Nationale Cyber Security Monitor 2020

Procesindustrie en Chemie/Life Sciences

THALES

Pb 7

Analyse door Peter Vermeulen
Chief Analyst Pb7 Research

Sponsor*: Thales*

Inhoud

Hoofdsponsors

SOPHOS

THALES

Initiatiefnemers

INFO SECURITY MAGAZINE

AUTOMATIE PMA

Pb 7

Analyse

Het gebruik van technologie neemt sterk toe in de sectoren procesindustrie, chemie en life sciences. De groei komt niet zozeer vanuit de kantooromgeving, maar vooral vanuit de productiezijde. Het gebruik van OT is allerminst nieuw. Maar de laatste jaren wordt OT steeds meer gekoppeld aan kantoorsystemen. Met de toenemende kansen van bijvoorbeeld kunstmatige intelligentie en machine learning, neemt de behoefte toe om data te koppelen en in verschillende IT-systemen te verwerken sterk toe. Met de groeiende connectiviteit, nemen ook de risico's voor cybersecurity toe. Aangezien de sector op IT-security eerder volger is dan leider, is er een groeiende noodzaak om op cybersecuritygebied een paar stevige stappen te zetten.

IT-security

Op IT-security-vlak zien we een aantal bemoedigende ontwikkelingen. Het aantal IT-security incidenten met schade lijkt eerder te zijn gestabiliseerd dan gegroeid. Op zich zeggen bedrijven dat ze met meer incidenten te maken hebben gehad, maar dat het minder vaak tot schade leidt. Er zijn ook incidenten waar minder bedrijven mee te maken hebben gehad, zoals DDOS-aanvallen, computerinbraak en ook ransomware.

Wat ook goed gaat, is dat we voor het eerst zien is medewerkersbewustzijn en identity & access management nu ook een hoge prioriteit krijgen naast netwerkbeveiliging en secure content & threat management. Bedrijven buiten de proces/chemie zijn daar wel al wat verder in, maar deze trend is ook binnen de sector duidelijk herkenbaar.

Ook bij het Internet of Things zien we duidelijk vooruitgang. Gelukkig, moeten we wellicht zeggen, omdat er bij veel bedrijven nog een lange weg te gaan is. We zien dat steeds meer bedrijven secure by design toepassen op IoT en dat ze zich steeds meer bewust worden dat ze leveranciers daar ook op moeten beoordelen.

Maar er valt op het vlak van cybersecurity ook nog meer dan genoeg te verbeteren. Dat er minder vaak incidenten met schade zijn, betekent niet dat de totale schade afneemt. Cybercriminelen zijn steeds gerichter bezig om individuele bedrijven binnen te dringen, vaak met een combinatie van verschillende technieken, om daar een grote buit te halen. We zien ook dat het aantal incidenten dat veroorzaakt wordt door onoplettende medewerkers duidelijk toeneemt, waardoor die extra aandacht voor medewerkersbewustzijn duidelijk gerechtvaardigd wordt.

OT-security

Op het gebied van OT-security, de bescherming van productiesystemen, valt nog een wereld te winnen. De risico's nemen hier snel toe, doordat veel productiesystemen aan het kantoornetwerk zijn gekoppeld en/of aan het Internet. Ook de leveranciers van machines spelen daarbij een rol, aangezien zij hun machines steeds vaker online willen uitlezen en online onderhoud willen plegen. Het ontbreekt bij veel organisaties in de industrie aan een elementair bewustzijn van de risico's. Als gevolg daarvan ontbreekt het aan beleid, aan maatregelen en aan budget om maatregelen te verwezenlijken. Hoewel de aandacht voor cybersecurity risico's zeker groeit, is er nog een lange weg te gaan.

Als het om cybersecurity gaat, is stilzitten geen optie. De belangen en daarmee de risico's worden steeds groter, terwijl we als samenleving nog altijd niet in staat zijn om cybercriminelen effectief aan te pakken. Daarbij zouden organisaties minder in hokjes moeten denken: cybersecurity strekt zich uit tot ver buiten het traditionele IT-domein. Zeker voor bedrijven in de sectoren procesindustrie, chemie & life sciences waar OT een grote rol speelt, betekent het dat een holistische aanpak waarbij IT en OT in hun samenhang worden opgepakt, de topprioriteit moet gaan krijgen.

