Digitale veiligheid van Greenport West-Holland

Eindrapportage

GREENPORT West-Holland

HSD securitydelta.nl

provincie Zuid-Holland

Auteurs:
Dr. Marcel Spruit,
Lector Cyber Security & Safety

Dr. Emiel Kerpershoek,
Senior Onderzoeker Cybersecurity

De Haagse Hogeschool,
Kenniscentrum Cybersecurity
Lectoraat Cyber Security & Safety

let's change
YOU. US. THE WORLD.

Den Haag, maart 2022

DE HAAGSE HOGESCHOOL

De Haagse Hogeschool
Johanna Westerdijkplein 75
2521 EN Den Haag
www.dehaagsehogeschool.nl

Auteurs:
Dr. Marcel Spruit, Lector Cyber Security & Safety
Dr. Emiel Kerpershoek, Senior Onderzoeker Cybersecurity

De Haagse Hogeschool,
Kenniscentrum Cybersecurity
Lectoraat Cyber Security & Safety

Foto's/illustraties omslag en binnenwerk: Shutterstock.com
Vormgeving: Desk-Hopping DTP

Voorwoord

De voor u liggende onderzoeksrapportage geeft een beeld van de digitale veiligheid van de verschillende typen organisaties die actief zijn in het glastuinbouwcluster West-Holland. Voor productieorganisaties, zaadveredelingsorganisaties, handelsorganisatie en technisch toeleveranciers wordt een impressie gegeven van hun risicobewustzijn en de maatregelen die zij treffen om hun organisaties te beschermen tegen digitale veiligheidsincidenten. De aanleiding voor dit onderzoek vormt het verschijnen van de Roadmap gericht op het verbeteren van de weerbaarheid van de digitale economie van de Provincie Zuid-Holland, waarin het glastuinbouwcluster is aangemerkt als een van de aandachtsgebieden.

De rapportage is tot stand gekomen in nauwe samenwerking met de opdrachtgevers Greenport West-Holland en Security Delta (HSD) en is gefinancierd door de Provincie Zuid-Holland. We willen de organisaties in het glastuinbouwcluster bedanken voor hun openheid en hun meedenken in dit onderzoek. We zijn verheugd dat we met de tussentijdse bevindingen van ons onderzoek al een bijdrage hebben kunnen leveren aan de totstandkoming van het Cyberweerbaarheidscentrum i.o. en hopen hier, met de aanbevelingen in deze rapportage, ook in de toekomst een rol in te kunnen spelen.

Dr. Marcel Spruit, Lector Cyber Security & Safety
Dr. Emiel Kerpershoek, Senior Onderzoeker Cybersecurity
Den Haag, maart 2022

Managementsamenvatting

Eind 2020 is de *Roadmap verbeteren weerbaarheid digitale economie Provincie Zuid-Holland* gepubliceerd. In deze roadmap wordt het glastuinbouwcluster West-Holland aangewezen als één van de sectoren waarvan de digitale veiligheid het eerste aandacht behoeft. Dit vormde de aanleiding voor het huidige onderzoek naar de staat van de digitale veiligheid voor de verschillende typen organisaties die actief zijn in het glastuinbouwcluster. Het onderzoek heeft tot doel om een 'thermometer' in de sector te steken en richt zicht op de vraag '*Hoe is het gesteld met digitale veiligheid in het glastuinbouwcluster en wat is nodig om dit te verbeteren?'*

Op basis van interviews met representanten uit het glastuinbouwcluster en externe deskundigen op het gebied van digitale veiligheid, alsmede een enquête bij productieorganisaties, wordt een impressie gegeven van de relevante dreigingen voor de digitale veiligheid, de mogelijke impact ervan, het risicobewustzijn in het glastuinbouwcluster, de maatregelen die de organisaties treffen voor hun digitale veiligheid en de hulpmiddelen en ondersteuning die ze nodig hebben om hun digitale veiligheid te verbeteren.

Het onderzoek laat zien dat er een grote variatie is in het kennisniveau over relevante dreigingen voor de digitale systemen. Verscheidene bedreigingen, bijvoorbeeld supply chain-aanvallen, zijn slecht bekend, of worden onderschat. Niet alle dreigingen zijn voor alle organisaties even relevant, maar het lijkt erop dat vrijwel alle organisaties de voor hun relevante dreigingen voor de digitale veiligheid structureel onderschatten.

Alle organisaties in het glastuinbouwcluster zijn in belangrijke mate afhankelijk van hun digitale systemen. Door verdergaande digitalisering worden de digitale systemen steeds omvangrijker en steeds meer met elkaar en met het internet verweven en worden organisaties steeds afhankelijker van deze systemen. Dit zorgt niet alleen voor een grotere kwetsbaarheid, maar ook voor een grotere impact van incidenten met digitale systemen. De mogelijke impact van verstoring en misbruik van de digitale systemen wordt door de meeste organisaties structureel onderschat.

Op het eerste gezicht lijkt het aantal recente incidenten met digitale systemen in het glastuinbouwcluster beperkt. Dit lijkt echter een te lage inschatting doordat incidenten onopgemerkt kunnen zijn gebleven door onvoldoende monitoring en registratie. Hiernaast hebben incidenten uit het verleden weinig voorspellende waarde voor de toekomst. Door toenemende digitalisering en verwevenheid van digitale systemen binnen en buiten de organisatie, in combinatie met een toenemende waarde van de digitale gegevens in de organisaties, lijkt het slechts een kwestie van tijd tot criminele organisaties en statelijke actoren hun pijlen op deze cluster gaan richten.

Voor alle typen organisaties in het glastuinbouwcluster geldt dat ze nog de nodige maatregelen moeten treffen om de digitale veiligheid op een voldoende niveau te brengen. Ten tijde van het onderzoek was het glastuinbouwcluster over de hele linie digitaal onveilig. Veel organisaties, vooral productieorganisaties, hadden zelfs de meest basale maatregelen nog niet getroffen. Verder ontbrak het vaak aan gevoel van urgentie bij de directie, directiebetrokkenheid bij digitale veiligheid, de inzet van capabele menskracht voor digitale veiligheid en het toepassen van standaarden en standaard technieken voor digitale veiligheid.

In dit rapport worden aanbevelingen gedaan om de digitale veiligheid in het glastuinbouwcluster te verbeteren. De aanbevelingen zijn geclusterd in vier categorieën:

- Het verbeteren van het risicobewustzijn op het gebied van de digitale veiligheid.
- Het vergroten van de expertise op het gebied van digitale veiligheid.
- Het geven van ondersteuning bij het verbeteren van de digitale veiligheid.
- Het bevorderen van samenwerking en informatiedeling op het gebied van digitale veiligheid.

Om de aanbevelingen goed te kunnen implementeren, is het nuttig om groepen organisaties in kaart te brengen die te maken hebben met vergelijkbare problematiek op het gebied van digitale veiligheid en waartussen zodanig vertrouwen mogelijk is dat er overlegd en samengewerkt kan worden op het gebied van digitale veiligheid. Ondersteuning voor en coördinatie op het implementeren van de aanbevelingen kan verzorgd worden door het Cyberweerbaarheidscentrum GWH i.o.

INHOUDSOPGAVE

Voorwoord 3

Managementsamenvatting 5

1 Inleiding 9
1.1 Achtergrond 9
1.2 Doelstelling 10
1.3 Het glastuinbouwcluster 10
1.4 Onderzoeksaanpak 11

2 Literatuur 13
2.1 Digitalisering: Informatietechnologie & Operationele technologie 13
2.2 Dreigingslandschap in Nederland in 2021 13
2.3 Digitale veiligheid 14
2.4 Criteria voor digitale veiligheid van organisaties 16
2.5 Een collectieve aanpak van digitale veiligheid 16

3 Bevindingen en implicaties 17
3.1 Beeld van relevante dreigingen in het glastuinbouwcluster 17
3.2 Impact van digitale incidenten 19
3.3 Ervaringen met digitale incidenten 21
3.4 Digitaal veiligheidsniveau van organisaties in het glastuinbouwcluster 22
3.5 Behoefte aan hulpmiddelen en ondersteuning 27

4 Aanbevelingen 29
4.1 Risicobewustzijn verbeteren 30
4.2 Expertise vergroten 31
4.3 Ondersteuning inrichten 32
4.4 Samenwerking versterken 34

Bijlage 1: Interviewprotocol 36

Bijlage 2: Enquête 39

Bijlage 3: Geïnterviewden 42


AI

1 Inleiding

1.1 Achtergrond

Het glastuinbouwcluster omvat circa 2700 primaire glastuinbouwbedrijven (glasgroenteteelt, sierteelt) vermeerdering), maar ook vermeerderingsbedrijven, zaad-veredelingsorganisaties, handelsorganisaties en technisch toeleveranciers en kassenbouwers. Los van de bijdrage van de technisch toeleveranciers, kassenbouwers en zaadveredelingsorganisaties vertegenwoordigde het glastuinbouwcluster in 2019 een economische waarde van 7,9 miljard euro, ofwel 1% van het bruto binnenlands product van Nederland in dat jaar.[1] Ongeveer 85% hiervan heeft betrekking op de export van groenten, bloemen en planten.[2] Hiernaast vertegenwoordigen ook technisch toeleveranciers, kassenbouwers en zaadveredelingsorganisaties een aanzienlijke economische waarde. Zo wordt jaarlijks wereldwijd voor circa 1,4 miljard euro geïnvesteerd in de bouw van nieuwe met name hightech kassen. Ongeveer 900 miljoen euro hiervan heeft betrekking op opdrachten aan Nederlandse bedrijven.[3] Ook op het gebied van werkgelegenheid is het glastuinbouwcluster een belangrijke sector. Met ruim 87.000 arbeidsjaren, vertegenwoordigde het glastuinbouwcluster in 2019 1,1% van de nationale werkgelegenheid.

Voor een sector met deze omvang in economische waarde en werkgelegenheid kan Nederland het zich niet permitteren dat deze sector wordt verstoord of overgenomen door partijen in het buitenland. Als het gaat om digitale veiligheid gaat de aandacht van de Nederlandse overheid nog vooral uit naar dreigingen voor en kwetsbaarheden van vitale sectoren in Nederland. Echter, ook niet-vitale sectoren als het glastuinbouwcluster vertegenwoordigen een aanzienlijk belang voor de Nederlandse economie en samenleving. Het is daarom van belang dat ook het glastuinbouwcluster voldoende weerbaar is om nationale en internationale dreigingen voor de digitale veiligheid van de organisaties binnen de sector het hoofd te kunnen bieden. Ook vanuit de overheid worden nu stappen gezet om naast de vitale sectoren ook de niet-vitale sectoren te informeren over actuele dreigingsinformatie vanuit het Nationaal Cyber Security Centrum (NCSC).[4]

Net als veel andere sectoren is het glastuinbouwcluster in belangrijke mate afhankelijk geworden van digitale systemen en het internet. Sinds enkele decennia wordt het klimaat in de kassen beheerst met een computer die onder meer de verwarming en ventilatie aanstuurt en worden sensoren en actuatoren in de kas gebruikt voor bewatering en bemesting van gewassen of het uitvoeren van gewasmetingen. Vaak kan dit soort monitoring en aansturing op afstand worden bestuurd, bijvoorbeeld door een informatiesysteem van een derde partij of via een app op de smartphone van de teler. In de afgelopen jaren hebben ook nieuwe vormen van digitalisering als drones, robotisering, artificiële intelligentie en Internet of Things (IoT) hun intrede gedaan in de glastuinbouw. De digitalisering wordt in belangrijke mate gestuurd door de ambitie om efficiënter en effectiever te kunnen telen. Hierbij speelt het beeld van de autonome kas waarbij datagestuurd kan worden geteeld, met minimale inzet van personeel. Zo kan verdergaande digitalisering van de sector helpen om duurzamer om te gaan met energie, water en gewasbeschermingsmiddelen, om tekorten aan gekwalificeerd 'groen' personeel op te vangen en om het managen op afstand van kassen in het buitenland te vereenvoudigen.[5] De historie van de sector waarin Nederland zich heeft ontwikkeld als koploper in de internationale (glas) tuinbouw en de wil om huidige en toekomstige uitdagingen op te pakken, maakt dat het glastuinbouwcluster een sector is die sterk wordt gedreven door digitale innovaties.

Alhoewel digitale innovaties een belangrijke drijfveer zijn, staat het onderwerp digitale veiligheid in het glastuinbouwcluster niet hoog op de agenda. Voortschrijdende digitalisering leidt tot gebruik van meer apparatuur, programmatuur en koppelingen tussen digitale systemen. Omdat door toenemend gebruik van digitale systemen ook de digitale veiligheid onder druk komt te staan, is het van belang dat dit onderwerp meer prioriteit krijgt. Uit recent onderzoek naar de cybergereedheid van de economie van de Provincie Zuid-Holland blijkt dat in het glastuinbouwcluster digitale veiligheid vooral wordt gezien als een kostenpost en te weinig als een voorwaarde voor succesvolle ontwikkeling en groei. Om de digitale veiligheid beter op de agenda te krijgen heeft de Provincie Zuid-Holland een roadmap opgesteld voor het verbeteren van de cyberweerbaarheid in de verschillende sectoren in de provincie. In deze roadmap wordt het glastuinbouwcluster aangemerkt als een logisch startpunt voor het verbeteren van de cyberweerbaarheid. Het glastuinbouwcluster is relatief afhankelijk van innovaties in digitale systemen en

1 Voor de totale tuinbouwsector bedroeg de productiewaarde in 2020 ca. 27,9 miljard euro en 2,7% van het bbp. Zie ook de Digitaliseringsvisie Glastuinbouw, 2021.
2 **https://agrimatie.nl/ThemaResultaat.aspx?subpubID=2232&themaID=2280&indicatorID=2919&sector ID=2240**
3 The role of digitalisation in feeding and greening the megacities: Digitaliseringsvisie Glastuinbouw 2021, Greenport West-Holland/ InnovationQuarter.
4 **https://tweakers.net/nieuws/186756/nederlandse-overheid-waarschuwt-niet-vitale-bedrijven-voor-digitale-aanvallen.html**
5 The role of digitalisation in feeding and greening the megacities: Digitaliseringsvisie Glastuinbouw 2021, Greenport West-Holland/ InnovationQuarter.

vertegenwoordigt een grote economische waarde, waardoor verstoring van de digitale systemen grote impact kan hebben op de bedrijfsvoering van de organisatie of op de logistieke keten als geheel.[6] Hiermee vormde de roadmap een directe aanleiding voor het initiëren van het huidige onderzoek naar de digitale veiligheid van de Greenport.

Het onderzoek is uitgevoerd in opdracht van Greenport West-Holland[7] en financieel mogelijk gemaakt door de Provincie Zuid-Holland[8].

1.2 Doelstelling

In vervolg op het vooronderzoek naar de cybergereedheid van de economie van de Provincie Zuid-Holland is de doelstelling van dit onderzoek om de stand van de digitale veiligheid in het glastuinbouwcluster in kaart te brengen en aanbevelingen te formuleren voor het verbeteren van de digitale veiligheid. De centrale vraagstelling in dit onderzoek luidt:

Hoe is het gesteld met digitale veiligheid in het glastuinbouwcluster en wat is nodig om dit te verbeteren?

Om deze vraag te kunnen beantwoorden, worden in het onderzoek de volgende deelvragen beantwoord:

- Wat zijn de relevante dreigingen voor de digitale veiligheid van organisaties in het glastuinbouwcluster?
- Wat is de potentiële impact van digitale veiligheidsincidenten op organisaties in het glastuinbouwcluster?
- Zijn er al digitale veiligheidsincidenten opgetreden in het glastuinbouwcluster?
- Welk niveau van digitale veiligheid hebben organisaties in het glastuinbouwcluster op dit moment?
- Wat is de behoefte aan hulpmiddelen en ondersteuning voor het verbeteren van de digitale veiligheid van organisaties in het glastuinbouwcluster?

Dit onderzoek resulteert in een onderzoeksrapport, inclusief aanbevelingen die kunnen bijdragen aan het verbeteren van de digitale veiligheid van het glastuinbouwcluster.

1.3 Het glastuinbouwcluster

In het glastuinbouwcluster zijn verschillende typen organisaties actief. Deze organisaties zijn verantwoordelijk voor de inrichting van digitale veiligheid van hun eigen organisatie, en als ketenpartners verantwoordelijk voor de digitale veiligheid van het glastuinbouwcluster als geheel. In dit onderzoek onderscheiden wij de onderstaande typen organisaties.[9]

Productieorganisaties: Telers en vermeerderingsbedrijven zijn kleine tot grote organisaties die gewassen telen, of zaden en stekken opkweken. De groep is zeer divers van aard, variërend van kleine telers tot telers die zich hebben verenigd in telersverenigingen die een rol spelen in de handel en grote organisaties met locaties en afzetmarkten in het buitenland.[10] Productieorganisaties zijn in sterke mate afhankelijk van de beschikbaarheid van digitale gegevens ten behoeve van geautomatiseerde klimaatbeheersing en gewasbehandeling.

Handelsorganisaties: Middelgrote en grote organisaties die zich richten op handel, verpakking en transport van producten, import en export (o.a. van lokaal geproduceerde food en non-food producten) en opslag in warehouses. Voor handelsorganisaties geldt dat als de benodigde digitale gegevens niet beschikbaar zijn door uitval of verstoring van systemen dit kan leiden tot het stagneren van handel en transport van bederfelijke producten.

Zaadverdelingsorganisaties: Grote internationaal georiënteerde organisaties die zich richten op de ontwikkeling van zaden en rassen. Productieorganisaties in binnen- en buitenland vormen de belangrijkste afnemers. Intellectueel eigendom speelt een belangrijke rol, waardoor vertrouwelijkheid van digitale systemen een belangrijke factor is. Net als productieorganisaties zijn ook zaadveredelingsorganisaties in sterke mate afhankelijk van de beschikbaarheid van digitale gegevens voor onder meer klimaatbeheersing.

