekening wel juist is. Daarom vinden wij dat de auditor ook de industriële systemen zou moeten beoordelen!

Het is belangrijk onderscheid te maken tussen het uiteindelijke bedrijfsrisico en het zogenaamde auditrisico: dat een kwaadwillende gemakkelijk de cijfers in het productiesysteem kan aanpassen (de zogenaamde 'can do'), wil nog niet zeggen dat dit ook daadwerkelijk gebeurd is (de zogenaamde 'did do'). Het is dus van belang te bepalen of aanvullende werkzaamheden, zoals gegevensgerichte (substantive) controles, nodig zijn door te bepalen hoe waarschijnlijk een risico eigenlijk is. Denk daarbij echter wel aan de bronnen van de gegevensgerichte controles, want die kunnen we niet zomaar vertrouwen.

Aan de andere kant, als auditors IT-beveiliging van industriële controlesystemen moeten meenemen in hun

Oplossingen

1. *Zorg dat je grip krijgt op de toegangscontrole van het netwerk en procescontrolesystemen.* Vanuit de gedachte dat toch niemand bij het op zichzelf staande systeem kan komen, zijn de wachtwoorden vaak zwak. Meestal worden eenvoudige wachtwoorden als 'engineer' of 'operator' gebruikt. Indringers die de bedrijfsomgeving binnen zijn gekomen, kunnen zo gemakkelijk doorstappen naar de procescontroleomgeving.
2. *Focus op detectieve maatregelen in plaats van een preventieve aanpak.* Er moeten analyses in de beveiliging worden ingebouwd waarbij risico's of fraude actief kunnen worden opgespoord. Met alleen het patchen van softwareversies of veranderen van wachtwoorden ben je er niet, met name omdat de software vaak vrij oud is en de komende 20 jaar niet gaat veranderen (immers, een fabriek wordt opgestart met het plan deze 20 à 30 jaar te laten draaien).
3. *Zorg voor het juiste beleid.* De verantwoordelijkheid voor de IT-beveiliging moet bij de juiste persoon liggen. Vaak is er lokaal iemand verantwoordelijk voor de beveiliging, bijvoorbeeld de hoofd-engineer of facility-manager. Hebben personen in deze functie wel de juiste kennis en middelen? Wat helpt is een stuurgroep van zowel mensen die het proces snappen als degenen die over beveiligingsrisico's gaan (bijvoorbeeld de CISO). Daarnaast moet de raad van bestuur ook eigenaarschap nemen, want uiteindelijk draait het om hun bedrijf en personeel.
4. *Probeer de wereld van engineers te begrijpen.* Zij werken in een andere wereld dan jij als IT-professional gewend bent. In industriële omgevingen gaat het om het 24 uur per dag draaiend houden van een productiesysteem. De veiligheid van die installatie staat voorop. Daarbij zijn engineers zich vaak niet bewust van de risico's op IT-gebied. Daar is sturing nodig. Wat vooral werkt is 'echte' risico's te onderkennen. Dus niet 'de virusscanner is niet geïnstalleerd', maar 'door deze combinatie van instellingen is het mogelijk de ladder logic vanaf het internet aan te passen'.

IT en de daaruit voortvloeiende beveiligingsrisico's zijn onoverkomelijk vervlochten geraakt met de productie-processen in industriële omgevingen

aanpak, dan zullen organisaties hier ook voldoende maatregelen moeten treffen. Het is uiteindelijk deze wisselwerking waarvoor de discussie binnen de beroepsgroep op gang gebracht dient te worden!

Literatuur

[Lang11] R. Langner, *Stuxnet: Dissecting a Cyberwarfare Weapon*, IEEE Security & Privacy, June 2011, pp. 49-51.

Over de auteurs

Ir. R. Heil MSc CISSP CISA is senior manager bij KPMG Advisory N.V. Hij is gespecialiseerd in IT-auditing en adviesdiensten op het gebied van informatiebeveiliging (processen en diepgaande techniek), cyber defense / cyber resilience, specifiek Threat Management (tactisch en operationeel), Vulnerability Management en beveiliging van complexe industriële omgevingen (ICS).

J. Hogenboom MSc CISSP is senior consultant bij KPMG Advisory N.V. Hij is gespecialiseerd in (grootschalige) interne en externe penetratietesten, de beveiliging van Industrial Control Systems (ICS), technische security reviews, security design, cyber defense en ICS/IT-audits. Veel van deze opdrachten zijn uitgevoerd op grootschalige en complexe omgevingen in binnen- en buitenland.

M.J. Sprengers MSc is werkzaam bij KPMG Advisory N.V. als IT-beveiligingsadviseur en verricht operationele werkzaamheden voor (technische) IT-beveiligingsopdrachten. Hij heeft ruime ervaring met IT- en ICS-beveiligingsvraagstukken en is gespecialiseerd in meerdere facetten: ethical hacking, social engineering, de beveiliging van Industrial Control Systems (ICS), SAP-systemen en het uitvoeren van penetratietesten op (web)applicaties, (technische) IT-audits en security framework reviews.

D. Waalewijn MSc is werkzaam als consultant bij KPMG Advisory N.V. Hij is gespecialiseerd in de beveiliging van industriële omgevingen en in ethical hacking.