Achtergrond

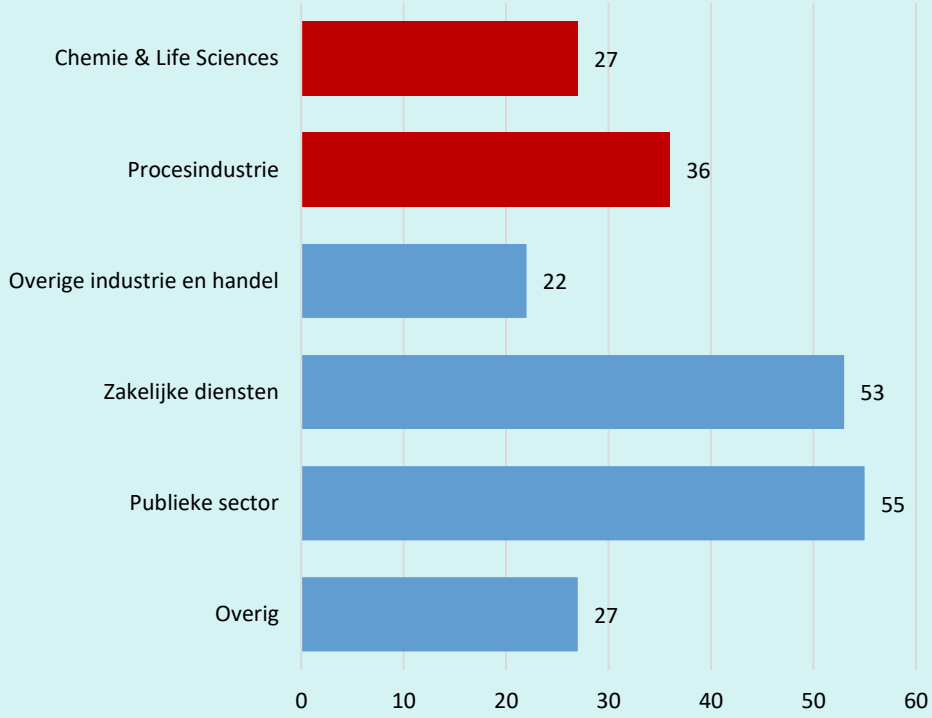
De Nationale Cybersecurity Monitor is de opvolger van de Nationale IT Security Monitor. Met deze monitor houdt Pb7 Research in samenwerking met Infosecurity Magazine en Automatie | PMA de vinger aan de pols van de Nederlandse cybersecuritymarkt. Waar de monitor zich in de voorgaande edities beperkte tot de IT-securitymarkt, met af en toe een klein IoT-uitstapje, kijken we dit jaar ook naar OT-security in de sectoren chemie & life sciences en de procesindustrie.

Wat niet is veranderd, is dat we onderzoeken wat de belangrijkste trends en investeringen zijn in de zakelijke markt bij bedrijven met 50 of meer medewerkers. Het onderzoek is dit jaar mede mogelijk gemaakt dankzij de steun van hoofdsponsor Thales, die ook het onderzoek naar Chemie & Life Sciences en de Procesindustrie mogelijk heeft gemaakt. In het onderzoek proberen we vraagpunten over een aantal jaar heen te herhalen zodat we goed inzicht krijgen in de ontwikkelingen. Maar we borduren ook voort op de laatste bevindingen en houden onze ogen open voor nieuwe thema's. Zo hebben we in deze editie ook weer goed gekeken naar de belangrijkste drijfveren achter security-investeringen en het veranderende dreigingsbeeld. Ook hebben we net als vorig jaar naar IoT gekeken en hebben verdere stappen gezet op het vlak van OT.

Het onderzoek is uitgevoerd door onafhankelijk ICT-onderzoeksbureau Pb7 Research. In oktober en november van 2019 zijn 220 bedrijven met 50 of meer medewerkers ondervraagd met behulp van een web panel survey.

Het document dat u nu leest, is een samenvatting van de belangrijkste resultaten en conclusies uit het onderzoek en vertegenwoordigt de visie en mening van Pb7 Research. De sponsoren van het onderzoek zijn het dus niet per definitie eens met de analyse en de conclusies.

Figuur 1: Steekproefverdeling Nederland (N=220)



Nationale IT Security Monitor 2020

In de afgelopen jaren hebben we gezien dat dreigingen steeds tastbaarder werden, terwijl de impact van incidenten steeds groter worden door de snel toenemende verwevenheid van de bedrijfsvoering met ICT. In een wereld van digitale transformatie, vervult security een cruciale rol. Het ontbreken van adequate security kan tot incidenten leiden die het voortbestaan van vrijwel iedere organisatie kunnen ondermijnen. Het beschikken over adequate beveiliging kan bedrijven daarom juist ook een belangrijk concurrentievoordeel bieden.

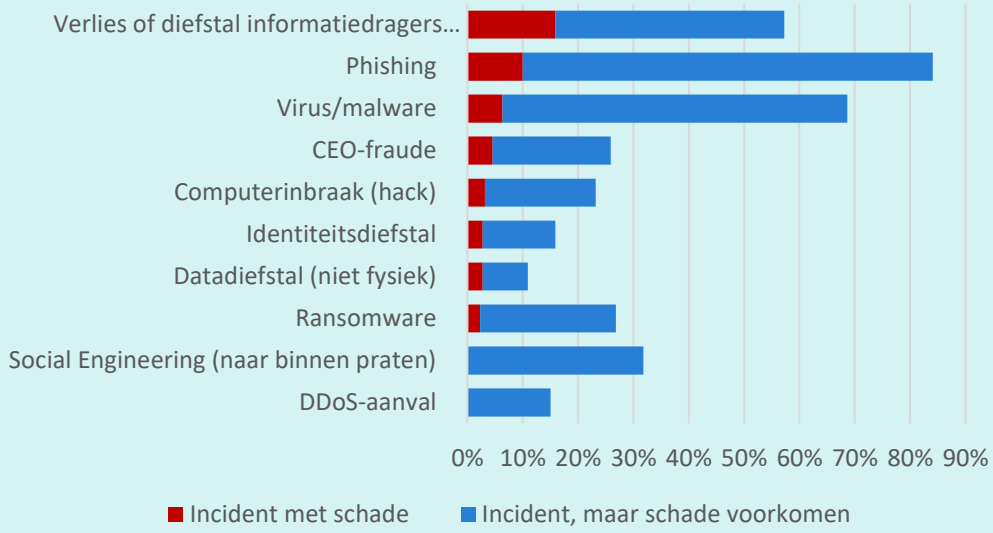
Bij veel organisaties is security ook onder de aandacht gekomen door wet- en regelgeving zoals de AVG. Opvallend genoeg blijft dat de gemoederen danig bezighouden. Eind september stuurde het CIO-platform een brandbrief aan de Autoriteit Persoonsgegevens omdat het ondoenlijk blijkt voor afnemers om ieder voor zich alle softwareleveranciers lang de AVG-meetlat te leggen. Begrijpelijk, maar het getuigt niet van een sterk vooruitziende blik. Wet- en regelgeving blijven echter altijd een belangrijke factor binnen security en zullen dat ook steeds meer in de OT-wereld gaan zijn.