Technische toeleveranciers & kassenbouwers: Variëren van kleinere softwareleveranciers en IT-dienstverleners tot grote en internationaal georiënteerde leveranciers van hardware en kassenbouwers. Productieorganisaties en zaadveredelingsorganisaties in binnen- en buitenland

6 K. Gijsbers (2020). Cybergereedheid economie Provincie Zuid-Holland. Cyber4Board
7 **https://greenportwestholland.nl/**
8 **https://www.zuid-holland.nl/**
9 The role of digitalisation in feeding and greening the megacities: Digitaliseringsvisie Glastuinbouw 2021, Greenport West-Holland/ InnovationQuarter.
10 Bij het categoriseren van organisaties ten behoeve van dit onderzoek is ervoor gekozen om organisaties die naast teeltactiviteiten ook een duidelijke handelscomponent hebben in te delen in de categorie handelsorganisaties. De voornaamste reden hiervoor is dat handelsactiviteiten veelal resulteren in een hoger risicoprofiel voor de organisatie ten aanzien van hun digitale veiligheid.

vormen de belangrijkste afnemers. Voor de grote technisch toeleveranciers en kassenbouwers, maar ook voor IT-dienstverleners die in het glastuinbouwcluster actief zijn, geldt dat beschikbaarheid, integriteit en vertrouwelijkheid van hun systemen essentieel zijn om de netwerken en systemen van de klanten te beschermen.

Brancheverenigingen en koepels: Organisaties die telers, telersverenigingen of technisch toeleveranciers en kassenbouwers vertegenwoordigen, onder andere op het gebied van regionaal, nationaal en Europees beleid dat implicaties heeft voor de sector. Ook spelen zij vaak een ondersteunende rol in de professionalisering van hun leden op uiteenlopende terreinen.

Ook tussen organisaties van hetzelfde type bestaan verschillen die van invloed zijn op de digitale veiligheidsvraagstukken waarmee de organisatie te maken heeft. Zo vormen grote organisaties die internationaal actief zijn wellicht eerder een doelwit voor gerichte cyberaanvallen dan kleinere organisaties die vaker te maken hebben met ongerichte dreigingen. Los van het type organisatie hebben individuele organisaties in het glastuinbouwcluster uiteenlopende risicoprofielen.[11]

1.4 Onderzoeksaanpak

Dit onderzoek is uitgevoerd in 2021 en de eerste twee maanden van 2022. Voor de beantwoording van de onderzoeksvragen wordt in dit onderzoek gebruik gemaakt van desk research, semigestructureerde interviews en een enquête.

De desk research als methode van onderzoek omvat analyse van wetenschappelijke en vakliteratuur en documentatie over het glastuinbouwcluster en is gebruikt voor het theoretisch kader van het onderzoek en voor het opstellen van het protocol voor de interviews (zie bijlage 1) en de enquête. Voor de analyse van de digitale veiligheid van organisaties in het glastuinbouwcluster is gebruik gemaakt van het 3-pijlermodel voor informatiebeveiliging.[12]

In de eerste fase van het onderzoek zijn verkennende interviews gevoerd met cybersecurity-deskundigen van buiten de sector om meer zicht te krijgen op de eisen die aan organisaties in de glastuinbouw gesteld worden op het gebied van digitale veiligheid en best practices voor de aanpak van digitale veiligheid.

11 Zie ook **https://www.digitaltrustcenter.nl/stappenplan-risicoanalyse**

12 M. Spruit (2017). Volwassenheid informatiebeveiliging; 3-Pijlermodel. De Haagse Hogeschool. DOI: https:/doi.org/10.13140/RG.2.2.24840.16641

Vervolgens zijn interviews uitgevoerd met vertegenwoordigers van de verschillende typen organisaties in het glastuinbouw-cluster om de staat van de digitale veiligheid in hun organisatie in kaart te brengen en om met hen te spreken over hun risicoperceptie en ondersteuningsbehoefte. Per organisatie is gesproken met één persoon waardoor het beeld dat uit het interview is ontstaan van de inrichting van de digitale veiligheid van de organisatie onvolledig kan zijn. Wel bood de semigestructureerde aard van de interviews ruimte om door te vragen op de antwoorden van de geïnterviewde om onduidelijkheden of interpretatieverschillen op te helderen. De analyse van de interviews is eerst afzonderlijk uitgevoerd door de twee betrokken onderzoekers en daarna in onderlinge afstemming bijgeslepen.

De externe cybersecurity-deskundigen die zijn benaderd voor een interview zijn geselecteerd uit het netwerk van de onderzoekers. De organisaties die zijn benaderd voor de interviews zijn geselecteerd uit een lijst met organisaties in het glastuinbouwcluster die is opgesteld door Greenport West-Holland (GWH). Hiernaast is gebruik gemaakt van de sneeuwbalmethode waarbij geïnterviewden werden gevraagd naar potentiële interviewkandidaten bij andere organisaties uit het glastuinbouwcluster.

Anders dan bij de uitvoering van audits is tijdens de interviews niet gevraagd naar bewijs om de informatie uit het interview te staven. De verslagen van de interviews zijn niet geautoriseerd waardoor kleine interpretatiefouten bij de onderzoekers niet kunnen worden uitgesloten. Bovenstaande punten vormen echter geen belemmering voor het huidige onderzoek omdat dit beoogt om een indicatie te geven van de staat van de digitale veiligheid van de verschillende typen organisaties in het glastuinbouwcluster en niet om voor elke organisatie het veiligheidsniveau grondig vast te stellen.

In aanvulling op de desk research en de interviews is een enquête uitgevoerd (zie bijlage 2) om voor met name de productieorganisaties nader in kaart te brengen welke risico's zij zien voor de digitale veiligheid van hun organisatie en welke maatregelen zij hiervoor hebben getroffen. De vragen in de enquête zijn gebaseerd op het 3-pijlermodel voor volwassenheid van informatiebeveiliging[13] en de informatiebeveiligingsstandaard ISO 27001. De enquête is op 20 december 2021 uitgezet onder leden van Glastuinbouw Nederland[14] en leden van GroentenFruit Huis[15] en, na verzending van een reminder, gesloten op 11 januari 2022. Er zijn 66 reacties op de enquête ontvangen, waarvan 57 van productieorganisaties. Gezien de korte reactietijd rondom de jaarwisseling en mogelijke enquêtemoeheid bij de aangeschreven organisaties, bestaat de kans dat vooral organisaties hebben gereageerd met affiniteit voor digitale veiligheid. Dit kan de scores van met name de productieorganisaties enigszins positief kleuren.

13 M. Spruit (2017). Volwassenheid informatiebeveiliging; 3-Pijlermodel. De Haagse Hogeschool. DOI: https:/doi.org/10.13140/RG.2.2.24840.16641

14 **https://www.glastuinbouwnederland.nl/glastuinbouw/over-de-glastuinbouw/**

15 **https://groentenfruithuis.nl/**

2 Literatuur

2.1 Digitalisering: Informatietechnologie & Operationele technologie

De afgelopen decennia hebben zich grote ontwikkelingen voorgedaan in digitalisering op het gebied van informatie-technologie (IT), ook wel informatie- en communicatietech-nologie (ICT) genoemd. Hieronder wordt computergerelateerde technologie verstaan die kan worden gebruikt voor het creëren, verwerven, bewerken, opslaan, distribueren, presenteren en/of vernietigen van (digitale) gegevens.[16] De afgelopen decennia hebben zich grote ontwikkelingen voorgedaan op het gebied van IT-systemen voor kantoorautomatisering en administratieve automatisering, zoals de opkomst van mobiele apparatuur, de groei van het internet, de invoering van cloud computing, het werken vanuit verschillende locaties, het toepassen van kunstmatige intelligentie, etc.

Lange tijd ging digitalisering vooral over de IT. Minder vaak wordt hierbij gedacht aan de ontwikkelingen op het gebied van operationele technologie (OT), ook wel aangeduid met termen zoals procesautomatisering, industriële automatisering, Industrial Control Systems, etc.[17] Onder OT wordt computergerelateerde technologie verstaan om fysieke processen, systemen en infrastructuur te monitoren of aan te sturen. Dit kan bijvoorbeeld betrekking hebben op het automatiseren van de productie of van logistieke processen. Alhoewel het functioneren van de OT-systemen vaak bepalend is voor de bedrijfsvoering van organisaties krijgt de digitale veiligheid ervan nog vaak te weinig aandacht.[18] [19]

Ook in het glastuinbouwcluster spelen OT-systemen voor het monitoren en aansturen van fysieke processen en systemen een belangrijke rol. De ontwikkeling van OT-systemen, zoals klimaatsystemen, bewateringssystemen en productierobots, heeft in de afgelopen jaren een vlucht genomen. Doordat OT-systemen vaak kunnen worden aangestuurd door een analyseprogramma op een pc, of een app op een smartphone, zijn er ook steeds meer koppelingen ontstaan met IT-systemen.

Doordat steeds meer gegevens uit OT-systemen worden geanalyseerd in IT-systemen, zijn aanzienlijke gegevens-stromen ontstaan tussen de OT- en IT-systemen. Doordat IT-systemen in het algemeen met het internet zijn verbonden en OT-systemen gekoppeld zijn aan de IT-systemen, zijn de OT-systemen ook met het internet verbonden. Dit heeft voor de functionaliteit weliswaar voordelen, maar zorgt er ook voor dat alle dreigingen van het internet, zoals cyberspionage, ransomware, DDoS-aanvallen, hacktivisme, etc. nu ook voor de OT-systemen gelden. Of anders gezegd: cybercriminelen en statelijke actoren kunnen nu niet alleen de IT-systemen aanvallen, maar ook de OT-systemen. En dat doen ze ook.[20]

2.2 Dreigingslandschap in Nederland in 2021

In het recent verschenen Cybersecuritybeeld Nederland 2021 (CSBN 2021) concluderen de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC) dat de dreiging vanuit criminele organisaties en ook van statelijke actoren die gerichte aanvallen uitvoeren op vitale processen net als in voorgaande jaren onverminderd hoog blijft. De trend is hierbij dat de dreiging van deze actoren op gebied van de IT- en de OT-systemen zal toenemen voor de sectoren die hun processen verder automatiseren.[21]

In Nederland en in het buitenland zijn in de afgelopen jaren diverse voorbeelden geweest van deze toenemende dreiging.[22] Zo zijn in 2021 wereldwijd diverse ransomware-aanvallen uitgevoerd door criminele groepen op vitale sectoren, zoals energievoorziening, watervoorziening, (petro)chemische industrie, voedselvoorziening, transport, financiële instellingen en overheid. Een aantal aanvallen heeft het nieuws gehaald. Enkele voorbeelden hiervan uit het recente verleden zijn de uitschakeling van uraniumcentrifuges in Iran (2010), de uitval elektriciteitsnetwerk in Oekraïne (in 2015 en 2016), een ransomware-aanval op een containeroverslagbedrijf in Nederland (2017), een aanval op het elektriciteitsnetwerk (2018) en een oliepijplijn (2021) in de VS en diverse overheidsinstanties, defensieorganisaties en financiële instanties in de VS en Europa met de Ivanti Pulse Connect

16 M. Spruit (2018). Informatie onder controle. MS.
17 H. Luiijf en M. Klaver (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. International Journal of Critical Infrastructure Protection, nr. 35, pag. 1-16.
18 H. Luiijf en R. Lassche (2006). SCADA (on)veiligheid: een rol voor de overheid?. TNO-KEMA.
19 E. Luiijf (2012). Onbewust onveilig. Informatiebeveiliging, nr. 4, pag. 4-7
20 R. Brennenraedts, et al. (2020). Informatie-uitwisseling landelijk dekkend stelsel cybersecurity. WODC.
21 NCSC (2021). Cybersecuritybeeld Nederland CSBN 2021. NCTV/NCSC.
22 E. Luiijf (2012). Onbewust onveilig. Informatiebeveiliging, nr. 4, pag. 4-7.

Secure hack (2021).[23] [24] [25] Diverse online incidentenlijsten laten zien dat slechts een klein deel van alle incidenten het nieuws haalt en daarmee het topje van de ijsberg vormt.[26]

Het aantal incidenten op het gebied van IT- en OT-systemen dat in zich in het verleden heeft voorgedaan heeft weinig voorspellende waarde voor de te verwachten incidenten in de toekomst. Voortschrijdende digitalisering in een sector waar steeds meer koppelingen ontstaan tussen steeds meer IT- en OT-systemen vergroten het aanvalsoppervlak. Daarnaast ontwikkelen criminele organisaties en statelijke actoren steeds meer nieuwe en makkelijker toe te passen aanvalstechnieken, waardoor de dreiging nog verder toeneemt. Het aantal digitale incidenten in het algemeen en van sterk automatiserende sectoren in het bijzonder zal in de naaste toekomst sterk toenemen.

2.3 Digitale veiligheid

In het CSBN 2021 concluderen de NCTV en het NCSC dat de weerbaarheid tegen digitale dreigingen in Nederland nog altijd onvoldoende is.[27] Zij stellen vast dat, net als in voorgaande jaren, veel organisaties elementaire digitale veiligheidsmaatregelen, zoals het gebruik van sterke wachtwoorden en het tijdig patchen van kwetsbaarheden in systemen, niet of niet voldoende hebben getroffen. NCTV en NCSC zien ook grote verschillen in het kennisniveau van organisaties op het gebied van cybersecurity en digitale weerbaarheid. Met name kennisverschillen binnen het MKB, maar ook kennisverschillen tussen grote bedrijven en hun (MKB-)ketenpartners, waarbij een incident bij de één ook vaak impact heeft op de ander. Bovendien kunnen incidenten in de ene sector impact hebben op organisaties in een andere sector.[28]

De Cyber Security Raad (CSR) geeft aan dat de digitale weerbaarheid voor vitale processen in Nederland anno 2021 nog niet op orde is, waardoor basale dreigingen niet goed kunnen worden gepareerd of gedetecteerd.[29] Bedrijven en overheidsorganisaties in vitale sectoren worden weliswaar door het NCSC op de hoogte gehouden van actuele dreigingen, kwetsbaarheden en oplossingen om de cyberweerbaarheid te verhogen, maar deze berichtgeving is vooral toegespitst op IT-systemen en veel minder op OT-systemen die in veel vitale sectoren ook een belangrijke rol spelen.[30] Verstoring of uitval van digitale systemen in niet-vitale sectoren, zoals de glastuinbouw, kan ook leiden tot een aanzienlijke kostenpost voor de samenleving, maar deze sectoren kunnen nog geen gebruik maken van de diensten van het NCSC.[31]

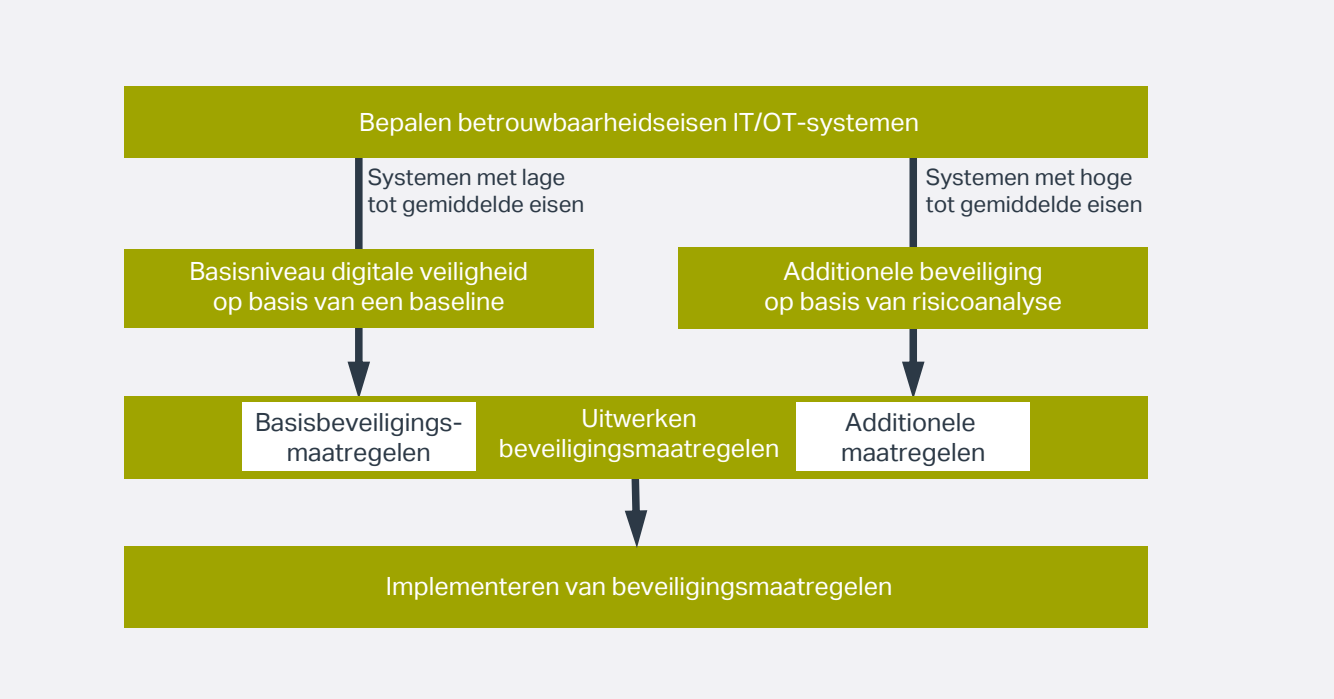
Vanwege het belang van de IT en de OT voor de bedrijfsvoering van de organisaties in het glastuinbouwcluster is het beveiligen ervan belangrijk voor de continuïteit van deze organisaties en van het cluster als geheel. Deze beveiliging wordt aangeduid als digitale veiligheid, cybersecurity, of cyberweerbaarheid.
Het NCSC definieert dit als:[32]

Het geheel aan maatregelen om (relevante) risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van (cyber)incidenten en wanneer (cyber)incidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken.

Deze definitie laat zien dat het van belang is om in kaart te brengen wat een aanvaardbaar risiconiveau is voor de organisatie en welke maatregelen kunnen worden getroffen om dit risiconiveau te bereiken.