Dreigingsbeeld

Wat incidenten betreft, zien we geen significante verschillen tussen bedrijven in de procesindustrie en chemie en in andere sectoren. Als we kijken naar het type IT-veiligheidsincidenten dat plaatsvindt binnen Nederlandse organisaties, zien we dat het afgelopen jaar vooral het aantal incidenten toeneemt dat specifiek gericht is op de gebruiker. CEO-fraude lijkt, tegen deze trend in, wat op zijn retour. Er zijn verder wat meer incidenten met het verlies van informatiedragers, zoals laptops of opslagmedia. We zien vooral een toename van het aantal bedrijven dat phishing meldt, hoewel het aantal bedrijven dat ook daadwerkelijk schade daardoor heeft geleden, nauwelijks is gegroeid. Ook het aantal incidenten met social engineering is toegenomen, hoewel onze respondenten daar geen schade weten te melden. Deze trend geldt voor al deze incidenten: ze komen vaker voor, maar Nederlandse organisaties weten te voorkomen dat dit ook vaker tot schade leidt.

Figuur 2: Incidenten

Met welke van de volgende incidenten heeft uw organisatie de afgelopen 12 maanden te maken gehad?



Tegenover de groei van bovenstaande type incidenten, zien we dat er ook incidenten zijn die minder vaak voorkomen. De sterkste terugloop zien we bij DDOS-aanvallen, computerinbraak (hacking) en, wellicht verrassend, bij ransomware. Ransomware richt zich steeds vaker op individuele, grote organisaties. Het aantal getroffen bedrijven neemt daardoor af, terwijl de totaalschade in euro's juist toeneemt.

Investeringen

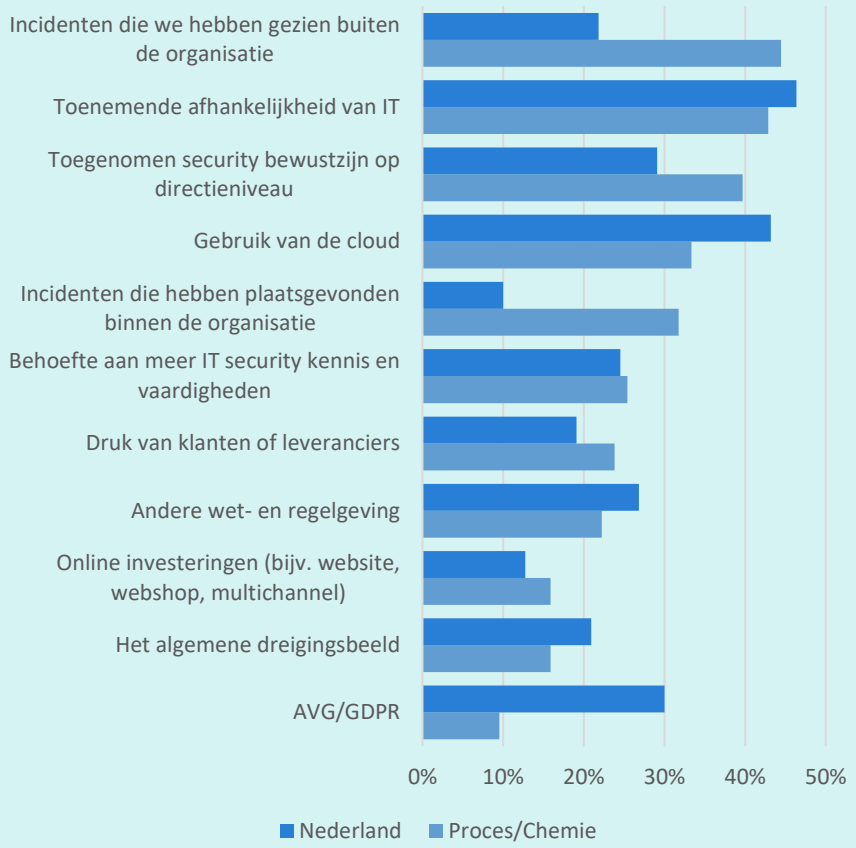
De uitgaven aan IT-security blijven sterk stijgen om het toenemende aantal pogingen en de toenemende complexiteit het hoofd te bieden. Volgens de ondervraagde bedrijven in proces/chemie stegen de uitgaven aan IT-security met 13% in 2019, duidelijk boven het marktgemiddelde van 11%. Voor 2020 verwacht men zelfs 14%.

In de proces/chemie sector zien we dat de belangrijkste drijfveer voor security investeringen relatief vaak te maken heeft met de weerslag van incidenten, vooral incidenten die men bij andere partijen heeft zien gebeuren. Het positieve daarin is dat er een goede blik naar buiten is. Maar het blijft een reactieve aanpak met alle risico's van dien. Gelukkig is de sector niet alleen reactief: ook het bewustzijn dat de bedrijfsvoering beschermd dient te worden tegen aanvallen is zich sterk aan het ontwikkelen, zei het nog niet zo sterk als in andere sectoren.