Bij het inrichten van de digitale veiligheid in een organisatie kan onderscheid worden gemaakt tussen twee deels parallelle sporen, zie figuur 1.[33]

23 **https://www.trouw.nl/buitenland/cyberaanval-legt-oliepijpleiding-amerika-plat-ook-in-nederland-wordt-gevreesd-voor-hacks-bij-infrastructuur~b4a6a43b/**
24 R. Brennenraedts, et al. (2020). Informatie-uitwisseling landelijk dekkend stelsel cybersecurity. WODC.
25 **https://en.wikipedia.org/wiki/Ivanti_Pulse_Connect_Secure_data_breach**
26 zie bijvoorbeeld **https://en.wikipedia.org/wiki/List_of_security_hacking_incidents**
27 NCSC (2021). Cybersecuritybeeld Nederland CSBN 2021. NCTV/NCSC.
28 H. Luiijf en M. Klaver (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. International Journal of Critical Infrastructure Protection, nr. 35, pag. 1-16.
29 Cybersecurityraad (2021). Integrale aanpak cyberweerbaarheid. CSR.
30 **https://www.digitaltrustcenter.nl/nieuws/digital-trust-center-start-met-actief-informeren-bedrijven-over-digitale-dreigingen**
31 E. Luiijf (2012). Onbewust onveilig. Informatiebeveiliging, nr. 4, pag. 4-7.
32 NCSC (2021). Cybersecuritybeeld Nederland CSBN 2021. NCTV/NCSC.
33 M. Spruit, e.a. (2015). Safe in cyberspace; van awareness naar actie. Sdu.



Figuur 1. De tweesporenaanpak van digitale veiligheid

Het eerste spoor omvat de beveiligingsmaatregelen die nodig zijn om een basisniveau van digitale veiligheid te halen. Omdat de hiervoor benodigde maatregelen voor veel organisaties gelijk zijn, vormen deze de basis voor veel informatiebeveiligingsbaselines die organisaties kunnen gebruiken als checklist voor hun digitale veiligheidsmaatregelen. Een baseline is een samenhangende set maatregelen die organisatiebreed kunnen worden ingevoerd, wat kan bijdragen aan de herkenbaarheid, de efficiëntie en de effectiviteit van de maatregelen binnen de organisatie.[34]

Voor het kiezen van de maatregelen voor het eerste spoor kan bijvoorbeeld gebruik gemaakt worden van de zeer gangbare informatiebeveiligingsbaseline zoals beschreven in de informatiebeveiligingsstandaard ISO 27002. Een sterk vereenvoudigde set maatregelen dat een eerste stap kan vormen voor het eerste spoor is door het Digital Trust Center beschreven: [35]

- Inventariseer kwetsbaarheden
- Kies veilige instellingen
- Voer updates uit
- Beperk toegang tot systemen en data
- Voorkom virussen en andere malware

Het tweede spoor in de tweesporenaanpak richt zich op het grondig onder de loep nemen van de essentiële IT- en OT-systemen. Voor deze essentiële systemen mag men er niet vanuit gaan dat het basisniveau van digitale veiligheid uit het eerste spoor voldoende is en wordt voor elk essentieel systeem een risicoanalyse uitgevoerd. Hiermee worden de eventueel benodigde aanvullende maatregelen in kaart gebracht om daarmee de extra hoge risico's voor deze systemen voldoende te reduceren.[36] De aanpak in het tweede spoor is hiermee grondiger, maar ook tijdrovender.

34 M. Spruit en M. de Graaf (2004). Een twee-sporenaanpak voor informatiebeveiliging. Management Executive, nr. 1, pag. 34-37.
35 **https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen**
36 M. Spruit, e.a. (2015). Safe in cyberspace; van awareness naar actie. Sdu.

2.4 Criteria voor digitale veiligheid van organisaties

Voor dit onderzoek is, gebaseerd op het 3-pijlermodel voor volwassenheid van informatiebeveiliging[37] en de informatiebeveiligingsstandaard ISO 27001, een aantal criteria opgesteld om de volwassenheid van de digitale veiligheid van organisaties in het glastuinbouwcluster in kaart te brengen, zie tabel 1.Het gaat om zaken die door de organisaties moeten doen om digitale veiligheid een goede plek te geven in de organisatie. Voor organisaties die meer risico's lopen ligt de lat uiteraard hoger.

Tabel 1. Criteria voor de digitale veiligheid van organisaties

Er is directe betrokkenheid en commitment van de directie en management ten aanzien van de digitale veiligheid van de organisatie.
De elementaire beveiligingsmaatregelen voor de digitale systemen, zoals voorgesteld door het DTC[38], zijn op orde.
De rollen en taken voor de digitale veiligheid zijn toegekend binnen de organisatie (één of meer daarvoor toegeruste functionarissen zijn aangewezen voor de digitale veiligheid van de organisatie).
Er zijn formele afspraken met de leveranciers gemaakt over de digitale veiligheid van de door hun geleverde of beheerde systemen en over het herstel na incidenten.
Er is een baseline voor de digitale veiligheid van de organisatie geïmplementeerd waarmee een basisniveau van digitale veiligheid gerealiseerd wordt.
Er worden risicoanalyses uitgevoerd op alle belangrijke IT- en OT-systemen van de organisatie, ten minste bij aanschaf en bij elke belangrijke wijziging in een systeem of het dreigingslandschap.
Het netwerk en relevante IT- en OT-systemen van de organisatie worden gemonitord door de organisatie of een hiervoor ingeschakelde externe partijen en er worden testen en audits uitgevoerd.

2.5 Een collectieve aanpak van digitale veiligheid

Het glastuinbouwcluster is een omvangrijke sector met veel verschillende organisaties. De organisaties zijn georganiseerd in ketens, waarbinnen organisaties voor hun digitale veiligheid ook van elkaar afhankelijk zijn. Het is daarom van belang dat de organisaties in het glastuinbouwcluster op dit gebied gezamenlijk optrekken. Collectiviteit ten behoeve van digitale veiligheid in het glastuinbouwcluster kan zich richten op een aantal verschillende onderwerpen, zie tabel 2.

Tabel 2. Onderwerpen voor een collectieve aanpak van digitale veiligheid

Het vergaren en borgen van kennis op het gebied van digitale veiligheid, alsmede van de relevante dreigingen en kwetsbaarheden.
Het onderling delen van informatie over digitale veiligheid, onder meer over beveiligingsniveaus, toegepaste standaarden, incidenten, etc.
Het coördineren van de samenwerking op het gebied van digitale veiligheid tussen organisaties in het glastuinbouwcluster en met relevante organisaties daarbuiten.
Het vergroten van het risicobewustzijn binnen de organisaties in het glastuinbouwcluster, met name bij de organisaties waar dit nog niet goed gerealiseerd is.

37 M. Spruit (2017). Volwassenheid informatiebeveiliging; 3-Pijlermodel. De Haagse Hogeschool. DOI: https:/doi.org/10.13140/RG.2.2.24840.16641

38 **https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen**

3 Bevindingen en implicaties

Om de centrale onderzoeksvraag "*Hoe is het gesteld met digitale veiligheid in het glastuinbouwcluster en wat is nodig om dit te verbeteren?*" te kunnen beantwoorden, presenteren we in dit hoofdstuk de bevindingen van het onderzoek voor de vijf deelvragen:

1. Wat zijn de relevante dreigingen voor de digitale veiligheid van organisaties in het glastuinbouwcluster?
2. Wat is potentiële impact van digitale veiligheidsincidenten op organisaties in het glastuinbouwcluster?
3. Zijn er al digitale veiligheidsincidenten opgetreden in het glastuinbouwcluster?
4. Welk niveau van digitale veiligheid hebben organisaties in het glastuinbouwcluster op dit moment?
5. Wat is de behoefte aan hulpmiddelen en ondersteuning voor het verbeteren van de digitale veiligheid van organisaties in het glastuinbouwcluster?

3.1 Beeld van relevante dreigingen in het glastuinbouwcluster

Er is een grote variatie in het kennisniveau over relevante dreigingen voor de digitale systemen van de eigen organisatie. Verscheidene bedreigingen, bijvoorbeeld supply chain-aanvallen, zijn slecht bekend, of worden onderschat. Niet alle dreigingen zijn voor alle organisaties even relevant. Zo zijn bijvoorbeeld sommige organisaties vatbaarder voor digitale spionage dan andere. Maar het lijkt erop dat vrijwel alle organisaties de voor hun relevante dreigingen voor de digitale veiligheid structureel onderschatten.

3.1.1 Bevindingen

In de interviews met de vertegenwoordigers van de verschillende typen organisaties uit het glastuinbouwcluster en met externe cybersecurity-deskundigen is gesproken over het beeld dat zij hebben van de meest relevante dreigingen op het gebied van digitale veiligheid. De focus lag hierbij op de eigen organisatie en daarnaast op het glastuinbouwcluster als keten. De enquête voegde extra respons toe, met name vanuit de productieorganisaties.

In de onderstaande tabellen is een overzicht gegeven van de typen dreigingen en actoren waarvan de grootste dreiging uitgaat. Hierbij moet worden opgemerkt dat genoemde dreigingen en actoren grotendeels aan elkaar gerelateerd zijn. De meest genoemde dreigingen en actoren zijn eerst vermeld. Sommige van de genoemde dreigingen en actoren werden door de externe deskundigen naar voren gebracht.

Tabel 3. Typen dreigingen voor de digitale veiligheid van het glastuinbouwcluster

Typen dreigingen
Malware (bijv. ransomware)
Hacking
Phishing
(Bedrijfs)spionage
Menselijke fouten (onopzettelijk)
Supply chain-aanvallen
Sabotage (digitaal en fysiek)
Storingen in apparatuur en programmatuur (bijv. door elektriciteitsuitval)
Natuurlijke dreigingen (bijv. blikseminslag, wateroverlast, etc.)

Tabel 4. Typen actoren waar dreiging voor de digitale veiligheid van het glastuinbouwcluster vanuit gaat

Typen actoren
Cybercriminelen
Statelijke actoren
Actiegroepen/hacktivisten
IT-/OT-beheerders
Gebruikers
Klanten en leveranciers (ketenpartners)

Bij het beeld dat de verschillende organisaties in het glastuinbouwcluster hebben van de dreigingen voor de digitale veiligheid is op hoofdlijnen onderscheid te maken tussen de verschillende typen organisaties:

Productieorganisaties, en vooral de kleinere productieorganisaties, schatten de kans op digitale veiligheidsincidenten doorgaans laag in omdat zij zichzelf niet als een interessant doelwit zien en daarbij over het hoofd zien dat cybercriminelen vaak niet gericht aanvallen maar met 'hagel' schieten. Bovendien onderschatten ze de toenemende hoeveelheid IT en OT in hun eigen organisatie, veelal gekoppeld aan het internet, waardoor het aanvalsoppervlak voor cybercriminaliteit steeds groter wordt. Ook de toename van het aantal aanvallen door criminele organisaties en de ontwikkelingen van nieuwe aanvalstechnieken wordt hierbij vaak over het hoofd gezien. Hun beeld van de dreigingen voor de eigen organisatie, en voor de keten als geheel, beperkt zich doorgaans tot storingen die kunnen optreden in de systemen en, in veel mindere mate, op cybercriminelen die hun IT-systemen infecteren met malware. Er is weinig aandacht voor andere dreigingen voor hun IT-systemen. Nog minder aandacht is er voor dreigingen voor en kwetsbaarheden in hun OT-systemen. Opvallend is dat circa 90% van de productieorganisaties zich niet al te veel zorgen maakt over de dreigingen voor hun IT- en OT-systemen.

Dit staat in schril contrast met hoe de gesproken cybersecurity-deskundigen tegen de dreigingen voor deze groep organisaties aankijken.

Handelsorganisaties zijn grote tot zeer grote organisaties. Zij hebben in het algemeen een wat vollediger beeld van de dreigingen voor en kwetsbaarheden in hun digitale systemen. Zij realiseren zich dat ze vanwege hun omvang en economische waarde een interessant doelwit zijn voor cybercriminelen. Naast storingen, malware en menselijke fouten, maken zij zich ook zorgen over bijvoorbeeld kwetsbaarheden in de supply chain en de impact die dit kan hebben op de digitale veiligheid van hun organisatie en van de sector als geheel. Hoewel er bij deze organisaties meer aandacht is voor dreigingen voor met name de IT-systemen, loopt de aandacht voor de dreigingen voor de OT-systemen hier nog bij achter en hebben ze een incompleet beeld van de dreigingen die hiervoor relevant zijn.

Zaadveredelingsorganisaties hebben een vollediger beeld van de dreigingen voor en de kwetsbaarheden in hun digitale systemen dan de meeste andere organisaties in het glastuinbouwcluster. Zij realiseren zich dat ze vanwege hun omvang, internationale oriëntatie en economische waarde, maar ook vanwege innovatieve processen en intellectueel eigendom, een interessant doelwit zijn. Naast onder meer storingen, malware, menselijke fouten en kwetsbaarheden in de supply chain, hebben zij ook oog voor (bedrijfs)spionage en gerichte aanvallen door internationale concurrenten en statelijke actoren. Alhoewel deze organisaties zich bewust zijn van deze dreigingen is het dreigingsbeeld niet altijd even volledig en worden meer complexe dreigingen en actoren veelal onderschat. Bovendien beschikken zij niet altijd over voldoende kennis van geavanceerde aanvalsmethoden en van de meest recente kwetsbaarheden.

Technisch toeleveranciers hebben in het algemeen ook een vollediger beeld van de dreigingen voor en kwetsbaarheden in hun digitale systemen dan de meeste andere organisaties in het glastuinbouwcluster. Echter, binnen deze groep zijn de grote en internationaal georiënteerde kassenbouwers en leveranciers van (op afstand bestuurbare) hardware meer doordrongen van het brede pallet aan dreigingen en actoren dan de kleinere software-leveranciers. Net als de zaadveredelingsorganisaties hebben technisch toeleveranciers die IT en OT leveren meer oog voor (bedrijfs)spionage en gerichte aanvallen door internationale concurrenten en statelijke actoren. Toch geldt ook voor hen dat het dreigingsbeeld niet altijd even volledig is, dat de meer complexe dreigingen en actoren veelal onderschat worden en dat ze niet altijd voldoende kennis hebben van geavanceerde aanvalsmethoden en recente kwetsbaarheden.

3.1.2 Analyse & oplossingsrichtingen

In grote lijnen geldt op het gebied van dreigingen voor de digitale veiligheid het beeld dat is beschreven in het Cybersecuritybeeld Nederland 2021[39]. In deze jaarlijkse monitor signaleert de NCSC een aantal prominente risico's voor de Nederlandse samenleving, waaronder:

1. Spionage in de ontwikkeling van innovatieve technologieën of in de communicatie.
2. Sabotage en de inzet van ransomware-aanvallen op IT-systemen die door kunnen werken in OT-systemen en die belangrijke processen in de Nederlandse samenleving kunnen stilleggen.
3. Schending van de digitale ruimte in de vorm van geavanceerde supply chain-aanvallen in de ICT-leverancierskeken.
4. Grootschalige uitval door natuurlijke oorzaken, technische oorzaken of onopzettelijke menselijke fouten waardoor één of meer processen in de samenleving worden verstoord.

De NCSC geeft aan dat de Nederlandse samenleving in 2020 is getroffen door een breed scala aan digitale incidenten en dat het aantal in het jaar erna verder is toegenomen. Ook geven zij aan dat de voortschrijdende digitalisering in vrijwel alle sectoren in de Nederlandse samenleving ervoor zorgt dat de digitale en de fysieke wereld steeds minder goed van elkaar zijn te onderscheiden. Dit geldt ook voor het glastuinbouwcluster waar de digitaliseringsambitie voor de komende jaren hoog ligt en waar de IT-systemen, voor kantoor- en administratieve automatisering en aansturing van OT-systemen, en de OT-systemen, voor productie- en logistieke automatisering steeds meer met elkaar verweven raken.[40]

In dit onderzoek zien we dat de organisaties in het tuinbouwcluster die gemiddeld grotere risico's lopen, zoals de handelsorganisaties, de zaadveredelingsorganisaties en de technisch toeleveranciers, het dreigingsbeeld van NCSC in het algemeen wel op hun netvlies hebben. Minder compleet is hun beeld over welke dreigingen het dan precies gaat en in hoeverre hun IT- en OT-systemen daar kwetsbaar voor zijn. Zo geeft een deel van deze organisaties zelf al aan dat ze nog slechts beperkt aandacht besteden aan de meer complexe dreigingen zoals gerichte aanvallen door criminele organisaties, supply chain-aanvallen en spionage door statelijke actoren. Vanzelfsprekend scoort de ene organisatie iets beter en de ander iets minder, maar in het algemeen is hun dreigingsbeeld niet compleet.

39 NCSC (2021). Cybersecuritybeeld Nederland, CSBN 2021. NCTV/NCSC.

40 The role of digitalisation in feeding and greening the megacities: Digitaliseringsvisie Glastuinbouw 2021, Greenport West-Holland/InnovationQuarter.

Voor de organisaties die minder risico's lopen, zoals kleinere productieorganisaties, zijn minder dreigingen relevant. Maar hun dreigingsbeeld is in het algemeen nog beperkter, zodat ze toch een flink aantal voor hun relevante dreigingen over het hoofd zien of onderschatten.

De rode draad is dat over de hele linie organisaties de dreigingen die voor hun relevant zijn onderschatten. Dit betekent dat in de komende jaren meer aandacht nodig is om ontwikkelingen in dreigingen voor en kwetsbaarheden in de digitale systemen in deze sector in het oog te houden en hierover te communiceren. Het is aan te raden om daarbij gebruik te maken van specialistische kennis op dit gebied van buiten het glastuinbouwcluster.

3.2 Impact van digitale incidenten

Alle typen organisaties in het glastuinbouwcluster zijn in belangrijke mate afhankelijk van hun digitale systemen. Door verdergaande digitalisering worden IT- en OT-systemen steeds omvangrijker en steeds meer met elkaar en met het internet verweven en worden organisaties steeds afhankelijk van hun digitale systemen. Dit zorgt niet alleen voor een grotere kwetsbaarheid, maar ook voor een grotere impact van incidenten met digitale systemen. De mogelijke impact van verstoring en misbruik van de digitale systemen wordt door de meeste organisaties structureel onderschat.

3.2.1 Bevindingen

Uit de interviews en de enquête komt naar voren dat alle typen organisaties in het glastuinbouwcluster in belangrijke mate afhankelijk zijn van hun digitale systemen. Het beeld dat de geïnterviewden en de respondenten van de enquête hebben van de impact van incidenten met hun digitale systemen varieert aanzienlijk voor de verschillende typen organisaties.

Productieorganisaties zijn in sterke mate afhankelijk van de *beschikbaarheid* van onder meer de klimaatcomputers die de groeiomstandigheden en gewasbehandeling in de kas aansturen. In het algemeen schatten ze zelf in dat de impact van incidenten met hun OT-systemen, zoals de klimaatcomputer, hoger is dan wanneer deze hun IT-systemen betreffen. Het uitvallen van met name de OT-systemen kan al snel grote gevolgen hebben voor de kwaliteit van de gewassen, bijvoorbeeld wanneer de ramen van de kas niet of onvoldoende worden geopend op een hete zomerdag, of juist te lang openstaan op een koude winterdag. Toch maken de meeste productieorganisaties zich niet al te veel zorgen over problemen met hun IT- en OT-systemen en vertrouwen ze erop dat hun technisch toeleveranciers eventuele problemen met deze systemen tijdig zullen detecteren en oplossen. Deze houding is vooral gestoeld op gevoel, want maar weinig organisaties voeren serieus risicoanalyses uit. In mindere mate werd ook inbreuk op de *vertrouwelijkheid* van de digitale systemen gezien als een potentiële bron van schade voor de organisatie. Productieorganisaties willen vaak wel digitale gegevens delen binnen de coöperatie of met andere telers uit de regio als het om relatief uitontwikkelde producten gaat, maar niet daarbuiten vanwege de concurrentiepositie. Ook zou het uitlekken van prognoses en oogstgegevens kunnen leiden tot een verstoring van de prijsvorming voor gewassen. Schade als gevolg van de aantasting van de *integriteit* van de digitale systemen werd zeer beperkt gezien als een risico voor de organisatie. In lijn met de digitaliseringsambitie zullen productieorganisaties in de komende jaren verder digitaliseren waardoor IT- en OT-systemen omvangrijker worden en verder met elkaar en met het internet verweven raken en organisaties er steeds afhankelijker van worden. De impact van incidenten zal hierdoor verder toenemen.

Handelsorganisaties zijn voor hun bedrijfsvoering ook in belangrijke mate afhankelijk van de *beschikbaarheid* van hun digitale systemen. Wanneer deze systemen niet beschikbaar zijn, kan dat er voor handelsorganisaties toe leiden dat handel en transport van bederfelijke producten stagneert en daarmee al snel tot aanzienlijke schade leidt. Handelsorganisaties beschikken vaak over voldoende menskracht om de digitale veiligheid op te pakken en zijn hiervoor minder afhankelijk van hun technische toeleveranciers. Gezien de hogere risico's die deze organisaties lopen, is er te beperkt aandacht voor risicoanalyses waardoor de organisaties de impact van het uitvallen van hun systemen niet goed in kunnen schatten. De impact van aantasting van de *integriteit* en de *vertrouwelijkheid* van de digitale systemen wordt in mindere mate gezien als een risico voor de organisatie.,

Zaadveredelingsorganisaties zijn ook sterk afhankelijk van de *beschikbaarheid* van hun digitale systemen voor onder meer klimaatbeheersing in hun kassen. Ook voor het onderzoek dat een centrale plek inneemt in hun bedrijfsvoering is de beschikbaarheid van de digitale systemen van belang, maar dat is veelal minder tijdkritisch dan voor klimaatbeheersing in de kas. Voor de zaadveredelaars geldt dat inbreuk op de *vertrouwelijkheid* van de data wordt gezien als een belangrijke bron van schade voor de organisatie. Zaadveredelaars houden rekening met de aantasting van hun internationale concurrentiepositie als gevolg van (bedrijfs)spionage, maar ook met de invloed van geopolitieke spanningen en ambities van statelijke actoren op het gebied van ontwikkeling van een eigen glastuinbouwsector. Schade als gevolg van de aantasting van de *integriteit* van de digitale systemen werd in mindere mate gezien als een risico voor de organisaties. Ze vertrouwen erop dat integriteitsincidenten door hun eigen controles op de

systemen snel aan het licht zouden moeten komen en hersteld kunnen worden.

Technisch toeleveranciers dragen niet alleen voor hun eigen systemen maar ook voor die van hun klanten zorg voor de *beschikbaarheid* ervan en dit vormt daarmee een essentieel onderdeel van hun bedrijfsvoering. Uitval van hun eigen systemen kan doorwerken in de systemen van de klanten en het voorkomen ervan heeft hoge prioriteit. Technisch toeleveranciers ontwikkelen innovatieve systemen die wereldwijd in glastuinbouwsectoren worden gebruikt. Inbreuk op de *vertrouwelijkheid* van de systemen wordt daarom gezien als een potentieel grote bron van schade voor de marktpositie. Net als zaadveredelaars houden zij rekening met schade voor hun internationale concurrentiepositie als gevolg van (bedrijfs)spionage of het handelen van statelijke actoren. Ook voor technisch toeleveranciers die zich toeleggen op softwarepakketten of juist op het leveren van hightech kassen met bijvoorbeeld de nieuwste algoritmen voor de teelt van bepaalde gewassen is afscherming van intellectueel eigendom en daarmee vertrouwelijkheid van de systemen van groot belang. Schade als gevolg van de aantasting van de *integriteit* van de data werd in mindere mate gezien als een risico voor de organisatie. Zij vertrouwen erop dat integriteitsincidenten door hun eigen controles op de systemen snel aan het licht zouden moeten komen en hersteld kunnen worden.

3.2.2 Analyse & oplossingsrichtingen

Uit het onderzoek blijkt dat alle typen organisaties in het glastuinbouwcluster in belangrijke mate afhankelijk zijn van hun digitale systemen. De digitaliseringsvisie van het glastuinbouwcluster ziet in verdergaande digitalisering mogelijkheden om de sector efficiënter, effectiever en duurzamer te maken.[41] Het toekomstbeeld van een 'autonome kas' waar de inzet van kunstmatige intelligentie, drones en robotica het mogelijk maken om datagestuurd, nauwkeuriger en met minder personeel te telen spreekt hierbij tot de verbeelding. Echter, hierdoor zullen de gebruikte IT-systemen voor kantoor- en administratieve automatisering en aansturing van OT-systemen en de OT-systemen voor productie- en logistieke automatisering in omvang toenemen en steeds meer met elkaar en met het internet verweven raken. Dit zorgt er niet alleen voor dat de vatbaarheid voor dreigingen wordt vergroot, maar ook dat de bedrijfsvoering in toenemende mate afhankelijk wordt van de digitale systemen.

Met name bij de productieorganisaties is er vooralsnog weinig oog voor de verwevenheid van de IT- en OT-systemen. Ze zijn vooral beducht voor de impact van incidenten met de OT-systemen, maar lijken er geen rekening mee te houden dat ook incidenten met de IT-systemen de OT-systemen kunnen raken, en dat de IT-systemen voor derden een brug vormen tussen het internet en de OT-systemen.

De grotere afhankelijkheid van digitale systemen betekent een grotere impact voor de organisatie als deze systemen uitvallen. Slechts zeer weinig organisaties voeren goede risicoanalyses uit. Bij de meeste organisaties worden de gevolgen van het uitvallen van digitale systemen onderschat. Niet alleen door onderschatting van de dreigingen voor en kwetsbaarheden in de digitale systemen, maar ook door onderschatting van de impact van het uitvallen van deze systemen. Bovendien wordt de invloed en de mogelijkheden van systeemleveranciers bij het voorkomen en oplossen van incidenten nogal eens te hoog ingeschat.

De impact door aantasting van de integriteit (correctheid) van digitale systemen wordt nog ernstiger onderschat. Door de inzet van digitalisering in de glastuinbouw worden de processen in hoge mate aangestuurd en uitgevoerd door digitale systemen. Naarmate de digitale systemen meer met elkaar verweven raken werkt het disfunctioneren van één systeem door in de andere systemen. Wanneer digitalisering ook wordt gebruikt om de inzet van personeel terug te brengen, dan zal het waarschijnlijk ook langer duren voordat het foutief functioneren van systemen wordt opgemerkt, waardoor de impact van incidenten verder toeneemt. De integriteit van de digitale systemen moet dan ook hoger op de agenda komen te staan.

Verder is het van belang dat met name de productie-organisaties meer aandacht gaan besteden aan de vertrouwelijkheid van de digitale systemen. Bij handels-organisaties, zaadveredelingsorganisaties en technisch toeleveranciers staat vertrouwelijkheid, in het licht van de grotere risico's die ze op dit vlak lopen, vaak al hoger op de agenda. Bij de productieorganisaties is dit nog in beperkte mate het geval, terwijl het uitlekken van digitale gegevens ook voor hen impact kan hebben op hun concurrentiepositie, of markt- en prijsverstorend kunnen werken.

41 The role of digitalisation in feeding and greening the megacities: Digitaliseringsvisie Glastuinbouw 2021, Greenport West-Holland/ InnovationQuarter.

3.3 Ervaringen met digitale incidenten

Op het eerste gezicht lijkt het aantal recente incidenten met IT en OT in het glastuinbouwcluster beperkt. Dit beeld lijkt echter een te lage inschatting doordat incidenten onopgemerkt kunnen zijn gebleven door onvoldoende monitoring en registratie. Hiernaast hebben incidenten uit het verleden weinig voorspellende waarde voor de toekomst. Door toenemende digitalisering en verwevenheid van IT- en OT-systemen binnen en buiten de organisatie, in combinatie met een toenemende waarde van de digitale gegevens in de organisaties in het glastuinbouwcluster, lijkt het slechts een kwestie van tijd tot criminele organisaties en statelijke actoren hun pijlen op deze cluster gaan richten.

3.3.1 Bevindingen

Uit de interviews en de enquête blijkt dat het aantal incidenten met digitale systemen in de afgelopen jaren is meegevallen. Een deel van de geïnterviewden en respondenten geeft aan zelf een incident te hebben meegemaakt, zij het niet altijd even ernstig. De geïnterviewden merken daarbij op dat het monitoren van de digitale systemen en de registratie van incidenten in veel gevallen te wensen over laten, dus het werkelijke aantal incidenten zou hoger kunnen liggen. Bovendien is er onduidelijkheid over wanneer een incident als zodanig beschouwd moet worden. Er gaat van alles mis, van zeer klein, zoals spam, tot zeer groot, zoals ransomware, maar niet alles wordt als incident geteld. Verder tellen sommigen storingen in de digitale systemen en het netwerk niet als incident, terwijl anderen dat wel doen.

Vanuit de verschillende typen organisaties komen de volgende beelden naar boven.

Productieorganisaties geven in een aantal gevallen aan dat zij naast storingen en menselijke fouten wel eens slachtoffer zijn geweest van een (ongerichte) ransomware-aanval waarbij IT-systemen werden geïnfecteerd. Uit het onderzoek blijkt dat ruim 5% van de productieorganisaties is getroffen door een serieuze verstoring met een infrastructurele oorzaak. Iets minder dan 10% van de organisaties heeft in de afgelopen 2 jaar te maken gehad met één of meer aanvallen op de digitale systemen van hun organisatie. Hiernaast geeft nog 10% van de organisaties aan dat zij andere organisaties kennen die door een cyberaanval zijn getroffen. Productieorganisaties horen ook geruchten van ransomware-aanvallen in het glastuinbouwcluster, maar ze weten doorgaans niet van de hoed en de rand. Voor de ransomware-aanvallen waar ze zelf mee te maken hebben gehad, gaven ze aan dat de leverancier van de geïnfecteerde systemen dit toen heeft kunnen verhelpen met behulp van back-ups, waardoor de impact van deze incidenten beperkt is gebleven.

Handelsorganisaties hebben in een enkel geval te maken gehad met van een ransomware-aanval waarbij IT-systemen werden geïnfecteerd, maar niet heel recent. Hiernaast noemen zij ook enkele gevallen van spear phishing[42] in de vorm van Business E-mail Compromise fraude.[43] Verder hebben zij geruchten gehoord over meer digitale veiligheidsincidenten in het glastuinbouwcluster, maar kennen daarvan niet de details.

Zaadveredelingsorganisaties maken geen melding van ransomware bij henzelf. Hierin speelt mogelijk mee dat ongerichte ransomware-aanvallen afdoende worden afgevangen door de digitale veiligheidsmaatregelen die deze organisaties hebben getroffen. Wel geeft een enkele veredelaar aan in het verleden te maken te hebben gehad met bedrijfsspionage of pogingen daartoe.

Technische toeleveranciers maken geen melding van ransomware bij henzelf. Wel geven zij aan dat sommige van hun klanten hier mee te maken hebben gehad. Dat technisch toeleveranciers zelf niet zijn getroffen komt mogelijk doordat ongerichte ransomware-aanvallen afdoende worden afgevangen door de digitale veiligheidsmaatregelen die deze organisaties hebben getroffen. Net als de zaadveredelingsorganisaties geven ook enkele technisch toeleveranciers aan in het verleden te maken te hebben gehad met bedrijfsspionage of pogingen daartoe en enkele gevallen van spear phishing in de vorm van Business E-mail Compromise fraude.

42 Phishing is het hengelen naar en andere gevoelige gegevens van mensen door middel van misleidende e-mails of berichten. Bij spear phishing wordt dit toegespitst op één persoon en zijn de misleidende e-mails of berichten vaak minder gemakkelijk als dusdanig te herkennen doordat er gebruik wordt gemaakt van beschikbare persoonlijke gegevens en bedrijfsgegevens voor meer geloofwaardigheid.

43 Business E-mail Compromise fraude is een vorm spear phishing waarbij de mail afkomstig lijkt van een collega of van een leidinggevende (in welk geval sprake is van CEO fraude) en waarin bijvoorbeeld een frauduleuze betaalopdracht wordt gegeven aan een medewerker van de financiële administratie.

3.3.2 Analyse & oplossingsrichtingen

Afgaande op de interviews en de resultaten uit de enquête lijkt het aantal recente incidenten met digitale systemen in het glastuinbouwcluster beperkt te zijn. Het is de vraag of dit beeld klopt. Ten eerste kan een deel van de incidenten onopgemerkt zijn gebleven doordat digitale systemen veelal niet goed worden gemonitord en een deel van de aanvallers moeite doet om niet op te vallen, zoals onder meer het geval is bij (bedrijfs) spionage en botnets[44]. Ten tweede worden niet alle digitale veiligheidsincidenten als zodanig herkend en aangemerkt. Zo kan een door malware veroorzaakte storing bijvoorbeeld worden beschouwd en opgelost als een 'gewone' storing. Ook andere incidenten veroorzaakt door elektriciteitsuitval, blikseminslag, onopzettelijke menselijke fouten, fraude, etc. worden veelal niet als digitaal veiligheidsincident beschouwd, terwijl ze dat wel zijn, omdat ze leiden tot uitval of verstoring van de digitale systemen en ingrijpende gevolgen kunnen hebben.

Zelfs als het aantal digitale veiligheidsincidenten tot op heden laag is gebleven, dan nog zegt dit nog weinig over de toekomst. Nu al laat de huidige cybercrime-praktijk in Nederland zien dat organisaties uit steeds meer sectoren slachtoffer worden, zoals ziekenhuiszorg, onderwijsinstellingen en vitale sectoren.[45] [46] Gezien de voortschrijdende digitalisering en de waarde van organisaties binnen het glastuinbouwcluster lijkt het slechts een kwestie van tijd voordat criminelen hun pijlen ook hierop gaan richten. Daarnaast is een deel van het glastuinbouwcluster vanwege de unieke kennis aantrekkelijk voor criminele organisaties en statelijke actoren uit het buitenland. Dergelijke actoren kunnen in korte tijd een aanzienlijke digitale aanvalscapaciteit in stelling brengen. Dit betekent dat de kans op incidenten met digitale systemen door storingen en aanvallen in de naaste toekomst snel kan stijgen.

Om de digitale veiligheid van het glastuinbouwcluster te verbeteren, is het van belang om goed inzicht te krijgen in de digitale incidenten die de sector treffen. Dit betekent dat de digitale systemen van organisaties in het glastuinbouwcluster goed moeten worden gemonitord om dreigingen en incidenten te detecteren. Ook is het van belang dat er sprake is van een goede incidentenregistratie voor het glastuinbouwcluster en dat hierover goed wordt gecommuniceerd binnen het glastuinbouwcluster om andere organisaties tijdig te kunnen informeren over actuele dreigingen en kwetsbaarheden.

3.4 Digitaal veiligheidsniveau van organisaties in het glastuinbouwcluster

Voor alle typen organisaties in het glastuinbouwcluster geldt dat ze nog de nodige maatregelen moeten treffen om de digitale veiligheid op een voldoende niveau te brengen. Ten tijde van het onderzoek was het glastuinbouwcluster over de hele linie digitaal onveilig. Veel organisaties, vooral productieorganisaties, hadden zelfs de meest basale maatregelen nog niet getroffen. Verder ontbrak het vaak aan gevoel van urgentie bij de directie, directiebetrokkenheid bij digitale veiligheid, de inzet van capabele menskracht voor digitale veiligheid en het toepassen van standaarden en standaard technieken voor digitale veiligheid.

3.4.1 Bevindingen

Een centraal onderdeel van het onderzoek vormde het in kaart brengen van het digitaal veiligheidsniveau van de organisaties. Op basis van de interviews en de enquête is per type organisatie in kaart gebracht in hoeverre zij voldoen aan de criteria voor digitale veiligheid uit paragraaf 2.4. Dit betrof respectievelijk het gevoel van urgentie in de organisatie om digitale veiligheid goed op te pakken, met name op directieniveau, het organiseren van de digitale veiligheid, met name de inzet van menskracht, het toekennen van rollen en taken en het maken van externe afspraken op het gebied van de digitale veiligheid, en diverse maatregelen om de IT- en OT-systemen van de organisatie te beveiligen en de beveiliging te toetsen.[47] [48] [49] [50] De gemiddelde resultaten voor de verschillende typen organisaties zijn voor ieder onderdeel weergegeven in tabel 5. Individuele organisaties kunnen wat hoger of lager scoren.