Dit jaar zien we eigenlijk voor het eerst een duidelijke verschuiving optreden in de prioriteiten die organisaties stellen bij het investeren in IT-security. In de afgelopen monitors werden netwerkbeveiliging en secure content & threat management als de belangrijkste prioriteiten

Figuur 3: Drijfveren voor security investeringen

Welke van de volgende ontwikkelingen hebben de grootste invloed op investeringen in IT-security voor de komende 12 maanden?

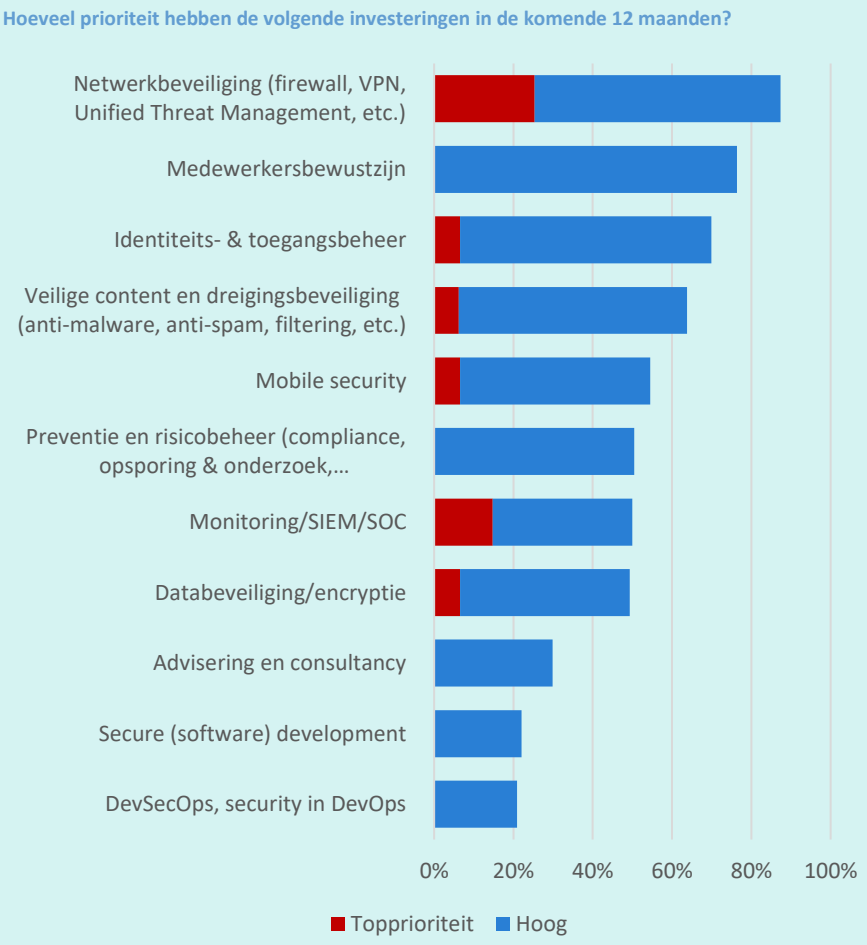


aangemerkt. Dit jaar wordt aan medewerkersbewustzijn het vaakst een hoge- of topprioriteit gegeven. Bedrijven in de proces/chemie sectoren lopen daar nog wel wat op achter. Bewustzijn staat weliswaar op 2, maar er wordt zelden topprioriteit aan gegeven. Het is belangrijk om te onderkennen dat een bewustzijnscursus niet een eenmalige gebeurtenis moet zijn. Niet alleen proberen cybercriminelen op steeds nieuwe manieren in te spelen op menselijke zwaktes, maar het bewustzijn is immers naarmate er tijd verstrijkt ook aan slijtage onderhevig.

Na medewerkersbewustzijn en netwerkbeveiliging heeft identiteits- en toegangsbeheer het vaakst een hoge of topprioriteit. Het idee van een digitale identiteit voor ieder gebruiker, met veelal rol-gebaseerde toegang tot informatie en systemen, zorgt ervoor dat niet alle poorten zomaar opengaan. Aan de andere kant kan het een solide oplossing vormen voor het wachtwoordenprobleem, zeker als het om 2-factor identificatie gaat. Een goede IAM-oplossing is gebruiksvriendelijker en voorkomt problemen met zwakke wachtwoorden.

Ieder jaar hameren we in de monitor op het belang van secure en privacy by design. Het belang van secure development lijkt sterk achter te blijven. Hoewel meer organisaties dan vorig jaar aangeven software te ontwikkelen op basis van secure by design en privacy by design, ligt er weer minder prioriteit bij het investeren in secure software development. Ook als we er rekening mee houden dat iets meer dan de helft van de ondervraagde bedrijven zelf software ontwikkelt of op maat laat ontwikkelen, valt dit, en ook in andere sectoren, tegen.