44 Een botnet is een verzameling van met malware geïnfecteerde computers die via deze malware op afstand kunnen worden bestuurd en gezamenlijk kunnen worden ingezet voor ongewenste activiteiten, zoals een DDoS-aanval. Zie P. van Houten, e.a.(2019). Informatiebeveiliging onder controle. Pearson.
45 CBS (2020) Cybersecuritymonitor 2020, CBS **https://www.cbs.nl/nl-nl/publicatie/2021/18/cybersecuritymonitor-2020**
46 NCSC (2021). Cybersecuritybeeld Nederland, CSBN 2021. NCTV/NCSC.
47 P. van Houten, e.a.(2019). Informatiebeveiliging onder controle. Pearson.
48 M. Spruit, e.a. (2015). Safe in cyberspace; van awareness naar actie. Sdu.
49 M. Spruit (2017). Volwassenheid informatiebeveiliging; 3-Pijlermodel. De Haagse Hogeschool.
50 ISO/IEC 27001, 2005

*Tabel 5. Overzicht digitaal veiligheidsniveau per organisatietype**

Organisatietype	Urgentie-gevoel	Organisatie van digitale veiligheid	Maatregelen voor IT (administratieve automatisering, kantoor-automatisering en aansturing van OT)				Maatregelen voor OT (productieautomatisering en logistieke automatisering)			
			Elementaire maatregelen	Baseline/ ISMS	Risicoanalyse	Monitoring/ testen/ audits	Elementaire maatregelen	Baseline/ ISMS	Risicoanalyse	Monitoring/ testen/ audits
Productie-organisaties	–	-/+	–	–	–	-/+	–	–	–	-/+
Zaadveredelings-organisaties	±	±	+	±	±	±	+	–	–	±
Technisch toeleveranciers/ kassenbouwers	±	±	+	-/+	±	-/+	+	–	–	–
Handelsorganisaties	±	±	+	-/+	–	±	+	–	–	–

* *Scores kunnen variëren van onvoldoende (–), middelmatig (±), tot goed (+).*

Bij de beoordeling van de organisaties zijn de risicoprofielen van de organisaties als uitgangspunt genomen. Wanneer een organisatie grotere risico's loopt dan andere organisaties, dan zal deze organisatie waarschijnlijk ook meer maatregelen moeten treffen om de risico's tot een acceptabel niveau terug te dringen. De score van een organisatie hangt af van de mate waarin de organisatie voldoende aan digitale veiligheid heeft gedaan, in het licht van de risico's die de organisatie loopt.

De tabel laat zien dat er voor de verschillende typen organisaties grote variaties bestaan in de mate waarin voldaan wordt aan de criteria voor de digitale veiligheid. Daarnaast zijn er dan de variaties van de individuele organisaties ten opzichte van de gemiddelde scores, maar in het algemeen waren de onderlinge verschillen binnen een groep niet erg groot. Waar de verschillen wel groot waren, is dat aangegeven met een range (–/+, oftewel variërend van – tot +).

Hieronder gaan we in op de aangetroffen niveaus voor het gevoel van urgentie voor digitale veiligheid, de organisatie van digitale veiligheid en de maatregelen voor de digitale veiligheid van de IT- en OT-systemen.

Het gevoel van urgentie voor digitale veiligheid

Bij de *productieorganisaties* is het slecht gesteld met het gevoel van urgentie voor digitale veiligheid. Minder dan 10% van de organisaties maakt zich serieus zorgen over incidenten met hun IT- of OT-systemen. Meer dan 70% van de organisaties geeft de eigen digitale veiligheid een voldoende of hoger. Dit beeld van de eigen digitale veiligheid is veel te rooskleurig. Mogelijk is het ingegeven door (te) groot vertrouwen in de leveranciers, maar het geeft ook blijk van een laag gevoel van urgentie.

Gezien de handel- en veilingactiviteiten en de breed vertakte connecties in het glastuinbouwcluster zijn *handelsorganisaties* verder met digitalisering en lopen daardoor meer risico's. Bovendien vormen ze een aantrekkelijk doelwit voor gerichte cyberaanvallen. In het algemeen hebben de handelsorganisaties een redelijk kennisniveau van de relevante dreigingen, maar qua aandacht van directie/management moet de digitale veiligheid nog te veel wedijveren met de commerciële doelstellingen van de organisaties.

Omdat intellectueel eigendom een belangrijke rol speelt in de bedrijfsvoering van *zaadveredelingsorganisaties* kan digitale veiligheid doorgaans rekenen op de aandacht van directie/management. De internationale oriëntatie, economische waarde en de specifieke kennis maken dat deze organisaties grote risico's lopen, waaronder die aangaande gerichte cyberaanvallen door criminele organisaties of statelijke actoren. Internationaal georiënteerde *technisch toeleveranciers* die zich toeleggen op het leveren van hardware en bouwers van hightech kassen lopen om vergelijkbare redenen grote risico's. Voor beide typen organisaties zien we dat het gevoel van urgentie voor de digitale veiligheid bovengemiddeld is, maar niet zo hoog als past bij hun risicoprofiel.

De organisatie van digitale veiligheid

De organisaties in het glastuinbouwcluster verschillen in de mate waarin zij de aanpak van digitale veiligheid hebben verankerd in de organisatie. Hierbij kan worden gekeken naar de menskracht die beschikbaar is voor de digitale veiligheid en naar de mate waarin zij hiervoor taken en rollen hebben toegewezen en afspraken over digitale veiligheid hebben gemaakt met de leveranciers.

De *productieorganisaties* hebben in het algemeen nauwelijks menskracht beschikbaar voor de digitale veiligheid. Kleinere productieorganisaties hebben doorgaans hun digitale veiligheid grotendeels of zelfs helemaal bij de technisch toeleveranciers gelegd, zij het meestal zonder daar goede afspraken over gemaakt te hebben. Voor de resterende taken op het gebied van de digitale veiligheid zijn weinig of geen mensen beschikbaar en deze taken worden dan ook meestal niet of nauwelijks opgepakt. Bij enkele grotere organisaties houdt de directie zich met de digitale veiligheid bezig, zijn er enkele medewerkers voor digitale veiligheid en zijn afspraken over digitale veiligheid gemaakt met de leveranciers.

Het beeld van de *handelsorganisaties*, de *zaadveredelings-organisaties* en de *technisch toeleveranciers* is grotendeels vergelijkbaar met het beeld van de grotere productie-organisaties. Zij hebben doorgaans aandacht en mensen beschikbaar voor de aanpak van de digitale veiligheid en hiervoor rollen en taken toegekend, alsmede afspraken over digitale veiligheid gemaakt met de leveranciers. Maar ook voor deze organisaties geldt dat dit, in het licht van het hogere risicoprofiel van deze organisaties, nog niet voldoende is ingevuld.

De maatregelen voor de digitale veiligheid van de IT- en OT-systemen

Voor de verschillende typen organisaties in het glastuinbouw-cluster is in kaart gebracht welke maatregelen zij hebben getroffen ten behoeve van de digitale veiligheid van de organisatie. Hierbij is gekeken naar het treffen van elementaire digitale veiligheidsmaatregelen,[51] het implementeren van een basisniveau van digitale veiligheid (baseline, bijv. gebaseerd op ISO 27002), aanvullende maatregelen op basis van risicoanalyse, monitoring om verdacht verkeer op de netwerken tijdig te detecteren, (penetratie)testen om kwetsbaarheden in de (toegang tot) digitale systemen in kaart te brengen, social engineering-testen om kwetsbaarheden in de fysieke toegang in kaart te brengen en audits om de compliance met de procedures en werkinstructies in kaart te brengen.

Voor de maatregelen die zijn getroffen om de digitale veiligheid van de IT- en OT-systemen te borgen laten de organisaties een uiteenlopend beeld zien. Ook tussen organisaties van hetzelfde type zijn hierbij opvallende verschillen.

Gezien de lagere risico's op het gebied van de digitale veiligheid hebben kleinere *productieorganisaties* in het algemeen wat minder beveiligingsmaatregelen nodig. Toch zitten de maatregelen van deze organisaties beduidend lager dan wat reëel is. Ruim 80% van de productieorganisaties geeft desgevraagd aan dat zij zelfs de elementaire digitale veiligheidsmaatregelen nog niet op orde hebben. Voor veel organisaties geldt dat een deel van de elementaire maatregelen is opgepakt door leveranciers, maar die beperken zich tot hun eigen systemen en koppelvlakken en in het algemeen niet de andere systemen van de klant.

Van de productieorganisaties die hun elementaire maatregelen getroffen hebben, maken maar weinig gebruik van een gestandaardiseerd basisniveau of baseline voor digitale veiligheid en risicoanalyses. Slechts vijf productieorganisaties gaven aan gebruik te maken van een al dan niet gestandaardiseerd basisniveau voor digitale veiligheid en twee organisaties voeren volledige risicoanalyses uit op hun kritische IT- en OT-systemen.

Ongeveer de helft van de productieorganisaties doet in mindere of meerdere mate iets aan monitoring van hun digitale systemen, veelal uitgevoerd door een van hun leveranciers. Een vijfde van de productieorganisaties maakt gebruik van enige vorm van testen om kwetsbaarheden voor de digitale veiligheid van hun organisatie in kaart te brengen.

Handelsorganisaties hebben door de bank genomen de digitale veiligheidsmaatregelen op orde. Wel varieert het beeld van de getroffen maatregelen op punten. Zo maakt een grote handelsorganisatie structureel gebruik van een gestandaardiseerd basisniveau voor digitale veiligheid van de IT-systemen en hebben zij een managementsysteem voor digitale veiligheid (ISMS) ingericht, terwijl een kleinere handelsorganisatie hier niet mee werkt. Voor de OT-systemen is nog geen gestandaardiseerd basisniveau voor digitale veiligheid in gebruik. Risicoanalyses die worden uitgevoerd omvatten niet alle kritische IT- en OT-systemen. In sommige gevallen waren ze beperkt tot procesniveau en werden niet alle relevante risico's hierin meegewogen. Van monitoren, testen en auditen wordt wel gebruik gemaakt, maar doorgaans met een beperkte scope en incidenteel. Ook hier geldt dat maatregelen op het gebied van de OT-systemen achterlopen.

De *zaadveredelingsorganisaties* scoren hoger dan gemiddeld op de digitale veiligheid, maar niet zo hoog als we op voorhand hadden verwacht. Zij hebben hun elementaire maatregelen op orde. Veelal werken zij tot op zekere hoogte met een gestandaardiseerd basisniveau voor digitale veiligheid, zij het dat deze doorgaans niet volledig is geïmplementeerd en ook niet voor de gehele organisatie is toegepast. Zo worden bijvoorbeeld de OT-systemen hierin niet altijd meegenomen.

51 Denk aan het inventariseren van kwetsbaarheden, kiezen van veilige instellingen, tijdig uitvoeren van updates, gebruik van anti-malware en selectieve toegang tot systemen en data. Zie ook **https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen**

Hetzelfde beeld is van toepassing op een managementsysteem voor digitale veiligheid, risicoanalyses, monitoren, testen en auditen. De zaadveredelingsorganisaties passen deze toe, maar veelal wordt hierbij een beperkte scope gehanteerd. Hierbij kan worden gedacht aan risicoanalyses die incidenteel worden uitgevoerd, bijvoorbeeld alleen voor nieuwe systemen, waarin niet alle relevante risico's worden meegewogen, of aan monitoren, testen en auditen die zich niet richten op de gehele organisatie en veelal incidenteel en niet periodiek worden uitgevoerd.

De *technisch toeleveranciers* vormen een meer gemêleerde groep als het gaat om de getroffen maatregelen. Het niveau varieert hierbij van weinig naar heel veel. Zo zijn er technisch toeleveranciers die zich nauwelijks bezig houden met een gestandaardiseerd basisniveau voor digitale veiligheid terwijl andere hier juist structureel mee werken en een managementsysteem voor digitale veiligheid hebben. Hetzelfde beeld is van toepassing op het gebruik van monitoren, testen en auditen. Een deel van de organisaties pakt dit gedegen en periodiek op, terwijl anderen hier minder structureel en volledig mee bezig zijn. Alle technisch toeleveranciers houden zich bezig met risicoanalyses, maar veelal hebben deze een beperkte scope, worden incidenteel uitgevoerd, bijvoorbeeld alleen voor nieuwe systemen, en niet alle relevante risico's worden meegewogen. In tegenstelling tot de andere organisaties in het glastuinbouwcluster maken technisch toeleveranciers nauwelijks gebruik van OT-systemen voor hun eigen bedrijfsvoering, waardoor zij ook geen maatregelen op dit vlak hebben getroffen.

3.4.2 Analyse & oplossingsrichtingen

Het onderzoek laat zien dat er voor alle typen organisaties in het glastuinbouwcluster een opgave ligt om het digitaal veiligheidsniveau te laten aansluiten bij het risicoprofiel van de eigen organisatie. Op de volgende thema's zien we ruimte voor verbetering:

1 De urgentie van de digitale veiligheid wordt nog onvoldoende gevoeld

Het gevoel van urgentie van digitale veiligheid van de IT- en OT-systemen is onvoldoende. Met name bij de kleinere productieorganisaties heeft de directie vaak geen aandacht voor de digitale veiligheid. Bij de andere organisaties is dat doorgaans wel het geval, maar zien we dat het urgentiegevoel niet in de pas loopt met het risicoprofiel van de organisatie.

Bij alle typen organisaties in het glastuinbouwcluster moet dan ook gewerkt worden aan het verhogen van het risicobewustzijn, enerzijds door opleiding en training en anderzijds door mensen uit de sector elkaar te laten beïnvloeden.

Daarnaast zou het onderwerp digitale veiligheid meer aandacht moeten krijgen op (tuinbouw)opleidingen, zodat de toekomstige werknemers in de glastuinbouw al tijdens hun opleiding met het onderwerp digitale veiligheid in aanraking komen en er meer gevoel voor krijgen.

2 Er is meer expertise nodig op het gebied van de digitale veiligheid

Met name bij kleinere productieorganisaties komt het vaak voor dat zij niemand hebben (in dienst of ingehuurd) die zich bezighoudt met de digitale veiligheid. Voor de meeste andere organisaties geldt dat ze weliswaar één of meer mensen voor de digitale veiligheid hebben, maar te weinig om voldoende invulling te kunnen geven aan de benodigde digitale veiligheid.

Sommige organisaties hebben moeite met het vinden van specialisten met voldoende kennis en ervaring op het gebied van digitale veiligheid. Het zou helpen als het glastuinbouw-cluster meer bekendheid krijgt bij platforms voor digitale veiligheidsspecialisten en opleidingen op het gebied van digitale veiligheid, zodat werving makkelijker wordt. Het beschikbaar stellen van afstudeerplaatsen en traineeplaatsen kan een eerste stap in die richting zijn.

3 De elementaire digitale veiligheidsmaatregelen niet op orde bij productieorganisaties

Het merendeel van de productieorganisaties heeft de elementaire digitale veiligheidsmaatregelen, zoals voorgesteld door het DTC, niet op orde. Met name voor veel kleine productie-organisaties speelt mee dat ze denken dat hun leveranciers de digitale veiligheid regelen. Deze organisaties moet duidelijk gemaakt worden dat leveranciers op dit gebied wel wat kunnen doen, maar dat er nog verscheidene digitale veiligheidstaken overblijven die de organisatie zelf moet regelen.

Voor veel productieorganisaties zijn de elementaire digitale veiligheidsmaatregelen lastig te realiseren. Deze organisaties hebben behoefte aan ondersteuning bij het realiseren van deze maatregelen en het maken van afspraken hierover met hun technisch toeleveranciers.

De meeste andere organisaties hebben hun elementaire digitale veiligheidsmaatregelen redelijk op orde. Deze organisaties kunnen wellicht een rol spelen bij het ondersteunen van de organisaties die er meer moeite mee hebben.

4 Baselines worden niet of met beperkte scope geïmplementeerd

Het implementeren van een gestandaardiseerd basisniveau of baseline voor digitale veiligheid is een stap verder dan het treffen van de elementaire digitale veiligheidsmaatregelen. De meeste productieorganisaties worstelen al met de elementaire maatregelen en een gestandaardiseerd basisniveau implementeren is dan helemaal een brug te ver. Toch bevat een gestandaardiseerd basisniveau voor digitale veiligheid slechts de beveiligingsmaatregelen die een organisatie minimaal zou moeten treffen voor een redelijke digitale veiligheid. Meer dan 90% van de productieorganisaties zit onder dit minimum.

Van de andere organisaties in het glastuinbouwcluster werkt een deel met een gestandaardiseerd basisniveau voor digitale veiligheid. Echter, deze is niet altijd volledig geïmplementeerd en omvat veelal niet alle kritische systemen van de organisatie.

Een complicatie is dat de beschikbare standaarden voor een basisniveau voor digitale veiligheid niet toegespitst zijn op organisaties in het glastuinbouwcluster. Dit geldt in het bijzonder voor de kleinere productieorganisaties. Er is dan ook behoefte aan één of meer gestandaardiseerde basisniveaus die toegespitst zijn de organisaties van het glastuinbouwcluster en zowel de IT als de OT meenemen.

5 Risicoanalyses, monitoren, testen en auditen vaak met beperkte scope geïmplementeerd

Risicoanalyses zijn nodig om voor alle kritische IT- en OT-systemen van een organisatie te bepalen hoeveel risico's deze systemen lopen en welke beveiligingsmaatregelen in aanvulling op het gestandaardiseerde basisniveau nodig zijn om de risico's tot aanvaardbare proporties terug te dringen. In aanvulling daarop kunnen monitoring, testen en auditen ingezet worden op te controleren dat er geen beveiligingsinbreuken komen en het gewenste niveau van digitale veiligheid gehandhaafd wordt.

Voor organisaties die nog worstelen met hun elementaire maatregelen of hun basisniveau voor digitale veiligheid, voegen risicoanalyses, monitoren, testen en auditen niet veel toe. Slechts twee productieorganisaties werken met volledige risicoanalyses. Een deel van de organisaties doet wel wat aan monitoren en/of testen, maar het is de vraag hoe nuttig dat is zonder een redelijk niveau van digitale veiligheid.

Van de overige organisaties in het glastuinbouwcluster werkt een deel met risicoanalyses, zij het niet altijd even volledig, alsmede met monitoring, testen en in een enkel geval audits. Echter, net als voor het gestandaardiseerd basisniveau, geldt hier dat deze maatregelen vaak een beperkte scope hebben. Met name de OT-systemen vallen ook bij deze organisaties veelal buiten de boot.

Goede en volledige risicoanalyses, alsmede effectieve monitoring, testen en audits zijn voor organisaties die grotere risico's lopen, zoals zaadveredelingsorganisaties, handelsorganisaties en technisch toeleveranciers, noodzakelijk om een voldoende digitaal beveiligingsniveau te handhaven. Het kan deze organisaties gemakkelijker gemaakt worden door samen te werken, informatie over dreigingen en kwetsbaarheden uit te wisselen en ondersteunende hulpmiddelen te krijgen, zoals specifieke baselines, risicoanalysegereedschap, auditprotocollen, etc.

3.5 Behoefte aan hulpmiddelen en ondersteuning

Veel organisaties hebben aangegeven dat ze behoefte hebben aan hulpmiddelen en ondersteuning. Om in die behoefte te voorzien is samenwerking nodig tussen de organisaties binnen het glastuinbouwcluster en met partijen daarbuiten. Het cyberweerbaarheidscentrum i.o. kan hierin een belangrijke rol vervullen als sectoraal coördinatiecentrum, als kenniscentrum en als facilitator voor het ontwikkelen van hulpmiddelen en het bieden van ondersteuning op het gebied van digitale veiligheid.

3.5.1 Bevindingen

In de interviews met externe cybersecurity-deskundigen is besproken welke hulpmiddelen en ondersteuning voor het verbeteren van de digitale veiligheid nuttig zouden kunnen zijn. In de interviews met de representanten vanuit het glastuinbouwcluster en in de enquête konden de mensen uit het tuinbouwcluster aangegeven aan welke van deze hulpmiddelen en ondersteuning men behoefte dacht te hebben. Het bleek dat er bij alle typen organisaties behoefte bestond aan verschillende hulpmiddelen en ondersteuning. Dit bleek vooral op de volgende terreinen te liggen:

- Het verbeteren van het risicobewustzijn op het gebied van de digitale veiligheid in het glastuinbouwcluster.
- Het vergroten van de expertise op het gebied van digitale veiligheid in het glastuinbouwcluster.
- Het ondersteunen bij het implementeren van maatregelen ten behoeve van de digitale veiligheid van de IT- en OT-systemen.
- Het bevorderen van de samenwerking en het onderling delen van informatie over digitale veiligheid in het glastuinbouwcluster.

In de interviews hebben enkele externe deskundigen en een aantal vertegenwoordigers van organisaties in het glastuinbouwcluster voorgesteld om een centraal cyberweerbaarheidscentrum in te richten om informatie over digitale veiligheid te verzamelen en te distribueren en organisaties in het glastuinbouwcluster te ondersteunen op het gebied van digitale veiligheid. Veel van de andere organisaties ondersteunden dat idee.

3.5.2 Analyse & oplossingsrichtingen

Er zijn grote verschillen tussen de organisaties in het glastuinbouwcluster. De gemeenschappelijke factor is dat de urgentie van de digitale veiligheid nog niet goed tot de organisatie doorgedrongen is, of dat de organisatie in meerdere of mindere mate met dit onderwerp worstelt.

In het geval van gebrek aan urgentiegevoel moet er iets aan risicobewustwording gedaan worden. In vrijwel alle gevallen stoelt het gebrek aan urgentiegevoel op onvoldoende kennis en/of onderschatting van de feitelijke risico's. Dit kan het beste aangepakt worden door informatieverstrekking vanuit peer-organisaties, in samenwerking met een centrale partij.

In het geval van worstelen met het onderwerp digitale veiligheid is er een centrale partij nodig. Deze kan fungeren als kennis- en coördinatiecentrum voor digitale veiligheid binnen het glastuinbouwcluster en bovendien samenwerking op dit gebied faciliteren tussen organisaties binnen het cluster en met organisaties daarbuiten.

Al met al is behoefte aan een centrale partij. Deze partij kan dan invulling geven aan de hierboven genoemde terreinen:

- Het verbeteren van het risicobewustzijn op het gebied van de digitale veiligheid in het glastuinbouwcluster.
- Het vergroten van de expertise op het gebied van digitale veiligheid in het glastuinbouwcluster.
- Het ondersteunen bij het implementeren van maatregelen ten behoeve van de digitale veiligheid van de IT- en OT-systemen.
- Het bevorderen van samenwerking en het onderling delen van informatie over digitale veiligheid in het glastuinbouwcluster.

De benodigde centrale partij is inmiddels in oprichting onder de naam Cyberweerbaarheidscentrum GWH (CWC). Het CWC wordt aangestuurd door Security Delta (HSD), gefaciliteerd door Greenport West-Holland (GWH) en heeft een startsubsidie gekregen van het Digital Trust Center (DTC).
Alle hierboven genoemde punten kunnen in principe door het CWC opgepakt gaan worden.


January
February
March
April
May
17%
86%
40%
59%
Current Rates & Spreads
:34
:45
:56
13690
86195
86134
51697
86143
89563
40963
Current Rates & Spreads
DOLLAR
EURO
FOREX
Current Rates & Spreads
Purchase
Selling
Time
USD
EUR
Bitcoin
Current Rates & Spreads
Purchase
Selling
Time
EUR/USD
GBP/USD
USD/CHF
Current Rates & Spreads
Support
Resistance
EUR/USD
GBP/USD
USD/JPY
USD/CHF
Current Rates & Spreads
INDEX COMPONENTS
EURRUB=X
RUB=X
GPBRUB=X
RTS.RS
GLZ14.NYM
AAPL
GOOG
MSFT
DOW J
E
MARKETS CLOSED
35812
08317
08356
73819
08365
01785
62185

4 Aanbevelingen

In dit hoofdstuk zijn de belangrijkste bevindingen van het onderzoek die zijn beschreven in het voorgaande hoofdstuk vertaald naar aanbevelingen voor het CWC Greenport WH om daarmee de digitale veiligheid van het glastuinbouwcluster te verbeteren. De aanbevelingen zijn verdeeld in vier thema's, te weten:

1. Risicobewustzijn bij directie en personeel ten aanzien van IT en OT verbeteren.
2. Expertise op het gebied van digitale veiligheid vergroten.
3. Ondersteuning voor digitale veiligheid inrichten.
4. Samenwerking op het gebied van digitale veiligheid versterken.

In de volgende paragrafen worden de thema's kort toegelicht en uitgewerkt.

Om de thema's te kunnen implementeren is het nuttig om groepen organisaties in kaart te brengen die te maken hebben met vergelijkbare problematiek op het gebied van digitale veiligheid en waartussen zodanig vertrouwen mogelijk is dat er overlegd en samengewerkt kan worden op het gebied van digitale veiligheid.

De groepen maken het mogelijk om onderling relevante informatie uit te wisselen en gerichter naar ondersteuning te zoeken. Voor organisaties die op het gebied van digitale veiligheid erg van elkaar verschillen is samenwerking op dat gebied niet nuttig. Zo is het weinig zinvol om een organisatie die de eerste stappen op het gebied van digitale veiligheid maakt op dat gebied te laten samenwerken met een organisatie die een gevorderd managementsysteem voor digitale veiligheid wil opzetten. Beide organisaties worstelen met volstrekt andere vraagstukken. Ook is het weinig zinvol om organisaties op het gebied van digitale veiligheid te laten samenwerken als er geen vertrouwensband is en ze weigeren elkaar relevante informatie toe te spelen.

Tevens is het van belang dat digitale veiligheid wordt benaderd als een aspect waarop de organisaties in de glastuinbouw elkaar niet gaan beconcurreren. Anders zouden concurrentieoverwegingen organisaties ervan kunnen weerhouden om elkaar relevante informatie op het gebied van digitale veiligheid te geven.

De groepsindeling hoeft niet per se de lijnen van de grootte of de typen organisaties te volgen. Zo kan bijvoorbeeld een grote productieorganisatie qua behoeften op het gebied van digitale veiligheid beter passen bij een zaadveredelingsorganisatie dan bij andere productieorganisaties, omdat die bijvoorbeeld minder ver gevorderd zijn op het gebied van digitale veiligheid. Een indeling van groepen naar aanleiding van vergelijkbare digitale veiligheidsvraagstukken en -risico's ligt daarmee meer voor de hand.

4.1 Risicobewustzijn verbeteren

De bevindingen van het onderzoek die zijn beschreven in hoofdstuk 3 schetsen het beeld dat het risicobewustzijn bij alle typen organisaties in het glastuinbouwcluster voor verbetering vatbaar is. Bij veel organisaties, met name productieorganisaties, ontbreekt bij directie en management het besef over de voor hun relevante risico's op het gebied van digitale veiligheid. De inrichting van digitale veiligheid staat nog in de kinderschoenen, of er is zelfs nog nauwelijks of niets aan gedaan. In een aantal van deze organisaties leeft de overtuiging dat het niet zo'n vaart zal lopen met dreigingen voor de digitalisering, of heerst de misvatting dat andere partijen de eventuele problemen wel zullen oplossen. Bij andere organisaties, met name organisaties die grote risico's lopen, zijn directie en management zich veelal bewust van de belangrijkste dreigingen voor de digitalisering en de impact die dat kan hebben. Toch ontbreekt het nog vaak aan goede risico-inschattingen, hetgeen leidt tot onderschatting van de risico's en te lage prioriteit van digitale veiligheid.

Het doel van dit thema is om het risicobewustzijn van directie en personeel ten aanzien van digitale veiligheid te verbeteren. In de onderstaande tabel worden activiteiten voorgesteld om organisaties in het glastuinbouwcluster hierin te ondersteunen.

Actoren die hierbij een rol spelen zijn: het CWC Greenport WH (CWC), technisch toeleveranciers (TT), brancheverenigingen, groepsambassadeurs (GA), de Haagse Hogeschool (HHS), overige kennis- en onderwijsinstellingen (K&O).

Nr.	Aanbeveling	Omschrijving
1.1*	Zoek groepsambassadeurs die het belang van digitale veiligheid uitdragen	Mensen kunnen vooral goed door 'gelijken' worden overtuigd om zaken anders te zien of anders aan te pakken. Mensen uit directie en management kunnen dus vooral goed worden overtuigd door andere directieleden en managers. Het is zaak om directieleden en managers uit organisaties binnen het glastuinbouwcluster te zoeken die zelf al helemaal overtuigd zijn van de noodzaak van digitale veiligheid en anderen hiervan graag willen overtuigen. Dergelijke mensen zijn dan 'groepsambassadeurs' die binnen hun groep het gesprek over digitale veiligheid stimuleren en de groep kunnen wijzen op de noodzaak van actieve inzet voor digitale veiligheid en op geschikte hulpmiddelen hiervoor. Dit kan zowel op bijeenkomsten die hierover worden georganiseerd als in bilaterale contacten. Omdat groepsambassadeurs ook groepsvorming stimuleren, is het van belang deze activiteit in de beginfase op te pakken.
1.2*	Organiseer aanbod van risicobewustzijnsworkshops en -opleidingen	Door middel van workshops (1 dagdeel) en opleidingen (2 dagen) risicomanagement voor managers en digitaal veiligheidsspecialisten in het glastuinbouwcluster. Het aanbod heeft tot doel om het risicobewustzijn te vergroten en kan worden toegespitst op groepen met vergelijkbare vraagstukken op het gebied van digitale veiligheid. Voor organisaties in een beginfase kan in een workshop worden ingegaan op het belang van de betrokkenheid van directie en management. Een opleiding voor digitale veiligheidsspecialisten van meer gevorderde organisaties kan zich richten op het verbeteren van kennis over geavanceerde dreigingen en nieuwe digitale aanvalsmethoden.
1.3*	Ontwikkel demonstrators om dreigingen, kwetsbaarheden en de impact ervan inzichtelijk te maken.	In aanvulling op de activiteiten van groepsambassadeurs en de risicobewustzijnsworkshops en -opleidingen kunnen demo's worden ontwikkeld waarin met gebruik van scenario's van digitale dreigingen de impact van incidenten voor de bedrijfsvoering kan worden gevisualiseerd. Hierbij kan worden gedacht aan scenario's met betrekking tot het optreden van een storing, een fout in gebruik of beheer, een ransomware-aanval, een supply chain-aanval, of een voorval van bedrijfsspionage in de digitale systemen. Het gebruik van dergelijke demo's om dreigingen en impact op een laagdrempelige wijze inzichtelijk te maken, is vooral geschikt om in een vroeg stadium te gebruiken om het gevoel van urgentie bij directie en management te verhogen.
1.4**	Organiseer seminars of bijeenkomsten waar technisch toeleveranciers uitleg kunnen geven over digitale veiligheid in relatie tot hun systemen	Digitale veiligheid vormt nog beperkt een onderwerp van gesprek tussen technisch toeleveranciers en gebruikers van hun systemen. Omdat er sprake is van een wederzijdse afhankelijkheid op het gebied van digitale veiligheid is het van belang dat partijen meer met elkaar in gesprek gaan over wat zij op dit gebied van elkaar verwachten. Een terugkerend overleg met technisch toeleveranciers en gebruikers kan hieraan bijdragen.

* Activiteiten die in de periode 2022-2023 zouden moeten worden gerealiseerd vanwege hoge urgentie of relatief eenvoudig karakter

** Activiteiten die in de periode 2024 tot 2026 kunnen worden opgepakt

4.2 Expertise vergroten

De bevindingen van het onderzoek schetsen het beeld dat in de organisaties niet altijd voldoende gespecialiseerde mensen beschikbaar zijn voor de digitale veiligheid. Het glastuinbouwcluster staat niet op het vizier van digitale veiligheidsopleidingen in de regio. Het aanbod van digitale veiligheidsspecialisten is in het algemeen al klein, laat staan voor specifiek het glastuinbouwcluster. Het is dan ook nodig om de wervingskracht van het glastuinbouwcluster voor deskundigen op het gebied van digitale veiligheid te versterken. Dat betekent dat meer mensen bereikt moeten worden, te beginnen met studenten, om vervolgens meer van deze mensen naar het cluster te trekken en ten slotte de kennis van deze mensen op peil te houden.

Het doel van dit werkpakket is er voor te zorgen dat de organisaties in het glastuinbouwcluster kunnen beschikken over meer mensen met de juiste expertise om digitale veiligheidsvraagstukken op te kunnen pakken.

Hierbij moet worden gedacht aan:

- De instroom van voldoende professionals op het gebied van digitale veiligheid in het glastuinbouwcluster (instroom vergroten).
- Digitale veiligheidsprofessionals waarvan de expertise voldoende aansluit op de praktijk (cybersecurity-opleidingen beter aan laten sluiten op de glastuinbouw).
- Tuinbouw-professionals met voldoende kennis van het onderwerp digitale veiligheid (tuinbouwopleidingen verbeteren).
- Bijscholingsmogelijkheden op het gebied van digitale veiligheid voor mensen die al werkzaam zijn in het glastuinbouwcluster (ondernemers, CS'ers, tuinbouwers, etc.).

In de onderstaande tabel worden activiteiten voorgesteld om organisaties in het glastuinbouwcluster hierin te ondersteunen.

Actoren die hierbij een rol spelen zijn:
Productieorganisaties (PO), handelsorganisaties (HO), zaadverdelingsorganisaties (ZO) en technisch toeleveranciers (TT), het CWC Greenport WH (CWC), Security Delta (HSD), Groepsambassadeurs (GA), de Haagse Hogeschool (HHS), overige kennis- en onderwijsinstellingen (K&O).

Nr.	Aanbeveling	Omschrijving
2.1**	Regel gastlessen door cybersecurity-professionals uit het glastuinbouw-cluster op de cybersecurity-opleidingen in de regio	Gastlessen bij cybersecurity-opleidingen in de regio door professionals uit het glastuinbouw-cluster kunnen helpen om de sector op het netvlies van opleidingen en studenten te krijgen. Dat bevordert de instroom van afgestudeerden op cybersecurity-gebied in het glastuinbouwcluster.
2.2*	Maak afspraken met cybersecurity opleidingen in de regio over de inzet van stagiairs en afstudeerders in het glastuinbouwcluster	Door overleg tussen het CWC en onderwijsinstellingen in de regio kan het aanbod van stage- en afstudeerplaatsen met de onderwijsinstellingen worden afgestemd. Hierdoor kan meer kennis over de digitale veiligheid in het glastuinbouwcluster worden ontwikkeld en kan wellicht een deel van de stagairs en afstudeerders voor de sector worden behouden.
2.3**	Inventariseer kennislacunes van afgestudeerden op het gebied van digitale veiligheid	Binnen het glastuinbouwcluster kan door het CWC worden geïnventariseerd in hoeverre afgestudeerden op het gebied van digitale veiligheid voldoende zijn toegerust voor het oppakken van vraagstukken op dit gebied in het glastuinbouwcluster en waar ruimte voor verbetering bestaat. Mogelijk kunnen ook brancheorganisaties van de glastuinbouw en technisch toeleveranciers hierover meedenken. De bevindingen kunnen dan naar de cybersecurity-opleidingen in de regio worden teruggekoppeld. In overleg is het dan wellicht mogelijk andere accenten in de opleidingen aan te brengen.
2.4*	Inventariseer minimale kennis op het gebied van digitale veiligheid voor glastuinbouw-professionals	CWC kan binnen het glastuinbouwcluster inventariseren over welke kennis en vaardigheden op het gebied van digitale veiligheid iedere glastuinbouw-professional zou moeten beschikken. CWC kan deze inzichten terugkoppelen naar de tuinbouwopleidingen in de regio, zodat deze opleidingen beter afgestemd kunnen worden op de behoefte van de praktijk waardoor toekomstige medewerkers in het cluster beter beslagen ten ijs komen.
2.5*	Organiseer kennissessies en bijscholing op het gebied van digitale veiligheid	Door middel van groepsgewijze kennissessies (1 dagdeel) gericht op directie/management en bijscholing (2 dagen) gericht op digitale veiligheidsspecialisten kan het kennisniveau op het gebied van digitale veiligheid van mensen die werkzaam zijn in het glastuinbouwcluster worden verhoogd. Tevens kunnen kennissessies en bijscholing ook bijdragen aan het risicobewustzijn van organisaties (zie ook WP-1, activiteit 1.3).