Figuur 4: Prioriteiten en investeringen



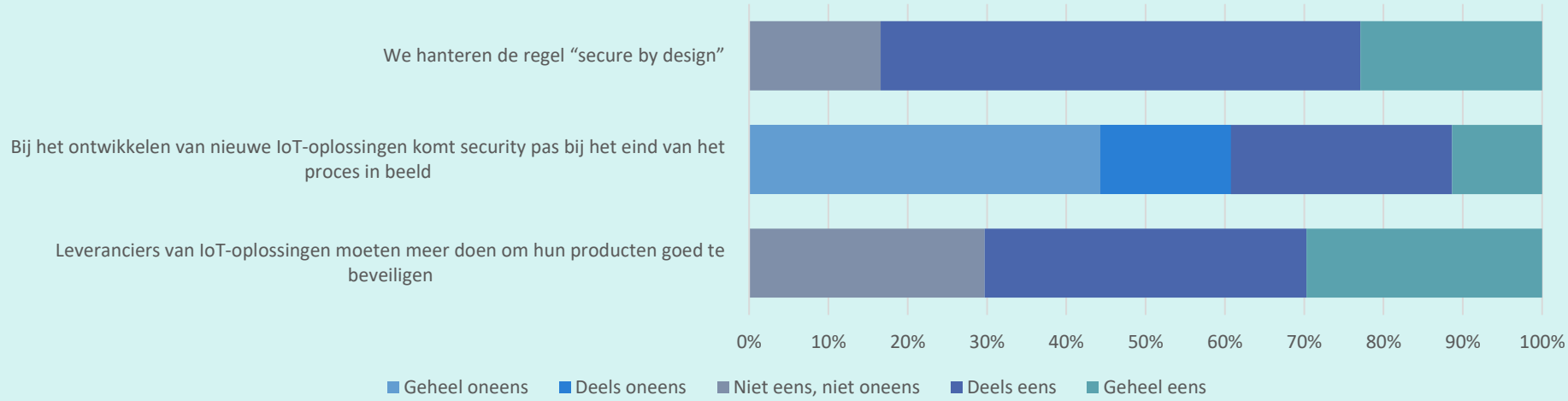
IoT Security

Bedrijven in de proces/chemie sectoren maken steeds breder gebruik van het Internet of Things (IoT). Toch staan we pas aan het begin, ondanks dat we al behoorlijk lang geleden zijn begonnen met het aan elkaar knopen van apparaten en dat inmiddels meer dan 85% van de respondenten in de proces/chemie sectoren zegt IoT-oplossingen in te zetten of te ontwikkelen. De toegenomen rekenkracht en de mogelijkheden die daardoor ontstaan om dingen autonoom slimme beslissingen te laten nemen dankzij kunstmatige intelligentie en machine learning, zorgen ervoor dat we een lange innovatiegolf verwachten. En dat brengt ook weer nieuwe bedreigingen met zich mee waar niet iedere organisatie even goed op is voorbereid.

Over de beveiliging van IoT bestaan veel zorgen, ook in de zakelijke markt. Het is lang niet altijd duidelijk hoe veilig het is om allerlei slimme apparaten maar aan het Internet of het bedrijfsnetwerk te hangen, zodat de leverancier bijvoorbeeld op afstand onderhoud kan plegen. Dat geldt zelfs voor een onderwerp als printers, waarmee hackers zich toegang tot uw bedrijfsnetwerk kunnen verschaffen. Gelukkig zien we dat het bewustzijn hieromtrent duidelijk is toegenomen.

Figuur 5: IoT en security

Q6B. Bent u het eerder eens of oneens met de volgende stellingen met betrekking tot IT-beveiliging rond IoT (Internet of Things) binnen uw organisatie?



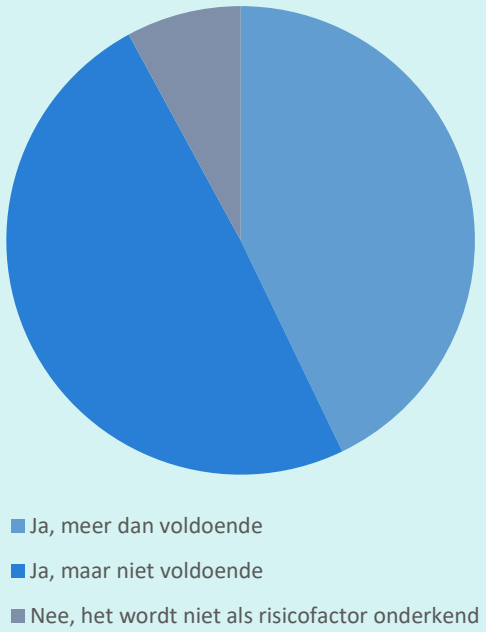
Onze respondenten maken zich alleen maar meer zorgen over de producten van IoT-productleveranciers, terwijl ze zelf vaker “secure by design” IoT ontwerpen. Dat geldt vooral voor bedrijven in de chemie/proces sectoren.

OT en Security

In de chemie/proces sectoren (procesindustrie, chemie en life sciences) wordt OT op grote schaal ingezet. Met OT hebben we het over hardware en software waarmee fysieke processen worden gecontroleerd en/of aangestuurd, zoals PLC’s en SCADA-systemen. Binnen veel organisaties is deze wereld qua organisatie grotendeels of volledig gescheiden van IT en dat geldt ook voor IT-security. Toch raken IT en OT elkaar steeds meer. In toenemende mate zijn OT-systemen verbonden aan dezelfde netwerken, zowel het Internet als bedrijfsnetwerken. Zo geeft meer dan de helft (56%) van de ondervraagde organisaties aan dat industriële controlesystemen met het kantoornetwerk zijn verbonden.

De respondenten geven aan dat er nog een behoorlijke slag te maken is, voordat OT-security zich op een professioneel niveau bevindt. 57% van de organisaties geeft aan dat cybersecurity in productieomgevingen onvoldoende of zelfs geheel niet wordt erkend als een risicofactor. En als we doorvragen naar de grootste uitdagingen op OT-securitygebied, dan geeft de helft (51%) aan dat het ontbreken van een goed zicht op de kwetsbaarheden een grote uitdaging is. Een bijna even grote groep (43%) zegt dat onvoldoende bewustzijn van de risico’s een groot probleem is.