* Activiteiten die in de periode 2022-2023 zouden moeten worden gerealiseerd vanwege hoge urgentie of relatief eenvoudig karakter

** Activiteiten die in de periode 2024 tot 2026 kunnen worden opgepakt

4.3 Ondersteuning inrichten

Uit de bevindingen van het onderzoek blijkt dat voor alle typen organisaties geldt dat zij moeten investeren in digitale veiligheid om het gewenste digitale veiligheidsniveau te halen. Door het organiseren van ondersteuning kunnen organisaties hierbij worden gefaciliteerd. Enerzijds kan het aanbod van kennissessies en opleidingen, zoals beschreven in thema 2, hieraan bijdragen. Anderzijds kunnen organisaties ook worden gefaciliteerd door het beschikbaar maken van actuele kennis van dreigingen, kwetsbaarheden en incidenten (vanuit NCSC en door kennisdeling in groepen) en door het ontwikkelen en aanbieden van een palet aan instrumenten die organisaties kunnen gebruiken om hun digitale veiligheid in kaart te brengen en om de benodigde maatregelen te selecteren, te implementeren, te testen en te monitoren. Omdat de organisaties in het glastuinbouwcluster op het gebied van digitale veiligheid erg van elkaar verschillen kunnen de te ontwikkelen instrumenten het beste volgens een cafetariamodel ingezet worden voor de organisaties die daar behoefte aan hebben.

Het doel van dit werkpakket is om instrumenten te ontwikkelen die organisaties in het glastuinbouwcluster kunnen toepassen om hun digitale veiligheid te meten en te verbeteren.

Actoren die hierbij een rol spelen zijn: het CWC Greenport WH (CWC), de Haagse Hogeschool (HHS), overige kennis- en onderwijsinstellingen (K&O).

Nr.	Aanbeveling	Omschrijving
3.1*	Organiseer workshops gericht op het op orde brengen van de elementaire digitale veiligheidsmaatregelen	Organisaties kunnen worden ondersteund door het aanbieden van een workshop voor het op orde brengen van elementaire digitale beveiligingsmaatregelen. Workshops kunnen hierbij worden toegespitst op verschillende doelgroepen. Voor organisaties die zich in een beginfase bevinden kan een workshop voor managers zich o.a. richten op een stappenplan voor het implementeren van de vijf elementaire maatregelen voor digitale veiligheid van DTC. Voor meer gevorderde organisaties kan een workshop worden aangeboden voor digitaal veiligheidsspecialisten en CISO's, gericht op vraagstukken als planning en afspraken in de organisatie, hoe te communiceren met het management over digitale veiligheid en hoe samen te werken met relevante derde partijen.
3.2*	Organiseer workshops gericht op de relatie met de technisch toeleveranciers	Organisaties kunnen worden ondersteund door het aanbieden van een workshop gericht op de relatie tussen klant en de technisch toeleveranciers. In deze workshops kan worden ingegaan op het maken van contractuele afspraken met leveranciers over digitale veiligheid, over aanbesteding, SLA's, inrichting van onderhoud en dienstverlening door derden en contractbeheer.
3.3*	Organiseer centrale communicatie over actuele dreigingsinformatie	In het glastuinbouwcluster zijn organisaties beperkt op de hoogte van actuele dreigingen, kwetsbaarheden en incidenten op het gebied van digitale veiligheid. Centrale communicatie over actuele dreigingen, kwetsbaarheden en incidenten, onder meer o.b.v. NCSC-dreigingsinformatie, maken het mogelijk om tijdig in de digitale omgeving in te grijpen en nieuwe incidenten te voorkomen. Het CWC kan hiervoor bij het NCSC een OKTT-status aanvragen die het ontvangen en verder distribueren van NCSC-dreigingsinformatie mogelijk maakt.
3.4*	Houd een centraal incidentenregister bij voor het glastuinbouwcluster	Het bijhouden van een centraal register voor digitale veiligheidsincidenten maar de problematiek voor de sector inzichtelijk en kan ook dienen als een collectief geheugen voor de sector. Ook maakt het inzichtelijk welke organisaties in de sector ervaringsdeskundig zijn op dit gebied en met wie contact kan worden opgenomen om te leren van hun ervaringen.
3.5*	Ontwikkel model baselines voor digitale veiligheid van IT- en OT-systemen in het glastuinbouwcluster	Een groot deel van de organisaties in het glastuinbouwcluster maakt geen gebruik van een baseline voor digitale veiligheid van de organisatie of heeft deze niet volledig geïmplementeerd. Een drempel voor het beter toepassen van een baseline is dat bestaande informatiebeveiligingsbaselines vaak onvoldoende toegespitst zijn op de organisaties en de systemen in het glastuinbouwcluster. Een baseline die recent is ontwikkeld door het CWC Agrifood kan hiervoor mogelijk als uitgangspunt dienen. Vertegenwoordigers van de verschillende groepen uit het cluster kunnen worden gevraagd om hieraan mee te werken.

Nr.	Aanbeveling	Omschrijving
3.6**	Ontwikkel een methode voor risicoanalyse die aansluit bij organisaties in het glastuinbouwcluster en hun IT- en OT-systemen	Een deel van de organisaties in het glastuinbouwcluster maakt geen of niet goed gebruik van risicoanalyse voor hun IT- en OT-systemen. Verschillende organisaties geven aan nog geen methode voor risicoanalyse te hebben gevonden die afdoende aansluit bij de OT-systemen. De Haagse Hogeschool heeft eerder voor de waterschappen een risicoanalysetool ontwikkeld. Deze zou als uitgangspunt kunnen dienen voor de te ontwikkelen tool. Vertegenwoordigers van de verschillende groepen uit het cluster kunnen worden gevraagd om de tool mee te helpen uitwerken en uitproberen.
3.7*	Organiseer een aanbod van testen om kwetsbaarheden in de digitale veiligheid van organisaties inzichtelijk te maken	Testen is een effectieve manier om zicht te krijgen op kwetsbaarheden in de digitale veiligheid. CWC kan afspraken maken met aanbieders van testen voor een aanbod dat is toegespitst op het glastuinbouwcluster. Hierbij kan worden gedacht aan penetratietesten om kwetsbaarheden in de toegang tot digitale systemen in kaart te brengen en social engineering-testen om kwetsbaarheden in de fysieke toegang in kaart te brengen.
3.8*	Stimuleer het gebruik van monitoren ten behoeve van de digitale veiligheid van de organisatie	Wijs de leden van GWH op het belang van het monitoren van de digitale systemen om verdacht verkeer op de netwerken tijdig te detecteren. CWC kan afspraken maken met aanbieders van monitoring hulpmiddelen en monitoring dienstverleners.
3.9**	Stimuleer het gebruik van audits ten behoeve van de digitale veiligheid van de organisatie	Wijs de leden van GWH op het belang van audits om de compliance met de procedures en werkinstructies in kaart te brengen. CWC kan afspraken maken met aanbieders van audits voor een aanbod dat is toegespitst op het glastuinbouwcluster.
3.10**	Ondersteun de inrichting van een managementsysteem voor de digitale veiligheid van de organisatie	Biedt een cursus aan waarin organisaties praktische handvatten wordt geboden voor het inrichten van een managementsysteem voor de digitale veiligheid van de organisatie.
3.11*	Ontwikkel een cyberscan voor het met meten van het digitaal veiligheidsniveau van de organisatie	Door het beschikbaar stellen van een cyberscan in de vorm van een zelfrapportagetool kunnen organisaties in het glastuinbouwcluster op een laagdrempelige wijze een indicatie krijgen van hun digitaal veiligheidsniveau. Hiernaast kan dit bijdragen aan het overzicht van de digitale veiligheidsopgave voor de sector als geheel. De enquête die op basis van het 3-pijlermodel voor volwassenheid van informatiebeveiliging en de informatiebeveiligingsstandaard ISO 27001 is ontwikkeld en ingezet voor het huidige onderzoek kan een uitgangspunt vormen voor een Cyberscan. De gegevens in de Cyberscan kunnen worden aangeleverd door managers of digitaal veiligheidsspecialisten van de organisatie.
3.12**	Ontwikkel een cyberschouw als opvolging van de cyberscan	Door het beschikbaar stellen van een cyberschouw kan het digitaal veiligheidsniveau van de organisatie nader worden geduid. Met een op 3-pijler model gebaseerde aanpak kan het digitaal veiligheidsniveau in kaart worden gebracht door het uitvoeren van verscheidene interviews per organisatie. Afhankelijk van de specialisatie en omvang van de organisatie kan hiervoor onder meer worden gesproken met de directie, CISO, stafmedewerker, middle management, en mensen op de werkvloer. Anders dan bij een audit wordt bij een cyberschouw niet aan de organisatie gevraagd om het digitaal veiligheidsniveau te onderbouwen met documentatie.

* Activiteiten die in de periode 2022-2023 zouden moeten worden gerealiseerd vanwege hoge urgentie of relatief eenvoudig karakter

** Activiteiten die in de periode 2024 tot 2026 kunnen worden opgepakt

4.4 Samenwerking versterken

De bevindingen van het onderzoek wijzen erop dat meer samenwerking tussen de organisaties in het glastuinbouwcluster onderling en met relevante organisaties buiten het cluster kan bijdragen aan het verbeteren van de digitale veiligheid van de sector. Zo bleek bijvoorbeeld dat organisaties in de sector nog weinig informatie met elkaar delen over digitale veiligheidsincidenten die hebben plaatsgevonden waardoor dreigingen en kwetsbaarheden over het hoofd kunnen worden gezien en risico's kunnen worden onderschat. Er is behoefte bij de organisaties aan een centraal aanspreekpunt waar organisaties uit het glastuinbouwcluster zich toe kunnen wenden voor informatie over digitale veiligheid, voor het melden van incidenten op het gebied van digitale veiligheid, voor het zoeken naar ondersteuning na een dergelijk incident en van waaruit samenwerking op het gebied van digitale veiligheid kan worden gestimuleerd. Hiervoor kan contact worden gelegd met bestaande horizontale overlegstructuren in de sector en kunnen groepen van gelijkgestemde organisaties uit het glastuinbouwcluster worden betrokken bij de aanpak van vraagstukken op het gebied van digitale veiligheid. Ook kan worden gekeken naar mogelijkheden voor samenwerking met gremia of samenwerkingsverbanden op het gebied van digitale veiligheid in aanpalende sectoren.

Parallel aan dit onderzoek zijn stappen gezet om een cyberweerbaarheidscentrum (CWC) voor de sector in te richten. De verwachting is dat dit CWC een coördinerende en faciliterende rol kan gaan spelen bij het vormgeven van samenwerking op het gebied van de digitale veiligheid.

Het doel van dit werkpakket is om samenwerking op het gebied van digitale veiligheid tussen organisaties in het glastuinbouwcluster en met relevante organisaties buiten het cluster te versterken. Het coördineren en faciliteren van samenwerking op het gebied van digitale veiligheid in het glastuinbouwcluster is primair een rol voor het CWC.

Nr.	Aanbeveling	Omschrijving
4.1*	Inrichten van een gefaseerde aansluitstrategie voor organisaties in het glastuinbouwcluster	Om duidelijkheid te creëren over het mandaat waarmee het CWC opereert en om voldoende voeling te houden met de vraagstukken en ondersteuningsbehoefte op het gebied van digitale veiligheid is van belang dat organisaties in het glastuinbouwcluster zich gefaseerd aansluiten bij het CWC. De verwachting hierbij is dat eerst voorlopers uit de sector zich zullen als organisatie zullen aansluiten bij het CWC. In een later stadium kunnen organisaties die niet als zelfstandige organisatie willen aansluiten mogelijk worden vertegenwoordigd door coöperaties of brancheverenigingen. Het is van belang om organisaties in het glastuinbouwcluster vroegtijdig de mogelijk te geven om zich bij het CWC aan te sluiten en hierin te participeren.
4.2**	Stimuleer en faciliteer de vorming van 'horizontale' overleggroepen op het gebied van digitale veiligheid	In het glastuinbouwcluster zijn organisaties beperkt op de hoogte van incidenten die in de sector plaatsvinden. Meer afstemming tussen organisaties hierover draagt bij aan het bewustzijn van digitale veiligheidsrisico's. Er kan worden geïnventariseerd welke organisaties groepsgewijs willen deelnemen aan overleggen waar incidenten vanuit de eigen organisaties, vanuit het glastuinbouwcluster en vanuit andere sectoren kunnen worden besproken, alsmede de merites van mogelijke aanpakken. Leveranciers of brancheorganisaties kunnen mogelijk bijdragen door het delen van al dan niet geanonimiseerde cases.
4.3*	Maak verbinding tussen het CWC en bestaande overlegstructuren in het glastuinbouwcluster	Om voeling te houden met de vragen op het gebied van digitale veiligheid die leven bij de verschillende typen organisaties in het glastuinbouwcluster en om draagvlak te creëren om deze vraagstukken vanuit het CWC op te pakken is van belang om het CWC te verbinden met bestaande overleggremia in de sector. Een eerste stap hierin kan zijn het aanstellen van een regisseur voor elk van de gremia. De regisseurs kunnen informatie ophalen bij hun achterban en hen wijzen op bijeenkomsten of ontwikkelingen die vanuit het CWC worden georganiseerd.
4.4*	Organiseer overleg over digitale veiligheid binnen de verschillende groepen in het glastuinbouwcluster	Binnen de groepen van gelijkgestemde organisaties in het glastuinbouwcluster kunnen overleggen over digitale veiligheid worden ingericht. De representanten van de groepen kunnen optreden als aanjagers. De overleggen kunnen zich richten op meerdere niveaus, zoals een overleg tussen ondernemers of tussen digitale veiligheidsspecialisten van de organisaties. Sommige groepen hebben wellicht al een geschikt overleg. In dat geval is verbinding maken met het bestaande overleg belangrijk. De groepsoverleggen vormen een belangrijke stap om het gesprek over digitale veiligheid in het glastuinbouwcluster vroegtijdig op gang te brengen.
4.5*	Verbind het CWC met bestaande CWC's in aanpalende sectoren	Bij het opstarten van het CWC voor het glastuinbouwcluster en de uitvoering van de werkpakketten kan contact worden gezocht met CWC in aanpalende sectoren. Een voorbeeld hiervan is het CWC Agrifood dat eerder is gestart en onlangs een cybersecurity baseline en assessment tool heeft ontwikkeld. Er kan relatief eenvoudig contact worden gelegd met enkele bekende CWC's in aanpalende sectoren.
4.6**	Richt een werkgroep in om te komen tot een plan van aanpak voor organisatieoverstijgende problematiek op het gebied van digitale veiligheid	De aanpak van organisatie-overstijgende problematiek op het gebied van digitale veiligheid vraagt om meer samenwerking tussen organisaties in het glastuinbouwcluster. Een werkgroep met o.a. groepsambassadeurs, representanten van de groepen en brancheverenigingen van de organisaties in het glastuinbouwcluster kan zich buigen over mogelijkheden voor een gezamenlijke aanpak van meer complexe organisatie-overstijgende vraagstukken zoals supply chain-aanvallen en bedrijfsspionage door statelijke actoren.

* Activiteiten die in de periode 2022-2023 zouden moeten worden gerealiseerd vanwege hoge urgentie of relatief eenvoudig karakter

** Activiteiten die in de periode 2024 tot 2026 kunnen worden opgepakt


CO
H_2O
O_2
Fe

Bijlage 1: Interviewprotocol

Bij een steekproef van organisaties uit West-Holland, afkomstig uit verschillende groepen uit de tuinbouwketen, wordt met behulp van interviews bepaald hoe deze organisaties omgaan met geautomatiseerde gegevensverwerking (ICT) en operationele technologie (OT), hoe de verantwoordelijkheden zijn belegd, welke dreigingen ze relevant vinden, welke risico's ze daardoor lopen, welke beveiligingsmaatregelen ze hebben getroffen, welke oplossingsrichtingen ze zien voor het aanpakken van de openstaande risico's en welke hulpmiddelen en ondersteuning ze voor het verbeteren van de digitale veiligheid nodig denken te hebben.

De selectie van te onderzoeken partijen is gebaseerd op de groepen van de tuinbouwketen. Uit de voor dit onderzoek meest relevante groepen wordt een steekproef genomen van twee partijen per groep. Hierbij is het uitgangspunt niet *compleetheid*, maar het verkrijgen van een *redelijke indicatie* hoe in iedere groep aangekeken wordt tegen en omgegaan wordt met digitale veiligheid, alsook de behoeften die er op dit gebied bestaan.

In de interviews wordt een indicatie gezocht hoe in de betreffende organisatie wordt aangekeken tegen en omgegaan met digitale veiligheid. Daarbij spelen de volgende onderzoeksvragen:

1. In hoeverre is de organisatie gedigitaliseerd en wat kunnen de gevolgen zijn als de digitalisering niet meer beschikbaar, integer of vertrouwelijk is?
2. Wat is het dreigingsbeeld ten aanzien van de digitale veiligheid van de organisatie en welke risico's levert dit op voor de organisatie?
3. Hoe (goed) is de informatiebeveiliging in de organisatie georganiseerd?
4. Welke externe hulpmiddelen en ondersteuning zijn op het gebied van digitale veiligheid nodig en welke partijen kunnen daar een rol in spelen?

Om voor de betreffende organisatie antwoord te krijgen op deze onderzoeksvragen wordt in een semigestructureerd interview ingegaan op de onderstaande vragen. Afhankelijkheid van te verwachtte deskundigheid van de te interviewen functionaris(sen) wordt van tevoren bepaald welke vragen voor dat interview relevant zijn.