Figuur 6: OT-security erkend als risico?

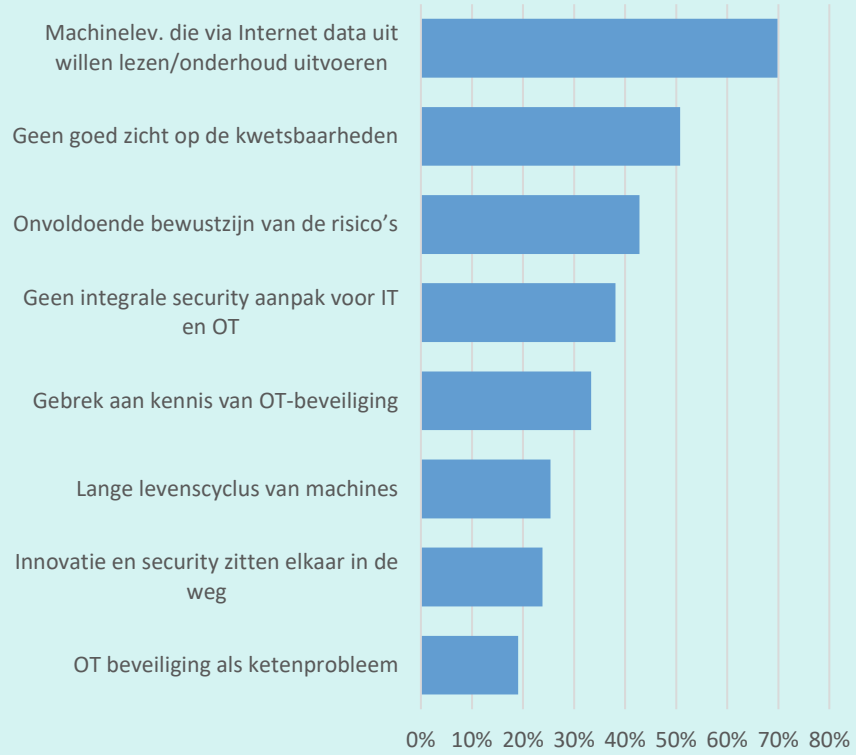


Maar aangezien elementaire kennis over OT-security vaak ontbreekt, is het niet vreemd dat de allergrootste uitdaging te maken heeft met machineleveranciers. Steeds meer machineleveranciers willen immers data uitlezen uit machines om de prestaties te monitoren ten behoeve van onderhoud. En een deel van dat onderhoud willen ze bovendien online doen. Zolang het niet duidelijk hoe veilig dit gebeurt, of welke

maatregelen nodig zijn om dit veilig te maken, is het niet onterecht dat deze leveranciers de online toegang wordt ontzegd.

Figuur 7: OT-security uitdagingen

Wat zijn voor u de grootste uitdagingen op het gebied van digitale beveiliging van OT?



We kunnen het hebben over alle maatregelen die bedrijven kunnen of moeten nemen om de besturing van de productieomgeving te beveiligen. Maar dat zet niet veel zoden aan de dijk als een organisatie onvoldoende is ingericht is op een cyberveilige productieomgeving. Bedrijven moeten zich ervan bewust worden dat cybercriminelen zich steeds meer richten op de zwakste plekken binnen een organisatie en dat een “connected” OT-systeem een grote aantrekkingskracht uitoefent. De gevolgen van een succesvolle aanval op een productiesysteem kunnen groot zijn: de financiële consequenties van het langdurig stilvallen van de productie kunnen groot zijn. De gevolgen kunnen zelfs nog groter zijn, indien een hacker in staat is om sabotage te plegen aan de fysieke omgeving, waardoor mensen in gevaar komen.

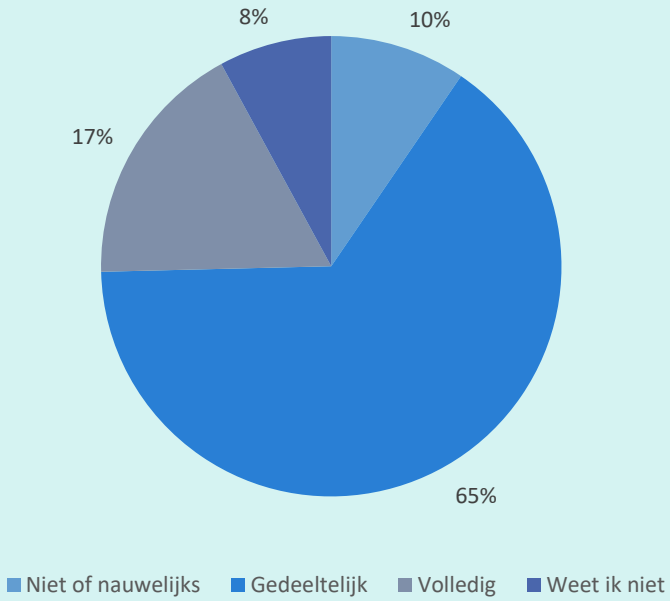
Bedrijven dienen allereerst de kwetsbaarheden en bijbehorende risico’s goed in kaart te brengen, zodat daarmee ook een beter bewustzijn kan worden gecreëerd binnen de organisatie. Als er inzicht is in de kwetsbaarheden (en dit vergt onderhoud!), kan inzichtelijk worden gemaakt welke beleid noodzakelijk is, welke maatregelen daarbij horen zijn en welk budget daarvoor vrijgemaakt dient te worden.

Een gevolg van deze exercitie zou wel eens kunnen zijn dat er vaker afwegingen moeten worden gemaakt tussen innovatie en security. Op dit moment zegt maar 1 op de 6 bedrijven dat cybersecurityrisico’s een rem vormen op digitale vernieuwing van de productieomgeving en dat zou de komende jaren wel een stevig kunnen gaan toenemen.

Op dit moment zullen bedrijven daarin nog wel de nodige stappen moeten nemen. Het is vaak niet of niet volledig inzichtelijk op welke wijze OT-systemen zijn gekoppeld aan de eigen IT-systemen of via netwerken benaderbaar zijn. De meeste bedrijven hebben er wel enig zicht op, maar dat is maar bij 1 op de 6 volledig voor wat betreft de samenhang van IT- en OT-systemen.

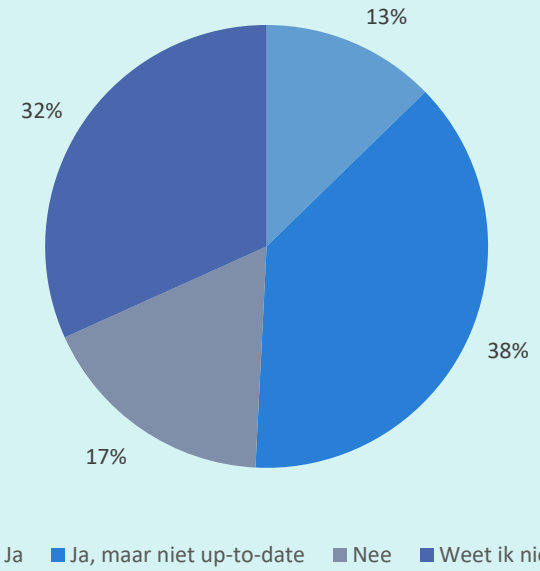
Figuur 8: Samenhang IT en OT-systemen

Is de samenhang tussen IT en OT-systemen in uw organisatie goed in kaart gebracht?



Figuur 9: Asset- en connectivity-database

Is er van uw OT-omgeving een up-to-date asset- en connectivity-database beschikbaar?



Als we doorvragen naar het gebruik van een asset- en connectivity-database voor de OT-omgeving, zien we dat bijna ieder organisatie in de proces/chemie sector nog wel een tandje bij mag schakelen. Op zich is zo'n database vaak wel aanwezig, maar deze is zelden up-to-date. Security in de OT-wereld staat voor een belangrijke inhaalslag!

Bijlage: Vragenlijst

Q1 In welke branche is uw organisatie actief?

- Datacenters/ICT-diensten/producten
- Procesindustrie
- Chemie & life sciences
- Voedingsmiddelenindustrie
- Maakindustrie
- Groothandel
- Detailhandel
- Bouw
- Maritieme sector
- (Overige) transport
- Financiële dienstverlening
- Overige zakelijke dienstverlening
- Overheid
- Onderwijs
- Zorg
- Overig

Q2. In welke mate bent u betrokken bij investeringen in IT-beveiliging binnen uw organisatie?

- Eindbeslisser
- Medebeslisser
- Belangrijke beïnvloeder
- Beïnvloeder
- Geen invloed [Programmer :SCREEN OUT]

Q3. Over hoeveel medewerkers beschikt uw organisatie?

- Minder dan 50 [SCREEN OUT]
- 50-99
- 100-249
- 250-499
- 500-999
- 1000 of meer

Q4. Welke van de volgende situaties zijn van toepassing op uw organisatie?

Ja/Nee

- We ontwikkelen zelf software
- We hebben IoT (Internet of Things)-oplossingen in gebruik of zijn ze aan het ontwikkelen

Q5. Met welke van de volgende IT-security incidenten heeft uw organisatie de afgelopen 12 maanden te maken gehad?

(1) Geen incidenten (2) Incident, maar schade voorkomen (3) Incident met schade (4) weet niet

- DDoS-aanval
- Ransomware
- Social Engineering (naar binnen praten)
- CEO-fraude
- Verlies of diefstal informatiedragers (laptop, USB-stick, etc.)
- Virus / malware
- Phishing
- Identiteitsdiefstal
- Computerinbraak (hack)
- Datadiefstal (niet fysiek)

Q6. Voor welk type incident bent u het meest bevreesd voor het komend jaar?

- DDoS-aanval
- Ransomware
- Social Engineering (naar binnen praten)
- CEO-fraude
- Verlies of diefstal informatiedragers (laptop, USB-stick, etc.)
- Virus / malware
- Phishing
- Identiteitsdiefstal
- Computerinbraak (hack)
- Datadiefstal (niet fysiek)
- Ik weet het niet, dat is juist het lastige
- Anders, namelijk_____

Q7. Wie is er binnen uw organisatie hoofdverantwoordelijk voor IT-beveiliging?

- CIO/IT Directeur
- CISO (Chief Information Security Officer)
- Hoofd informatiebeveiliging
- Netwerk- of systeembeheerder
- Riskmanager
- CFO/Financieel directeur
- CEO/Algemeen directeur
- Anders

[INDIEN Q4A="JA"]

Q8A. Bent u het eerder eens of oneens met de volgende stellingen met betrekking tot IT-beveiliging rond softwareontwikkeling binnen uw organisatie?

Geheel oneens/Oneens/Neutraal/Eens/Geheel eens/Niet van toepassing

- We hanteren de regel "secure by design"
- We hanteren de regel "privacy by design"
- Bij het ontwikkelen van nieuwe software komt security pas bij het eind van het proces in beeld

[INDIEN Q4B="JA"]

Q8B. Bent u het eerder eens of oneens met de volgende stellingen met betrekking tot IT-beveiliging rond IoT (Internet of Things) binnen uw organisatie?

Geheel oneens/Oneens/Neutraal/Eens/Geheel eens/Niet van toepassing

- We hanteren de regel "secure by design"
- Bij het ontwikkelen van nieuwe IoT-oplossingen komt security pas bij het eind van het proces in beeld
- Leveranciers van IoT-oplossingen moeten meer doen om hun producten goed te beveiligen

Q9. Met hoeveel procent groeien de uitgaven aan IT-beveiliging in 2019 binnen uw organisatie? En in 2020?

- 2019 _____%
- 2020 _____%

Q10. Welke van de volgende ontwikkelingen hebben de grootste invloed op investeringen in IT-security voor de komende 12 maanden?

- AVG/GDPR
- Andere wet- en regelgeving
- Toegenomen security bewustzijn op directieniveau
- Toenemende afhankelijkheid van IT
- Gebruik van de cloud
- Gebruik van mobiele apparaten en toepassingen
- Online investeringen (bijv. website, webshop, multichannel)
- Incidenten die hebben plaatsgevonden binnen de organisatie
- Incidenten die we hebben gezien buiten de organisatie

- Het algemene dreigingsbeeld
- Druk van klanten
- Behoefte aan meer IT-security kennis en vaardigheden
- Anders, namelijk_____

Q11. Hoeveel prioriteit hebben de volgende investeringen in de komende 12 maanden?

Geen enkele prioriteit/weinig/niet veel, niet weinig/Veel/Topprioriteit

- Identiteits- & toegangsbeheer
- Netwerkbeveiliging (firewall, VPN, Unified Threat Management, etc.)
- Veilige content en dreigingsbeveiliging (anti-malware, anti-spam, filtering, etc.)
- Preventie en risicobeheer (compliance, opsporing & onderzoek, incident/event management, etc.)
- Databeveiliging/encryptie
- Mobile security
- Medewerkersbewustzijn
- Monitoring/SIEM/SOC
- Advisering en consultancy
- Secure (software) development
- DevSecOps, security in DevOps
- Overig

Q12. Wordt bij verlies van privacygevoelige informatie ook gemeld bij de autoriteit persoonsgegevens, indien dit wettelijk verplicht is?

- Altijd
- Meestal
- Te weinig
- Niet
- Weet niet

Q12. Welke van de volgende beveiligingsmaatregelen heeft uw organisatie ingericht, specifiek met het oog op het beschermen van uw organisatie tegen complexe aanvallen?

- Toegangsbeheer
- Preventie (onderzoeken en blokkeren)
- Detectie (identificeren van verdachte events)
- Reactie (valideren van incidenten, in quarantaine plaatsen, etc.)
- Permanente monitoring
- Anders, namelijk

Q13. Welke van de volgende managed security services neemt u momenteel af en welke denkt u over 2 jaar af te nemen?

2018 2020

- Advies en implementatie
- Netwerkbeveiliging (firewall, VPN, evt. IDS, etc.)
- Managed security monitoring
- Penetratietesten en vaststellen kwetsbaarheden
- Compliance monitoring
- Anders, namelijk

Procesindustrie

Q1. Weerhouden cybersecurity risico's uw organisatie van digitale vernieuwingen in de productieomgeving/OT?

- Ja
- Nee
- Weet niet

Q2. Wordt cybersecurity binnen uw organisatie (voldoende) erkent als risicofactor binnen de productieomgeving/OT?

- Ja, meer dan voldoende
- Ja, maar niet voldoende
- Nee, het wordt niet als risicofactor onderkend
- Weet niet

Q3. Is het industriële controlesysteem verbonden met het kantoornetwerk?

- Ja
- Nee
- Niet van toepassing/weet niet

Q4. Wat zijn voor u de grootste uitdagingen op het gebied van digitale beveiliging van OT?

- Machineleveranciers die via het Internet gegevens uit willen lezen of onderhoud uitvoeren.
- Lange levenscyclus van machines
- Gebrek aan kennis van OT-beveiliging
- Geen goed zicht op de kwetsbaarheden
- Onvoldoende bewustzijn van de risico's
- Geen integrale security aanpak voor IT en OT
- Innovatie en security zitten elkaar in de weg.
- OT-beveiliging als ketenprobleem
- Anders, namelijk_____

Chemie & Life Sciences

Q1. Weerhouden cybersecurity risico's uw organisatie van digitale vernieuwingen in de productieomgeving/OT?

- Ja
- Nee
- Weet niet

Q2. Wordt cybersecurity binnen uw organisatie (voldoende) erkent als risicofactor binnen de productieomgeving/OT?

- Ja, meer dan voldoende
- Ja, maar niet voldoende
- Nee, het wordt niet als risicofactor onderkend
- Weet niet

Q3. Is het industriële controlesysteem verbonden met het kantoornetwerk?

- Ja
- Nee
- Niet van toepassing/weet niet

Q4. Wat zijn voor u de grootste uitdagingen op het gebied van digitale beveiliging van OT?

- Machineleveranciers die via het Internet gegevens uit willen lezen of onderhoud uitvoeren.
- Lange levenscyclus van machines
- Gebrek aan kennis van OT-beveiliging
- Geen goed zicht op de kwetsbaarheden
- Onvoldoende bewustzijn van de risico's
- Geen integrale security aanpak voor IT en OT
- Innovatie en security zitten elkaar in de weg.
- OT-beveiliging als ketenprobleem
- Anders, namelijk_____