Vragenlijst sector

Vraagstelling
0. Positionerende vragen vooraf:
1. Wat zijn de belangrijkste producten en/of diensten die uw organisatie levert?
2. Hoe belangrijk is uw organisatie voor de tuinbouwketen?
3. Van welke organisaties is uw organisatie vooral afhankelijk?
4. Welke rol heeft u in uw organisatie?
1. In hoeverre is de organisatie gedigitaliseerd en wat kunnen de gevolgen zijn als de digitalisering niet meer beschikbaar, integer of vertrouwelijk is?
1. In hoeverre is uw organisatie gedigitaliseerd? Betreft dit ICT en/of OT?
2. Wat zijn de belangrijkste systemen? Zijn deze intern of extern?
3. Van welke interne en externe digitale gegevens is uw organisatie afhankelijk?
4. Hoe belangrijk is het internet voor uw organisatie?
5. Welke consequenties kan het hebben als de digitalisering en/of het internet niet meer beschikbaar is?
6. Welke consequenties kan het hebben als digitale gegevens niet meer te vertrouwen zijn?
7. Welke consequenties kan het hebben als digitale gegevens uitlekken?
2. Wat is het dreigingsbeeld ten aanzien van de digitale veiligheid van de organisatie en welke risico's levert dit op voor de organisatie?
1. Is uw organisatie het afgelopen jaar getroffen door één of meer ernstige incidenten op het gebied van digitale veiligheid?
2. Welke dreigingen voor de digitale veiligheid vindt u voor uw organisatie het meest belangrijk?
3. Wat zou bij manifestatie van deze dreigingen de impact voor uw organisatie kunnen zijn?
4. Past uw organisatie risicoanalyses toe om de belangrijkste dreigingen voor de digitale veiligheid te bepalen?
3. Hoe (goed) is de informatiebeveiliging in de organisatie georganiseerd?
1. In hoeverre en hoe is (het beheer van) de ICT en/of OT van uw organisatie uitbesteed? Aan wie? Betreft dit ook de digitale veiligheid?
2. Welke medewerkers van uw organisatie hebben een rol in de digitale veiligheid van uw organisatie?
3. Wie zijn binnen uw organisatie de voornaamste trekkers van digitale veiligheid in uw organisatie?
4. Vindt op het gebied van digitale veiligheid vanuit uw organisatie afstemming plaats met andere organisaties?
5. Hoe bewust zijn uw collega's zich van het belang van digitale veiligheid en handelen ze daar ook naar?
6. Maakt uw organisatie gebruik van een baseline voor informatiebeveiliging, bijvoorbeeld ISO 27002, en hoe ver is dat gevorderd?
7. Heeft uw organisatie een managementstandaard voor informatiebeveiliging ingevoerd, bijvoorbeeld ISO 27001, en hoe ver is dat gevorderd?
8. Worden de informatiebeveiligingsprocessen en -maatregelen regelmatig getoetst, bijvoorbeeld met audits, penetratietesten, of social engineering?
4. Welke externe hulpmiddelen en ondersteuning zijn op het gebied van digitale veiligheid nodig en welke partijen kunnen daar een rol in spelen?
1. Van welke externe organisaties verwacht u (meer) hulpmiddelen en ondersteuning op het gebied van digitale veiligheid?
2. Wat voor soort hulpmiddelen en ondersteuning zouden dat kunnen zijn?
3. In hoeverre heeft uw eigen organisatie deze hulpmiddelen en ondersteuning nodig?

Aanvullend worden externe deskundigen op het gebied van cybersecurity bevraagd over dezelfde materie.

Vragenlijst externe deskundigen

Vraagstelling
Hoe belangrijk denkt u dat ICT en OT voor organisaties in de tuinbouwsector zijn?
Welke dreigingen voor de digitale veiligheid vindt u voor een organisatie in de tuinbouwsector met name belangrijk?
Wie zou binnen een organisatie in de tuinbouwsector de trekker moeten zijn van digitale veiligheid?
Welke organisatorische rollen zou een organisatie in de tuinbouwsector op het gebied van digitale veiligheid moeten hebben?
In hoeverre kunnen deze rollen met elkaar en met andere rollen gecombineerd worden?
Welke standaarden op het gebied van digitale veiligheid (ICT en OT) zijn relevant voor een organisatie in de tuinbouwsector?
Welke baseline(s) voor digitale veiligheid (ICT en OT) zijn geschikt voor een organisatie in de tuinbouwsector?
Welke managementstandaard voor digitale veiligheid is geschikt voor een organisatie in de tuinbouwsector?
Wat moet een organisatie in de tuinbouwsector minimaal geregeld hebben op het gebied van digitale veiligheid?
Als een organisatie in de tuinbouwsector onder dit minimum zit, waarmee kan dan het beste worden begonnen?
Wat moet een dergelijke organisatie zeker niet doen?
Welke vorm(en) van toetsing vindt u belangrijk voor digitale veiligheid?
Wat voor hulpmiddelen en ondersteuning op het gebied van digitale veiligheid zijn er voor organisaties in de tuinbouwsector? Wie kan die leveren?
Welke gremia zou de tuinbouwsector moeten opzetten om de organisaties in de sector op het gebied van digitale veiligheid te ondersteunen?
Welke andere adviezen heeft u voor organisaties in de tuinbouwsector?

Bijlage 2: Enquête

1. *Voor welk type organisatie bent u werkzaam? [gesloten vraag]*
   - Teler
   - Telersvereniging/coöperatie
   - Vermeerderingsbedrijf
   - Veredelaar
   - Handelsbedrijf
   - Anders, namelijk:

2. *Wat is uw functie? [open vraag]*

3. *Wat is de omvang van uw organisatie? [drie maal getal]*
   - Hoeveel locaties telt uw organisatie?
   - Hoeveel medewerkers (vast en ingehuurd) telt uw organisatie?
   - Wat is het teeltareaal van uw organisatie?

4. *Wat is de maximale impact als één of meer **IT-systemen*** voor kantoor- en administratieve automatisering van uw organisatie niet beschikbaar zijn of verkeerd functioneren? *(Denk bijvoorbeeld aan pc's, laptops, IT-netwerk, administratieve systemen, cloud-systemen, e.d.) [open vraag]*

5. *Wat is de maximale impact als één of meer **OT-systemen*** voor productie- en logistieke automatisering van uw organisatie niet beschikbaar zijn of verkeerd functioneren? *(Denk bijvoorbeeld aan klimaatcomputer, digitale sensoren, automatische bewatering, drones, sorteermachines, verpakkingsmachines, e.d.) [open vraag]*

6. *In hoeverre maakt u zich zorgen over mogelijke incidenten door problemen met één of meer IT- of OT-systemen van uw organisatie? [gesloten vraag]*
   - Ik maak me daar grote zorgen over
   - Ik maak me daar enigszins zorgen over
   - Ik maak me daar weinig zorgen over
   - Ik maak me daar geen zorgen over

7. *Kunt u kort toelichten waarom u zich veel zorgen of juist weinig zorgen maakt over het optreden van problemen met de IT- of OT- systemen van uw organisatie? [open vraag]*

8. *Kunt u een indicatie geven van het aantal keer dat er in het afgelopen jaar in directie/MT-overleggen is gesproken over digitale veiligheid? [getal]*

9. *Hebt u de afgelopen twee jaren één of meer incidenten gehad door problemen met uw IT- of OT-systemen? (Denk bijvoorbeeld aan voorvallen waarbij de systemen niet beschikbaar waren, niet correct waren of gegevens hebben gelekt als gevolg van systeemcrash, systeem-storing, elektriciteitsuitval, menselijke fout in gebruik of beheer van de systemen, virus, een aanval van buitenaf, etc.) [gesloten vraag]*
   - Ja, één keer*
   - Ja, meerdere keren*
   - Nee, maar één of meer organisaties die ik ken wel*
   - Nee, en in mijn omgeving ook niet over gehoord

   a. [open vraag, tonen bij *] Kunt u kort toelichten om wat voor incident(en) het hier ging?

10. *In hoeverre maken uw IT-systemen (kantoor- en administratieve automatisering) en OT-systemen (productie- en logistieke automatisering) gebruik van het internet? [meerdere antwoorden mogelijk, gesloten vraag]*
    - Voor beheer op afstand
    - Voor IT-clouddienstverlening
    - Voor OT-clouddienstverlening
    - Voor gegevensuitwisseling met bekende partijen (bijvoorbeeld leveranciers, technisch toeleveranciers, afnemers, onderhoudspartijen, transporteurs, e.d.)
    - Voor het delen van gegevens voor data-analyse
    - Nee, noch de IT- noch de OT- systemen maken gebruik van het internet
    - Weet ik niet
    - Anders, namelijk:

11. *Hoe is het beheer van uw IT- en OT-systemen vormgegeven? [gesloten vraag]*
    - We beheren onze IT- en OT-systemen zelf
    - Het beheer is deels uitbesteed aan één of meer externe partijen*
    - Het beheer van de IT- en OT-systemen is volledig uitbesteed aan één of meer externe partijen*
    - Weet ik niet
    - Anders, namelijk:

    a. [open vraag, tonen bij *] Aan welke partij(en) is dit uitbesteed?

12. *Zijn er met de IT-leveranciers (kantoor- en administratieve automatisering) en/of met OT-leveranciers (*productie- en logistieke automatisering) *expliciet afspraken gemaakt over, of normen gesteld aan digitale veiligheid? [meerdere antwoorden mogelijk]*
- Ja, met IT-leverancier(s)*
- Ja, met OT-leverancier(s)*
- Nee, er zijn geen expliciete afspraken gemaakt over, of normen gesteld aan digitale veiligheid met de IT- en OT-leveranciers

a. [open vraag, tonen bij *] Kunt u kort aangeven welke normen zijn gesteld aan digitale veiligheid of welke afspraken hierover zijn gemaakt met de IT-leveranciers (kantoor- en administratieve automatisering) en/of met OT-leveranciers (productie- en logistieke automatisering)? [meerdere antwoorden mogelijk]
- Normen of afspraken over digitale veiligheid met IT-leveranciers over:
- Normen of afspraken over digitale veiligheid met OT-leveranciers over:

13. *Wie is binnen uw organisatie verantwoordelijk voor de digitale veiligheid? [meerdere antwoorden mogelijk, gesloten vraag]*
- Eigenaar/directie/management
- Informatiebeveiligingsspecialist(en) / cybersecurityspecialist(en)
- Systeembeheerder(s)
- Ingehuurde systeembeheerder(s) of (informatie) beveiliger(s)
- Weet ik niet
- Anders, namelijk:

14. *Hoeveel mensen heeft uw organisatie (in dienst of ingehuurd) die zich specifiek toeleggen op digitale veiligheid van de IT- en OT-systemen (geheel of voor een deel van hun functie)? [aantal personen]*

15. *Welk rapportcijfer (1 – 10) geeft u voor de wijze waarop digitale veiligheid van uw organisatie op dit moment is geborgd? [getal]*

16. *Zijn voor uw organisatie de volgende beveiligingsmaatregelen getroffen?* [matrixvraag, antwoordcategorieën: *volledig / grotendeels / beperkt / niet / weet ik niet*]
- Het inventariseren en analyseren van de kwetsbaarheden in alle IT- en OT-systemen
- Het implementeren van veilige instellingen op alle apparatuur, software, netwerk en internetverbindingen
- Het regelmatig en tijdig implementeren van alle software- en beveiligingsupdates
- Het beperken van toegang tot de IT- en OT-systemen voor de eigen medewerkers en externe partijen
- Het voorkomen van virussen en andere malware op alle IT- en OT-systemen

17. *Maakt uw organisatie gebruik van een baseline of een checklist voor de digitale veiligheid van uw organisatie? [gesloten vraag]*
- Ja, wij maken gebruik van één of meer gestandaardiseerde baselines (bijv. ISO27002, IEC62443)*
- Ja, we maken gebruik van een eigen checklist voor digitale veiligheid van de organisatie**
- Nee
- Weet ik niet

a. [open vraag, tonen bij *] Kunt u aangeven welke baseline(s) uw organisatie gebruikt?
b. [tonen bij * en **] Kunt u globaal schatten (0 – 100%) hoever uw organisatie gevorderd is met het implementeren van de baseline(s) of checklist?

18. *Worden er in uw organisatie voor alle kritische IT-systemen (kantoor- en administratieve automatisering) en OT-systemen (productie- en logistieke automatisering) risicoanalyses uitgevoerd gericht op digitale veiligheid? [gesloten vraag]*
- Ja, voor ***elk*** kritisch IT- of OT-systeem wordt een impact- en/of privacyimpactanalyse ***én*** een kwetsbaarheid/ maatregelanalyse uitgevoerd ***én*** deze worden regelmatig geactualiseerd
- Ja, voor ***elk*** kritisch IT- of OT-systeem wordt incidenteel (bijvoorbeeld bij de aanschaf) of regelmatig een impact- en/of privacyimpactanalyse uitgevoerd
- Ja, voor ***elk*** kritisch IT-systeem wordt een risicoanalyse uitgevoerd, maar niet voor elk kritisch OT-systeem
- Ja, voor ***sommige*** kritische systemen worden impact- en/of privacyimpactanalyses en/of kwetsbaarheid/ maatregelanalyses uitgevoerd
- Nee, maar er is wel een risicoanalyse op organisatie/ procesniveau uitgevoerd
- Nee, we maken geen gebruik van risicoanalyses
- Weet ik niet

19. *Maakt uw organisatie gebruik van monitoring om verdacht verkeer op het netwerk tijdig te kunnen detecteren? [gesloten vraag]*
    - Ja, ons netwerk wordt gemonitord in eigen beheer
    - Ja, monitoring van ons netwerk wordt uitgevoerd door een externe partij
    - Nee, ons netwerk wordt niet gemonitord
    - Weet ik niet

20. *Worden er voor uw organisatie testen uitgevoerd om zwakke plekken in de digitale veiligheid van uw organisatie op te sporen? Denk bijvoorbeeld aan penetratietesten, red team testen, social engineering testen, e.d. [gesloten vraag]*
    - Ja, deze worden periodiek uitgevoerd
    - Ja, deze worden incidenteel uitgevoerd
    - Nee, wij maken geen gebruik van testen
    - Weet ik niet

21. *Wordt de digitale veiligheid van uw organisatie geaudit? [meerdere antwoorden mogelijk, gesloten vraag]*
    - Ja, periodiek met een interne audit
    - Ja, incidenteel met een interne audit
    - Ja, periodiek met een externe audit
    - Ja, incidenteel met een externe audit
    - Nee, de digitale veiligheid wordt bij ons niet geaudit
    - Weet ik niet

22. *Is uw organisatie gecertificeerd voor de digitale veiligheid? [meerdere antwoorden mogelijk, gesloten vraag]*
    - Ja, we zijn ISO 27001 gecertificeerd
    - Ja, we zijn IEC 62443 gecertificeerd
    - Ja, we zijn gecertificeerd op basis van een andere informatiebeveiligingsstandaard*
    - Nee, we zijn niet gecertificeerd, maar hebben wel een Information Security Management System (ISMS) ingericht
    - Nee, we zijn niet gecertificeerd maar werken wel met een standaard*
    - Nee, we zijn niet gecertificeerd
    - Weet ik niet

a. [open vraag, tonen bij *] Welke informatiebeveiligingsstandaard voor IT en/of OT betreft dit?

23. *Verschillende organisaties binnen het glastuinbouwcluster hebben aangegeven behoefte te hebben aan meer ondersteuning bij het inrichten van de digitale veiligheid van de organisatie. Kunt u aangeven of u zou overwegen om deel te nemen aan de volgende bijeenkomsten of initiatieven?*
    - Een voorlichtingsbijeenkomst over digitale veiligheid? JA/NEE/NVT
    - Een cursus (1 dagdeel) over eerste stappen bij het inrichten van digitale veiligheid van uw organisatie? JA/NEE/NVT
    - Een eendaagse cursus van over de inrichting van digitale veiligheid voor meer gevorderde organisaties? JA/NEE/NVT
    - Een test uitgevoerd door een externe partij om zwakke plekken in de digitale veiligheid van uw organisatie op te sporen? JA/NEE/NVT
    - Een quickscan om de volwassenheid van uw organisatie op het gebied van digitale veiligheid in kaart te brengen JA/NEE/NVT
    - Een periodiek overleg met collega-organisaties (eventueel binnen de eigen vereniging of coöperatie) over vraagstukken op het gebied van digitale veiligheid JA/NEE/NVT
    - Een cyberweerbaarheidscentrum, een kenniscentrum voor informatievoorziening en ondersteuning van het glastuinbouwcluster op het gebied van digitale veiligheid? JA/NEE/NVT

24. *Heeft u andere suggesties voor ondersteuning bij het inrichten van de digitale veiligheid van de organisatie? [open vraag]*

25. *Wilt u nog iets toevoegen of toelichten naar aanleiding van deze enquête? [open vraag]*

26. *Zou u verder betrokken willen worden bij het onderzoek naar digitale veiligheid van Greenport West-Holland? [meerdere antwoorden mogelijk, gesloten vraag]*
    - Ja, ik wil op de hoogte gehouden worden van de uitkomsten*
    - Ja, jullie kunnen mij benaderen om mee te denken over de uitkomsten en opvolging van dit onderzoek*
    - Nee

a. [open vragen tonen bij *] Hoe kunnen wij u bereiken? (Indien gewenst kunt u dit ook laten weten door een mail te sturen aan **e.f.p.kerpershoek@hhs.nl**)
    - Naam:
    - Organisatie:
    - E-mailadres:

Hartelijk dank voor uw medewerking!

Bijlage 3: Geïnterviewden

- Martijn van Andel, directeur, JEM-id
- John Bolte, lector Smart Sensor Systems, De Haagse Hogeschool
- Joep van den Bosch, CIO, Ridder
- Wouter van den Bosch, directeur, Kwekerij van den Bosch
- Remco Duijverman, product owner, Hoogendoorn
- Edwin Hoogesteger, CIO, Best Fresh Group
- Ruud Hoosemans, innovatiemanager, GroentenFruit Huis
- Marcel Jutte, directeur, Hudson Cybertec
- Eric Luiijf, eigenaar, Luiijf Consultancy
- Harrij Schmeitz, programmamanager Glas 4.0, Technology{}Pull
- Jacco Vooijs, Voorzitter sub-regio's Westland en Aalsmeer, Glastuinbouw Nederland
- Bas Wevers, CISO, Royal FloraHolland
- ICT manager, Certhon
- Specialist informatiebeveiliging, zaadveredelingsorganisatie
- CIO, zaadveredelingsorganisatie
- Innovatiemanager, telersvereniging glasgroenten

Adres- en contactgegevens

Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl