Digitale veiligheid van de Life Sciences & Health-sector

Onderzoeksrapport

Uitgevoerd door:

- Hogeschool Leiden, Lectoraat Digital Forensics & E-Discovery
- De Haagse Hogeschool, Lectoraat Cyber Security & Safety
- REQON, IT-Security

In opdracht van:

- Security Delta
- Stichting Leiden Bio Science Park
- Metropoolregio Rotterdam Den Haag

Februari 2023

let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

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

Auteurs:
Dr. Marcel Spruit
Dr. Emiel Kerpershoek
Harm Blankers BSc
Hans Bertens
Lieneke Paalman BSc

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

Voorwoord

De voor u liggende onderzoeksrapportage geeft een indruk van de digitale veiligheid van organisaties die actief zijn in de Life Sciences & Health-sector (LSH). Daartoe is voor een beperkt aantal organisaties onderzocht hoe het staat met de technische en organisatorische inrichting van digitale veiligheid.

Het onderzoek is geïnitieerd door Security Delta (HSD) en Stichting Leiden Bio Science Park. De aanleiding ervoor was de Roadmap gericht op het verbeteren van de weerbaarheid van de digitale economie van de Provincie Zuid-Holland, waarin de Life Sciences & Health-sector is aangemerkt als een van de aandachtsgebieden.

De rapportage is tot stand gekomen in nauwe samenwerking tussen Hogeschool Leiden, De Haagse Hogeschool, REQON en de opdrachtgevers Security Delta en Stichting Leiden Bio Science Park en is gefinancierd vanuit Metropoolregio Rotterdam Den Haag (MRDH). We willen de organisaties die hebben deelgenomen aan dit onderzoek bedanken voor hun medewerking en openheid.

We hopen dat de aanbevelingen in dit rapport opgepakt kunnen worden door de Life Sciences & Health-sector om zo de digitale veiligheid van hun organisaties te vergroten.

Dr. Marcel Spruit
Dr. Emiel Kerpershoek
Harm Blankers BSc
Hans Bertens
Lieneke Paalman BSc

Leiden, februari 2023

INHOUDSOPGAVE

1 Inleiding

1.1 Achtergrond

Incidenten met betrekking tot de digitale veiligheid van een organisatie, oftewel cyberincidenten, zijn aan de orde van de dag. De oorzaken kunnen kwaadwillende acties van binnen of van buiten de organisatie zijn, zoals fraude en ransomware, maar het kunnen ook onopzettelijke fouten zijn, zoals het verliezen van een USB-stick. Bovendien kunnen storingen in de digitale systemen tot cyberincidenten leiden. Volgens het CBS is in 2020 meer dan 60% van de bedrijven in Nederland ten minste één keer slachtoffer geworden van een cyberincident.[1] De schade loopt in de miljarden en wordt veroorzaakt doordat werkprocessen stil komen te liggen, verlies van relevante data, kostbare hersteloperaties en imagoschade.

Het Nationaal Cyber Security Centrum (NCSC) ondersteunt de vitale sectoren in Nederland bij het in beeld brengen en beheersen van risico's op het gebied van digitale veiligheid. Ook voor de niet-vitale sectoren die een belangrijke rol spelen in de economie van de Provincie Zuid-Holland, zoals de Life Sciences & Health-sector, is behoefte aan dergelijke ondersteuning. In opdracht van de Provincie Zuid-Holland is in 2020 een onderzoek uitgevoerd naar de mate waarin de provinciale economie bestand is tegen cyberaanvallen.[2] Uit dit onderzoek blijkt onder meer dat de Life Sciences & Health-sector in hoge mate gedigitaliseerd is en kwetsbaar is voor cyberdreigingen zoals het stelen van intellectueel eigendom en het lekken van persoonsgegevens. Dit beeld is bevestigd in een onderzoek dat in 2022 is uitgevoerd door Buck Consultant in opdracht van Security Delta (HSD).[3] Binnen de sector bestaan grote verschillen in de mate van risicomanagement op het gebied van de digitale veiligheid, waarbij vooral middelgrote en kleine bedrijven en instellingen de risico's vaak wel zien, maar niet weten hoe ze hiermee om moeten gaan. Deze groep heeft behoefte aan gerichte ondersteuning.

In navolging van een vergelijkbaar initiatief voor het glastuinbouwcluster in de Greenport West-Holland, hebben Security Delta en Stichting Leiden Bio Science Park (LBSP) het initiatief genomen voor een inventariserend onderzoek naar de digitale veiligheid van organisaties in de Life Sciences & Health-sector (LSH).

1.2 Doelstelling

In vervolg op het onderzoek uit 2020 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 de Life Sciences & Health-sector in kaart te brengen en aanbevelingen te formuleren voor het verbeteren van de digitale veiligheid. De centrale vraagstelling voor dit onderzoek luidt:

Hoe is het gesteld met digitale veiligheid in de Life Sciences & Health-sector en wat is nodig om dit te verbeteren?

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

1. Wat zijn de relevante dreigingen voor de digitale veiligheid van organisaties in de LSH-sector?
2. Wat is de potentiële impact van digitale veiligheidsincidenten op organisaties in de LSH-sector?
3. Welk niveau van digitale veiligheid hebben organisaties in de LSH-sector op dit moment?
4. Wat is de behoefte aan ondersteuning voor het verbeteren van de digitale veiligheid van organisaties in de LSH-sector?

Dit onderzoek resulteert in een onderzoeksrapport, inclusief aanbevelingen die kunnen bijdragen aan het verbeteren van de digitale veiligheid in de LSH-sector. Het Leiden Bio Science Park is een belangrijke clusters in de LSH-sector in Nederland en neemt een centrale plek in in dit onderzoek.

1.3 De Life Sciences & Health-sector

De Life Sciences & Health-sector (LSH) bestaat uit uiteenlopende bedrijven en instellingen met veelal een internationale oriëntatie. Een deel van de organisaties (Life- en BioScience) richt zich op R&D en productie van o.a. medicijnen, vaccins of biomarkers. Een ander deel van de organisaties richt zich op de ontwikkeling en productie van medische technologie (Medtech). Dit omvat zowel hoogwaardige apparatuur voor bijvoorbeeld operatiekamers en intensive careafdelingen in (poli-) klinieken, als medium en low tech producten voor zorg in en om huis. Tot slot omvat de Health-kant van de sector voornamelijk zorginstellingen (zowel cure als care) en gezondheidsondersteunende diensten, die primair ten goede komen aan de eigen inwoners van de provincie.

1 CBS (2021). *Cybersecuritymonitor 2020*. Centraal Bureau voor de Statistiek.
2 K. Gijsbers (2020). *Cybergereedheid economie Provincie Zuid-Holland*. Cyber4Board.
3 Buck Consultants (2022). *Verkenning behoefte cyberweerbaarheidscentrum Life Sciences & Health Sector Zuid-Holland*. Buck Consultants International.

De Life-& BioSciences en Medtech-sector in Zuid-Holland behoort tot de top van de wereld op het gebied van wetenschappelijk onderzoek en ondernemerschap. In 2020 telt deze sector in totaal 2.147 bedrijven met 68.461 werkzame personen. In het Leiden Bio Science Park zijn meer dan 400 innovatieve Life Sciences-bedrijven actief in de biotech/farma en de ontdekking en ontwikkeling van geneesmiddelen.[4] Al deze bedrijven en instellingen opereren binnen ketens van toeleveranciers, dienstverleners en afnemers c.q. eindgebruikers, die vaak de provinciegrens overstijgen. In deze ketens spelen digitale systemen een steeds belangrijkere rol en daarmee wordt ook de digitale veiligheid steeds belangrijker. Omdat dreigingen ten aanzien van de digitale veiligheid zich kunnen richten op de zwakke schakels in deze ketens, is voor het bestrijden ervan een ketenbenadering belangrijk.

1.4 Onderzoeksaanpak

Dit onderzoek is uitgevoerd in de maanden mei tot oktober 2022. Voor de beantwoording van de onderzoeksvragen wordt gebruik gemaakt van deskresearch, een enquête, semigestructureerde interviews en technische metingen. Deskresearch als methode van onderzoek omvat analyse van wetenschappelijke en vakliteratuur en relevante documentatie over digitale veiligheid van IT- en OT-systemen en is gebruikt voor het theoretisch kader van het onderzoek, voor het opstellen van de enquête en het protocol voor de interviews en voor de opzet van de technische metingen.

Bij aanvang van het onderzoek is een enquête uitgezet onder organisaties in de LSH-sector, mede met behulp van het Leiden Bio Science Park. Met de enquête wordt voor organisaties in kaart gebracht welke risico's ze zien voor de digitale veiligheid van hun organisatie en welke maatregelen ze hebben getroffen om hun organisatie tegen cyberincidenten te beschermen. De vragen in de enquête (zie bijlage 1) zijn gebaseerd op het 3-pijlermodel voor volwassenheid van informatiebeveiliging[5] en de informatiebeveiligingsstandaard NEN-EN-ISO/IEC 27001:2017.

Op 11 mei 2022 is de link naar de enquête verspreid via de nieuwsbrief van de Ondernemersvereniging Bio Science Park (OVBSP). Om de response op de enquête te vergroten is de enquête twee weken later gericht per mail verstuurd aan 75 leden van OVBSP die voor hun bedrijfsvoering primair gericht zijn op Life-, BioScience- en Medical Technology-activiteiten. Acht organisaties hebben de enquête ingevuld. Hiernaast is de enquête ook via enkele bijeenkomsten, gericht op cybersecurity en digitale innovatie, onder de aandacht gebracht bij LSH-organisaties in de Medical Delta (regio Den Haag, Delft, Rotterdam). Dit heeft geleid tot één extra reactie op de enquête. Hiermee hebben in totaal negen organisaties de enquête ingevuld. Aanvullend hebben wij van drie organisaties per mail een toelichting ontvangen op hun reden om de enquête niet in te vullen. De totale respons op de enquête komt hiermee uit op 12 organisaties. De uitvraagperiode van de enquête is gesloten op 25 oktober 2022.

Naast de enquête werden de aangeschreven organisaties ook uitgenodigd om deel te nemen aan het onderzoek door middel van het kosteloos uitvoeren van een volwassenheidsmeting van de digitale veiligheid van de organisatie en een technische scan van de veiligheid van het IT-netwerk. Twee organisaties in het LBSP hebben gebruik gemaakt van dit aanbod en boden hiermee gelegenheid voor een verdiepende analyse van de technische en organisatorische inrichting van digitale veiligheid van de organisatie. Twee andere organisaties hebben aangegeven dat ze zelf al regelmatig dit soort metingen en scans laten doen.

Meting volwassenheid digitale veiligheid

Voor het meten van de volwassenheid van de digitale veiligheid van een organisatie is gebruik gemaakt van het 3-pijlermodel voor informatiebeveiliging, zie figuur 1.1. Aan de hand van dit model is op basis van semigestructureerde interviews bepaald hoe goed de organisatie de 3 pijlers voor de digitale veiligheid heeft ingevuld. De interviews zijn afgenomen door ter zake deskundige interviewers. Voor veel vragen is het namelijk nodig om door te vragen om zeker te stellen dat de vraag goed is begrepen en met voldoende nuance is beantwoord. De vragen hebben betrekking op drie pijlers, namelijk:

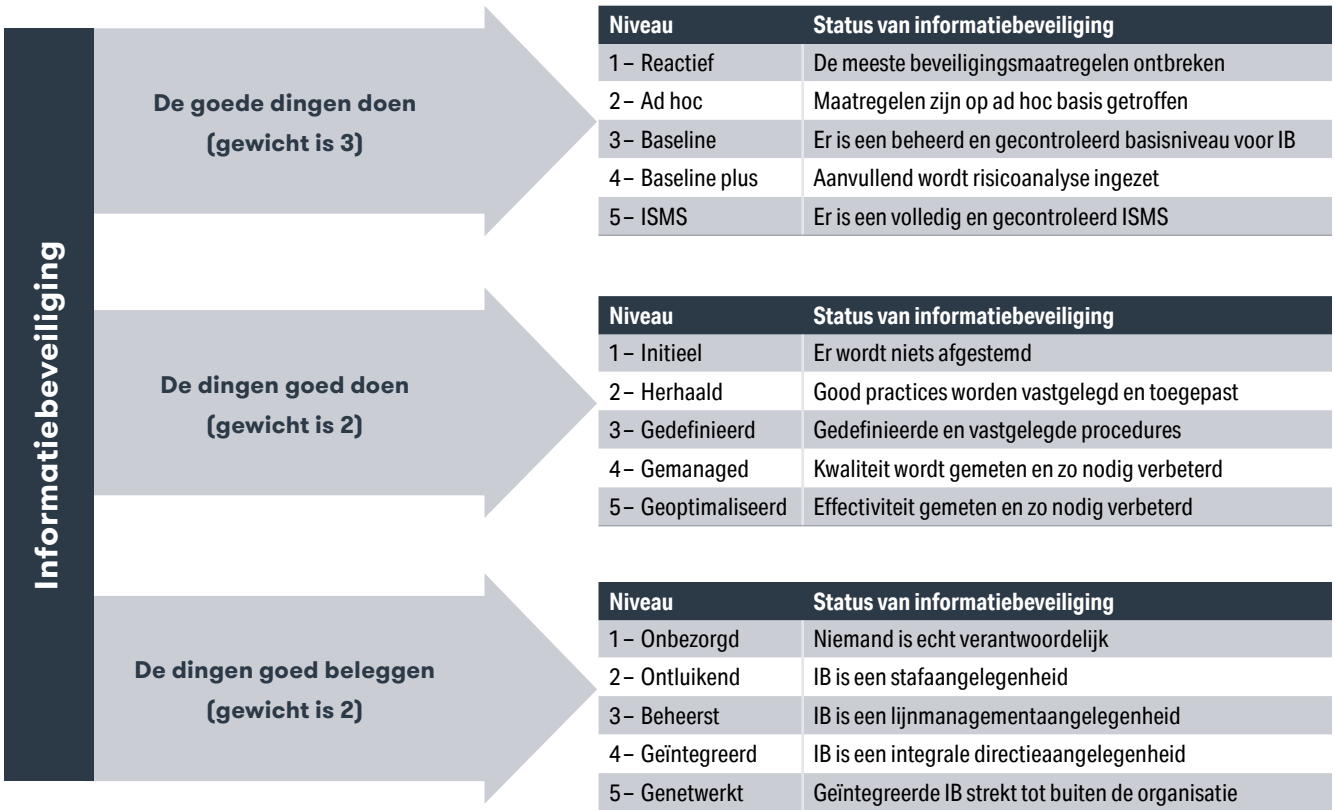
- De mate waarin de goede activiteiten voor digitale veiligheid worden uitgevoerd.
- De mate waarin de betreffende activiteiten goed worden uitgevoerd.
- De mate waarin de uitvoering en de aansturing van deze activiteiten goed zijn belegd.

Om kleuring door ondeskundigheid, bias en vooringenomenheid zoveel mogelijk te voorkomen, zijn de interviews bij voorkeur separaat uitgevoerd met verschillende functionarissen, namelijk:

- Iemand uit het management, bijvoorbeeld de CIO.
- Iemand die de beveiliging van de automatisering goed kent.
- Iemand die niet werkzaam is in een IT-, OT- of beveiligingsfunctie.

4 Buck Consultants (2022). *Verkenning behoefte cyberweerbaarheidscentrum Life Sciences & Health Sector Zuid-Holland.* Buck Consultants International.

5 M. Spruit (2017). *Volwassenheid informatiebeveiliging; 3-Pijlermodel.* Whitepaper, RAAK-project Veilig Water, Den Haag. DOI: 10.13140/RG.2.2.24840.16641.



Niveau	Status van informatiebeveiliging
1 – Reactief	De meeste beveiligingsmaatregelen ontbreken
2 – Ad hoc	Maatregelen zijn op ad hoc basis getroffen
3 – Baseline	Er is een beheerd en gecontroleerd basisniveau voor IB
4 – Baseline plus	Aanvullend wordt risicoanalyse ingezet
5 – ISMS	Er is een volledig en gecontroleerd ISMS

Niveau	Status van informatiebeveiliging
1 – Initieel	Er wordt niets afgestemd
2 – Herhaald	Good practices worden vastgelegd en toegepast
3 – Gedefinieerd	Gedefinieerde en vastgelegde procedures
4 – Gemanaged	Kwaliteit wordt gemeten en zo nodig verbeterd
5 – Geoptimaliseerd	Effectiviteit gemeten en zo nodig verbeterd

Niveau	Status van informatiebeveiliging
1 – Onbezorgd	Niemand is echt verantwoordelijk
2 – Ontluikend	IB is een stafaangelegenheid
3 – Beheerst	IB is een lijnmanagementaangelegenheid
4 – Geïntegreerd	IB is een integrale directieaangelegenheid
5 – Genetwerkt	Geïntegreerde IB strekt tot buiten de organisatie

Figuur 1.1: Het 3-pijlermodel schematisch weergegeven

In de interviews is gevraagd naar de inrichting van de informatiebeveiliging. Hierbij is niet gevraagd naar bewijsmateriaal om de gedane beweringen te onderbouwen. Er is dan ook geen sprake van een audit, maar van een indicatieve meting. Het interviewprotocol is opgenomen in bijlage 2. Elke deelnemende organisatie heeft een beknopte rapportage van de bevindingen ontvangen.

De score voor ieder van de drie pijlers kan lopen van 1 tot 5, waarbij 1 aangeeft dat de betreffende pijler nog niet is gerealiseerd en 5 aangeeft dat de pijler volledig is gerealiseerd.

De drie pijlers wegen niet even zwaar. Het uitvoeren van de goede activiteiten weegt het zwaarst (gewicht 3), want als de organisatie de verkeerde activiteiten doet, wordt informatiebeveiliging überhaupt niets. Als de werkwijze en de belegging meer volwassen worden, wordt de beveiliging effectiever, maar zelfs zonder dat werken de maatregelen toch, zij het minder effectief. De werkwijze en de belegging wegen daarom beide, en in dezelfde mate, minder zwaar (gewicht 2).

Het volwassenheidsniveau van informatiebeveiliging, M_{IB}, is het gewogen gemiddelde van de scores voor de drie pijlers (s_1,s_2,s_3). In formule weergegeven:

$$M_{IB} = \frac{s_1 \times 3 + s_2 \times 2 + s_3 \times 2}{3 + 2 + 2}$$

Technische meting

De basis van de technische meting voor het meten van de IT-beveiliging betrof een geautomatiseerde vulnerability scan uitgevoerd met de tool Nessus. De rijkweidte van de scan is voorafgaand aan de meting bij elke deelnemer met de systeembeheerder vastgesteld.

Daarna hebben de onderzoekers van REQON de bevindingen uit de scan handmatig gevalideerd en hebben ze de scanresultaten gecontroleerd op false positives. Ook hebben de onderzoekers een aantal basistests uitgevoerd, zoals het inloggen met standaard wachtwoorden en het bekijken van services die zonder wachtwoord toegankelijk zijn.

De resultaten zijn na het onderzoek direct met de deelnemer gedeeld. Daarnaast hebben de onderzoekers van REQON de deelnemers voorzien van een advies om de meest kritieke kwetsbaarheden te mitigeren. De bevindingen van de uitgevoerde technische metingen worden in de vorm van een trendanalyse beschreven in het eindrapport.


PULSE 82
DBP 80
STATUS: 15% COMPLETE
STABLE
104.2

2 Literatuur

2.1 Digitalisering: informatietechnologie & operationele technologie

De afgelopen decennia hebben zich grote ontwikkelingen voorgedaan op het gebied van informatietechnologie (IT) voor kantoorautomatisering en administratieve automatisering. Hierbij valt te denken aan 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. [6] Al deze ontwikkelen bieden steeds meer functionaliteit voor organisaties. Echter, ook het aantal en de diversiteit van de dreigingen met betrekking tot de IT is toegenomen.

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.[7] 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 aansturen van klimaatbeheersystemen, of robots in productie- of onderzoeksprocessen. Alhoewel het functioneren van de OT-systemen vaak cruciaal is voor de organisaties die ermee werken, krijgt de digitale veiligheid van deze systemen vaak nog te weinig aandacht.[8] [9]

Ook voor veel organisaties in de LSH-sector spelen OT-systemen voor het monitoren en aansturen van fysieke systemen en processen een belangrijke rol. Doordat OT-systemen vaak worden aangestuurd of uitgelezen door programmatuur op een pc, of een app op een smartphone, zijn er 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.[10]

2.2 Dreigingslandschap in Nederland

In het Cybersecuritybeeld Nederland 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 OT-systemen zal toenemen voor de sectoren die hun processen verder automatiseren.[11]

In Nederland en in het buitenland zijn in de afgelopen jaren diverse voorbeelden geweest van deze toenemende dreiging.[12] Zo zijn 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 zijn de uitschakeling van uraniumcentrifuges in Iran (2010), 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 die slachtoffer werden van de Ivanti Pulse Connect Secure hack (2021).[13] [14] [15] Diverse online incidentenlijsten laten zien dat slechts een klein deel van alle incidenten het nieuws haalt en daarmee het topje van de ijsberg vormt.[16]

6 M. Spruit (2018). *Informatie onder controle*. MS.
7 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.
8 H. Luiijf en R. Lassche (2006). *SCADA (on)veiligheid: een rol voor de overheid?*. TNO-KEMA.
9 E. Luiijf (2012). Onbewust onveilig. *Informatiebeveiliging*, nr. 4, pag. 4-7
10 R. Brennenraedts, et al. (2020). *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity.* WODC.
11 NCSC (2021). *Cybersecuritybeeld Nederland* CSBN 2021. NCTV/NCSC
12 E. Luiijf (2012). Onbewust onveilig. *Informatiebeveiliging*, nr. 4, pag. 4-7.
13 **https://www.trouw.nl/cs-b4a6a43b**
14 R. Brennenraedts, et al. (2020). *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity.* WODC.
15 **https://en.wikipedia.org/wiki/Ivanti_Pulse_Connect_Secure_data_breach**
16 zie bijvoorbeeld **https://en.wikipedia.org/wiki/List_of_security_hacking_incidents**

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 dan ook sterk toenemen.

2.3 Digitale veiligheid

De NCTV en het NCSC geven aan dat de weerbaarheid tegen digitale dreigingen in Nederland nog altijd onvoldoende is.[17] Zij stellen vast dat, net als in de afgelopen 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. De NCTV en het NCSC zien ook grote verschillen in het kennisniveau van organisaties op het gebied van digitale veiligheid 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.[18]

De Cyber Security Raad (CSR) geeft aan dat de digitale weerbaarheid voor vitale processen in Nederland nog niet op orde is, waardoor basale dreigingen niet goed kunnen worden gepareerd of gedetecteerd.[19] Bedrijven en overheidsorganisaties in vitale sectoren worden weliswaar door het NCSC op de hoogte gehouden van actuele dreigingen, kwetsbaarheden en oplossingen om de digitale weerbaarheid 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.[20] Verstoring of uitval van digitale systemen in niet-vitale sectoren, zoals de LSH-sector, kan ook leiden tot een aanzienlijke kostenpost voor de samenleving, maar deze sectoren kunnen nog geen gebruik maken van de diensten van het NCSC.

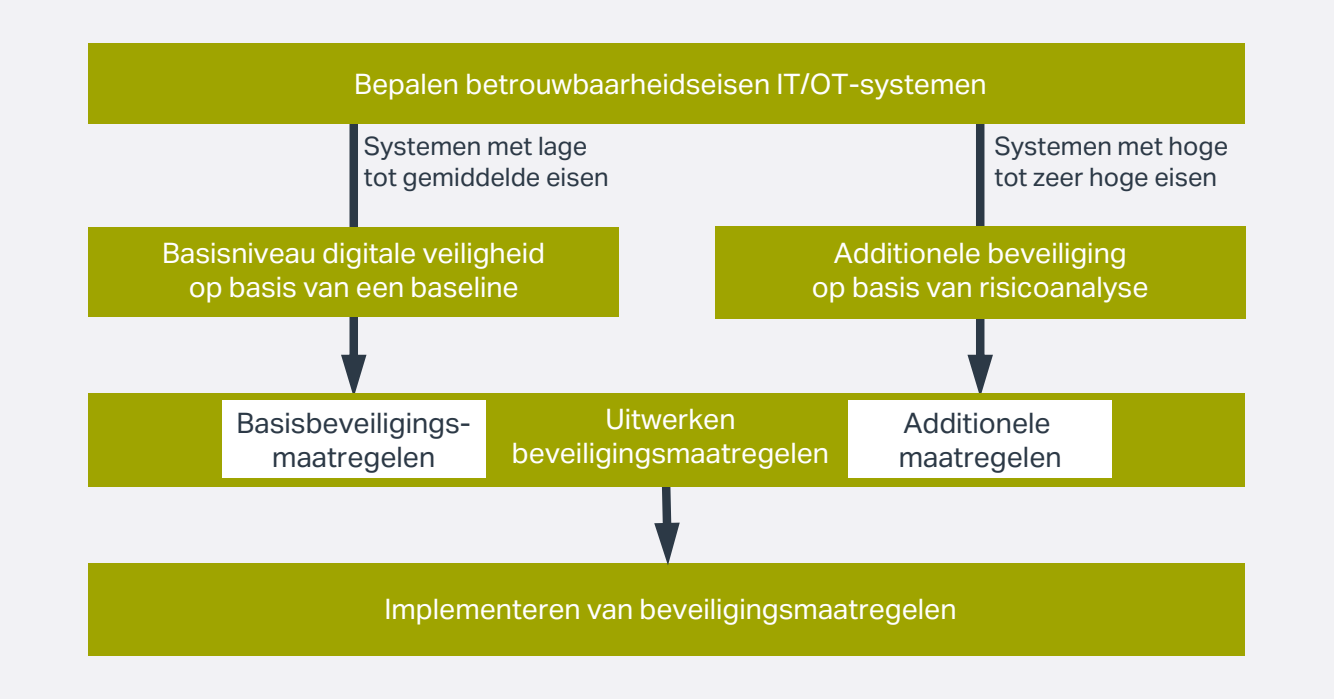
Vanwege het belang van de IT en de OT voor de bedrijfsvoering van de organisaties in de LSH-sector is het beveiligen ervan belangrijk voor de continuïteit van deze organisaties en van de sector als geheel. Dit wordt aangeduid als digitale veiligheid, cybersecurity, of cyberweerbaarheid.

Het NCSC definieert dit als:[21]

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 parallelle sporen, zie figuur 2.1.[22]

17 NCSC (2021). *Cybersecuritybeeld Nederland* CSBN 2021. NCTV/NCSC.
18 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.
19 Cybersecurityraad (2021). *Integrale aanpak cyberweerbaarheid.* CSR.
20 **https://www.digitaltrustcenter.nl/nieuws/digital-trust-center-start-met-actief-informeren-bedrijven-over-digitale-dreigingen**
21 NCSC (2021). *Cybersecuritybeeld Nederland* CSBN 2021. NCTV/NCSC.
22 M. Spruit, e.a. (2015). *Safe in cyberspace; van awareness naar actie*. Sdu.



Figuur 2.1: 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 vergelijkbaar zijn, vormen deze de basis voor veel baselines voor digitale veiligheid 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.[23]

Voor het kiezen van de maatregelen voor het eerste spoor kan gebruik gemaakt worden van de zeer gangbare informatiebeveiligingsbaseline zoals beschreven in de informatiebeveiligingsstandaard NEN-EN-ISO/IEC 27002:2017. Een sterk vereenvoudigde set maatregelen die een eerste stap kan vormen om te komen tot een basisniveau van digitale veiligheid is door het Digital Trust Center beschreven:[24]

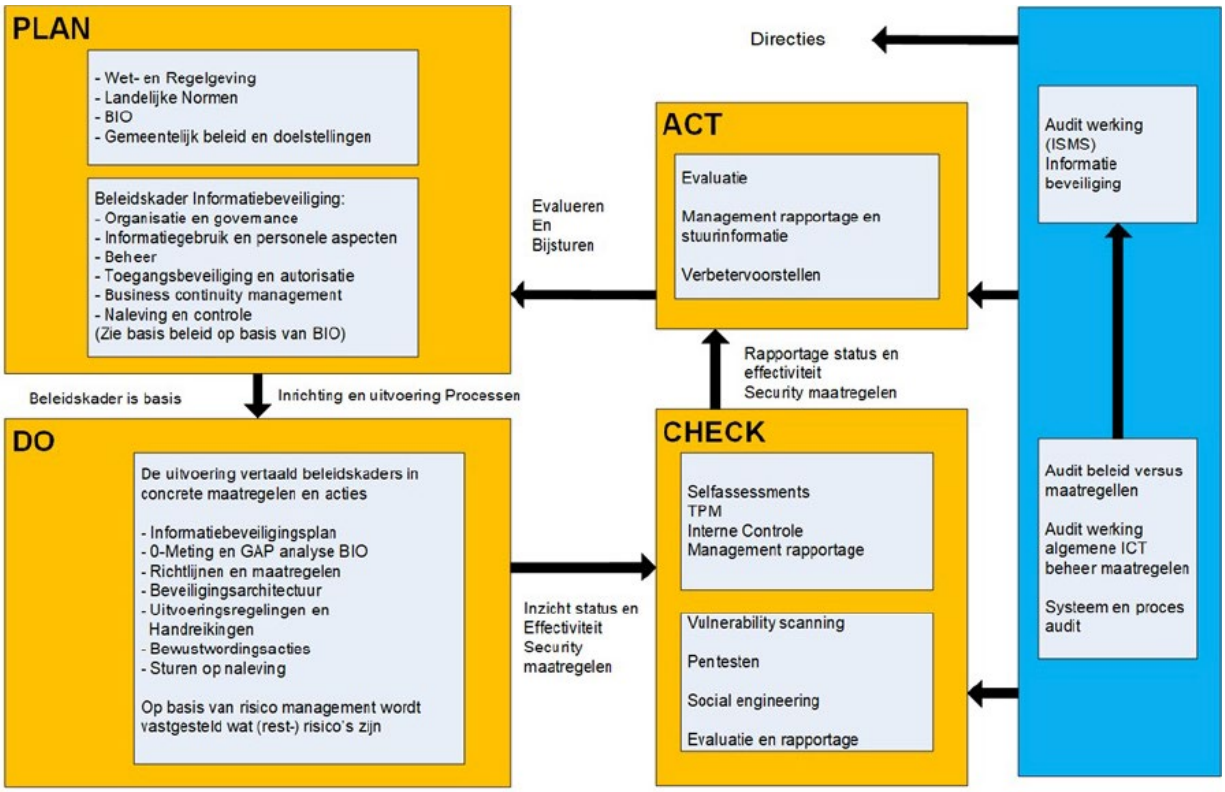
- Inventariseer kwetsbaarheden.
- Kies veilige instellingen.
- Voer updates uit.
- Beperk toegang tot systemen en data.
- Voorkom virussen en andere malware.

Deze set maatregelen, aangevuld met het inzetten van netwerkmonitoring om beveiligingsinbreuken vroegtijdig te signaleren, worden in dit onderzoek aangemerkt als elementaire maatregelen voor digitale veiligheid van de organisaties.

Als een basisniveau voor digitale veiligheid op basis van een baseline goed is geïmplementeerd, dan voegt het rechter spoor in de tweesporenaanpak het inzetten van risicoanalyses toe. Dit spoor 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.[25] De aanpak in het rechter spoor is hiermee grondiger, maar ook tijdrovender. Vandaar dat het rechter spoor alleen wordt ingezet voor essentiële IT- en OT-systemen en als het linker spoor reeds op orde is.

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

De tweesporenaanpak is in principe onderdeel van een plan-do-check-act-cyclus, oftewel een managementsysteem voor de digitale veiligheid van de organisatie, veelal aangeduid als een ISMS, zie figuur 2.2[26]. In een ISMS worden de benodigde maatregelen voor de digitale veiligheid conform de tweesporenaanpak geselecteerd en geïmplementeerd, en wordt de werking van deze maatregelen regelmatig geëvalueerd en zo nodig aangepast. Deze aanpak voegt evaluaties toe aan de baseline en risicoanalyses. De meest gebruikelijke evaluaties zijn het technisch testen van de toegang tot de IT- en OT-systemen (pentesten) en interne en externe audits van de organisatie van de digitale veiligheid.



Figuur 2.2: Opbouw van een managementsysteem voor digitale veiligheid (ISMS)

26 IBD (2019). *Handreiking Information Security Management System (ISMS).* Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten.

3 Bevindingen

3.1 Respons

Van de 75 organisaties die zijn uitgenodigd om deel te nemen aan het onderzoek hebben negen de enquête ingevuld en hebben drie organisaties per e-mail gereageerd op de enquête. De totale respons komt hiermee uit op twaalf organisaties. De groep van organisaties die aan de enquête heeft ingevuld is als volgt opgebouwd:

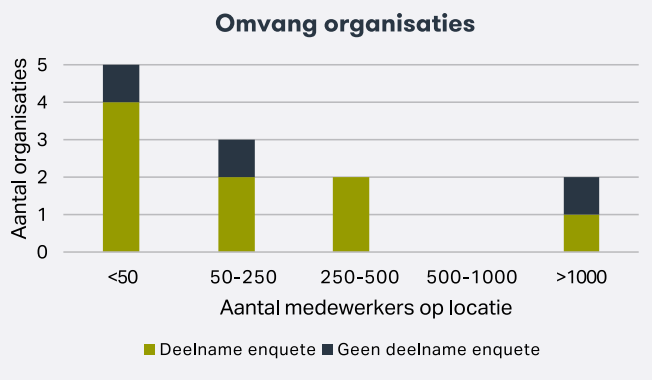
- Twee organisaties gericht op biotech.
- Twee organisaties gericht op life science.
- Twee organisaties gericht op farmaceutische activiteiten.
- Twee organisaties gericht op ondersteuning, training, onderwijs, of contractonderzoek.
- Eén zorginstelling.

De resterende drie organisaties hebben wel informatie gegeven, maar niet de enquête ingevuld:

- Twee organisaties gericht op farmaceutische activiteiten.
- Eén organisatie gericht op ondersteuning, training, onderwijs, of contractonderzoek.

De redenen waarom deze organisaties de enquête niet hebben ingevuld, lopen uiteen. Eén organisatie vanwege het feit dat ze al worden getest en geaudit, één organisatie omdat zij op het punt staan een deel van hun digitale infrastructuur te vervangen en één organisatie omdat het veiligheidsbeleid hen niet toestaat te communiceren over hun beveiliging.

De organisaties die hebben gereageerd op de uitnodiging voor deelname aan het onderzoek variëren van klein tot groot.



Figuur 3.1: Omvang van de twaalf organisaties die hebben gereageerd op de uitnodiging voor deelname aan het onderzoek in aantallen medewerkers

Van de negen organisaties die hebben deelgenomen aan de enquête hebben twee gebruik gemaakt van de verdiepende analyse in de vorm van een volwassenheidsmeting van de digitale veiligheid van de organisatie en een technische scan van de veiligheid van het IT-netwerk.

Gezien het beperkte aantal deelnemende organisaties en de toezegging van anonimiteit voor deze organisaties, wordt in de onderzoeksbevindingen geen onderscheid gemaakt naar de omvang of het type van de organisatie.

3.2 Relevante dreigingen

Ten behoeve van dit onderzoek is een overzicht gemaakt van relevante dreigingen voor de digitale veiligheid van organisaties in de LSH-sector. In de onderstaande tabellen is een overzicht gegeven van de verschillende typen dreigingen en van de actoren waarvan de grootste dreiging uitgaat. Hierbij moet worden opgemerkt dat de genoemde dreigingen en actoren deels aan elkaar gerelateerd zijn.

Tabel 3.1: Typen dreigingen voor de digitale veiligheid van LSH-organisaties

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 3.2: Typen actoren waar de dreigingen voor de digitale veiligheid vanuit gaan

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

Bij het beeld dat organisaties hebben van de dreigingen voor de digitale veiligheid vallen een aantal zaken op:

- Organisaties onderschatten vaak de omvang van de IT en OT, de mate waarin deze gekoppeld zijn aan het internet en het belang ervan voor hun eigen organisatie. Hierdoor wordt ook het aanvalsoppervlak voor cyberaanvallen onderschat.
- Er zijn nog altijd organisaties die ervan uitgaan dat zij geen interessant doelwit zijn voor cybercriminelen. Buiten het feit dat dit een misvatting is, worden hierbij ook alle ongerichte cyberdreigingen over het hoofd gezien.
- De meer internationaal georiënteerde organisaties met grote economische waarde waar vooral ook intellectueel eigendom een belangrijke rol speelt, zijn meer risicobewust. Toch hebben deze organisaties vaak nog onvoldoende kennis in huis om de meer complexe dreigingen, geavanceerde aanvalsmethoden en recente kwetsbaarheden goed het hoofd te kunnen bieden.

Het beeld van de dreigingen en actoren die van invloed zijn op de digitale veiligheid van organisaties in de LSH-sector sluit aan bij het beeld dat door het NCSC is beschreven in het Cybersecuritybeeld Nederland[27]. In deze jaarlijkse monitor signaleert het 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-leveranciersketen.
4. Grootschalige uitval door natuurlijke oorzaken, technische oorzaken of onopzettelijke menselijke fouten waardoor één of meer processen in de samenleving worden verstoord.

Het NCSC geeft aan dat het aantal digitale incidenten dat de Nederlandse samenleving heeft getroffen de afgelopen jaren is gegroeid. De voortschrijdende digitalisering in vrijwel alle sectoren zorgt ervoor dat de digitale en de fysieke wereld steeds minder goed van elkaar zijn te onderscheiden. Dit geldt ook voor de organisaties in de LSH-sector waar de bedrijfsvoering vaak zeer afhankelijk is van IT-systemen (kantoor- en administratieve automatisering en aansturing van OT-systemen) en OT-systemen (productie- en logistieke automatisering).

Al met al zien we dat organisaties in de LSH-sector de relevante dreigingen voor de digitale veiligheid van hun organisatie onderschatten. Voor een deel van de organisaties komt dat doordat zij zichzelf ten onrechte niet zien als een geschikt doelwit voor cybercriminelen en daarbij tevens alle ongerichte dreigingen over het hoofd gezien. Voor een ander deel van de organisaties komt dat doordat zij de frequentie van de dreigingen en de kwetsbaarheid van hun organisatie hiervoor onderschatten. Het vergroten van het risicobewustzijn op het niveau van hoger management en bestuur en uitbreiden van beschikbare expertise voor de organisatie als geheel, kunnen hierbij een bijdrage leveren aan het maken van een reëlere inschatting van de relevante dreigingen voor de digitale veiligheid van de organisatie.

3.3 Potentiële impact

Uit de enquête en de volwassenheidsmetingen komt naar voren dat de deelnemende organisaties in belangrijke mate afhankelijk zijn van hun digitale systemen. De organisaties geven aan dat de incidenten die de beschikbaarheid of de integriteit van de IT-systemen aantasten al na enkele uren een grote impact kunnen hebben op de bedrijfsvoering. Verstoring van IT-systemen kan leiden tot omzetverlies, reputatieschade en het (deels) stilvallen van bedrijfsprocessen. Drie kwart van de organisaties geeft aan dat ook aantasting van de beschikbaarheid en integriteit van hun OT-systemen grote impact heeft voor de organisatie. Dit kan leiden tot niet of niet goed functioneren van gebruikte laboratoriumautomatisering en robotica, met als gevolg dat productie en logistieke processen (deels) stil komen te liggen.

Aantasting van vertrouwelijkheid van IT- en OT-systemen heeft vooral voor organisaties met waardevol intellectueel eigendom een grote invloed. In dit geval kan het uitlekken van gegevens, bijvoorbeeld als gevolg van bedrijfsspionage, geopolitieke spanningen, of statenlijke ambities, de concurrentiepositie schaden. Hiernaast kan aantasting van de vertrouwelijkheid van de systemen inbreuk vormen op vertrouwelijkheidsclausules in contracten met externe partijen waarvoor de organisatie aansprakelijk kan worden gesteld. Verder speelt voor alle organisaties uiteraard ook de mogelijkheid dat incidenten kunnen leiden tot verlies van persoonsgegevens waardoor niet wordt voldaan aan de privacywet (AVG).

Het beeld dat organisaties hebben van de impact van cyberincidenten is in de meeste gevallen vooral een gevoelskwestie, aangezien maar weinig organisaties adequaat gebruik maken van risicoanalyses. Twee derde van de respondenten, met name bij de kleinere organisaties, geeft aan dat niet voor alle kritische IT- en OT systemen risicoanalyses zijn uitgevoerd, of dat dit alleen incidenteel wordt gedaan.

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

Al met al zien we dat organisaties in de LSH-sector in belangrijke mate afhankelijk zijn van hun digitale systemen, maar dat ze de potentiële impact van aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van deze systemen door cyberincidenten onderschatten. Dit komt onder meer doordat ze niet of niet goed gebruik maken van risicoanalyses. Ook lijken de organisaties weinig aandacht te hebben voor de verwevenheid van de gebruikte IT- en OT-systemen en het feit dat verstoring van systemen kan doorwerken in andere systemen. Dit leidt tot een verdere onderschatting van de impact van cyberincidenten. Ook hier kan het vergroten van het risicobewustzijn op het niveau van hoger management en staf van de organisatie bijdragen aan een reëler beeld van de potentiële impact van cyberincidenten, waardoor meer urgentie ontstaat voor het op orde brengen van de digitale veiligheid van de organisatie. Anderzijds kan ook ondersteuning vanuit bijvoorbeeld het LBSP, bijvoorbeeld door het coördineren van samenwerking en kennisdeling tussen digitale veiligheidsspecialisten van organisaties op het gebied van digitale veiligheid, bijdragen aan een reëler beeld van de potentiële impact van cyberincidenten.

3.4 Niveau van digitale veiligheid

Een centraal onderdeel van het onderzoek vormde het in kaart brengen van het digitaal veiligheidsniveau van de deelnemende organisaties. Op basis van de enquête is voor de de organisaties globaal in kaart gebracht hoe ze de digitale veiligheid hebben ingericht. Hierbij is onder meer gevraagd naar de elementaire maatregelen voor de digitale veiligheid:

- Veilige instellingen.
- Uitvoeren van updates en patches.
- Beperken van toegangsrechten.
- Gebruik van antimalware.
- Regelmatig maken van back-ups.
- Gebruik van monitoring van netwerkverkeer.

Hiernaast is in de enquête gevraagd naar de mate waarin de organisaties voor hun van IT- en OT-systemen gebruik maken van een baseline voor digitale veiligheid, risicoanalyse, testen en audits. De resultaten zijn per organisatie weergegeven in tabel 3.3 en geven een indruk van het niveau van digitale veiligheid van deze organisaties.

Tabel 3.3: Overzicht van aspecten van de digitale veiligheid per organisatie (niet uitgevoerd (–), deels uitgevoerd (±), uitgevoerd (+))

Organisatie	Elementaire maatregelen	Baseline	Risicoanalyse	Testen	Auditen
Organisatie A	±	–	–	–	–
Organisatie B	–	–	–	–	+
Organisatie C	+	+	+	+	+
Organisatie D	±	+	–	–	–
Organisatie E	–	–	–	–	–
Organisatie F	±	+	+	+	+
Organisatie G	–	–	–	+	–
Organisatie H	–	–	+	–	–
Organisatie I	±	+	+	+	+

De tabel laat zien dat er aanzienlijke verschillen zijn in de digitale veiligheid van de deelnemende organisaties, maar ook enkele opvallende overeenkomsten. Eén uitzondering daargelaten, laten de uitkomsten zien dat de organisaties zelfs de elementaire maatregelen voor hun digitale veiligheid nog niet op orde hebben. Sommige organisaties claimen een baseline voor digitale veiligheid te hebben geïmplementeerd, of zelfs een managementsysteem voor digitale veiligheid (ISMS), maar dat is niet effectief als de elementaire maatregelen niet goed zijn gerealiseerd. Evengoed zijn risicoanalyse, testen en audits niet effectief als de organisatie geen gebruik maakt van een baseline voor de digitale veiligheid van de organisatie.

Volwassenheidsmeting

Bij twee organisaties die hebben deelgenomen aan de enquête is tevens een volwassenheidsmeting van de digitale veiligheid van deze organisaties uitgevoerd. Een belangrijke meerwaarde die dit bood ten opzichte van de enquête is dat de volwassenheidsmeting een gedetailleerder en genuanceerder beeld geeft van de organisatie van de digitale veiligheid in de betreffende organisaties.

Uit de metingen bleek dat beide organisaties beduidend lager scoorden voor de volwassenheid van de digitale veiligheid dan voor de betreffende organisaties mocht worden verwacht. Veel maatregelen ontbraken, wat de kans op incidenten aanzienlijk verhoogde. De organisaties stemden nog nauwelijks af over digitale veiligheid waardoor de digitale veiligheid vooral ad hoc werd ingevuld. De belegging van digitale veiligheid was niet goed geregeld, waardoor de beschermengel de belangrijkste speler voor de digitale veiligheid werd. Al met al was de kans op ernstige cyberincidenten onnodig hoog.

Uit de volwassenheidsmeting kwam naar voren dat beide organisaties hun digitale veiligheid beter moeten organiseren.

De voorgestelde verbeteringen betroffen:

- **De digitale veiligheid beter organiseren:**
  - Formuleer de ambities op het gebied van digitale veiligheid en communiceer dit naar de organisatie.
  - Realiseer voldoende personele capaciteit voor de digitale veiligheid en stel bijvoorbeeld een informatiebeveiligingsfunctionaris aan.
  - Maak duidelijke afspraken over de eisen op het gebied van digitale veiligheid met de persoon of organisatie die daar invulling aan moet geven.

- **De basismaatregelen voor digitale veiligheid op orde brengen:**
  - Stel een overzicht op van de interne en externe IT- en OT-systemen, met de instellingen, koppelingen, status, SLA's en wie de interne/externe beheerders ervan zijn.
  - Zorg voor een goed beheerde en beveiligde firewall tussen het interne netwerk en het internet.
  - Verbeter netwerksegmentering en scheid IT en OT.
  - Zorg voor netwerk monitoring om beveiligingsinbreuken vroegtijdig te signaleren.
  - Loop alle toegangsinstellingen van de IT en de OT na en corrigeer onveilige instellingen.
  - Zorg dat patching van de IT en de OT geregeld is, zodat alle systemen tijdig voorzien worden van de laatste beveiligingsupdates.
  - Loop alle afspraken over de informatievoorziening met externe partijen na, ook op het gebied van digitale veiligheid, pas deze zo nodig aan de eigen behoeften aan en zorg voor een goede registratie van de afspraken.
  - Loop alle back-upvoorzieningen na en voer regelmatige recovery-tests uit om zeker te stellen dat verloren data hersteld kan worden.

- **De toetsing van de digitale veiligheid regelen:**
  - Organiseer regelmatig een penetratietest door een externe partij om kwetsbaarheden in de IT en de OT op te sporen.
  - Organiseer regelmatig een interne audit door een ervaren auditor (niet de eigen IT-beheer- en informatiebeveiligingsfunctionaris).

Technische meting

Bij beide organisaties waar een volwassenheidsmeting van de digitale veiligheid is uitgevoerd, is ook een technische meting van de veiligheid van het IT-netwerk uitgevoerd. Deze meting heeft voor beide organisaties kritieke kwetsbaarheden in de IT-omgeving aangetoond, waardoor de organisaties zeer kwetsbaar zijn voor cyberaanvallen.
De belangrijkste bevindingen die bij beide organisaties naar voren kwamen, hadden betrekking op de volgende punten:

- **Netwerksegmentatie**
  De netwerksegmentatie bij beide organisaties was onvoldoende en vormde een risico voor de IT-beveiliging van de organisatie. In beide gevallen bleken er gevoelige OT-apparaten te zijn die niet voldoende van andere netwerksegmenten waren afgescheiden, zoals bijvoorbeeld gebouwbeheersystemen en labinstrumenten. Dit maakte de netwerken kwetsbaar voor aanvallen van niet-vertrouwde netwerken zoals het gastennetwerk of het open medewerkersnetwerk. Netwerksegmentatie is een belangrijke maatregel bij het reduceren van de impact van een cybersecurity-incident bijvoorbeeld door een ransomware-aanval.

- **Patchmanagement**
  De resultaten van de technische meting lieten ook zien dat het patchmanagement bij beide organisaties niet naar behoren was ingericht. Er werden bij beide organisaties een groot aantal diensten aangetroffen die onder een sterk verouderde versie actief waren. Bij beide partijen was de achterstand het grootst bij de OT-apparaten die door een externe partij werden beheerd.

- **Wachtwoordbeleid**
  Ten slotte bleek uit de scan ook dat het wachtwoordbeleid bij beide organisaties nog verbeterd kon worden. Zo werden er verschillende apparaten gevonden waarop kon worden ingelogd met standaard inloggegevens.

Een belangrijke factor in het ontstaan van deze problemen is dat beide organisaties onvoldoende duidelijke en sluitende afspraken hadden met hun externe IT-leveranciers. Dit resulteerde in een aantal situaties waarbij bepaalde services niet waren voorzien van updates, omdat de organisatie van mening was dat dit binnen het beheer van de externe leverancier viel. Bij navraag bleek echter dat dit onder de verantwoordelijkheid van de organisatie zelf viel en niet van de IT-leverancier. Door deze grijze gebieden zijn verschillende systemen uit beeld verdwenen en zijn deze niet voorzien van updates, standaard wachtwoorden niet gewijzigd en netwerken niet veilig gesegmenteerd.

Resumé

Samenvattend laten de enquête, de volwassenheidsmeting en de technische meting zien dat het niveau van digitale veiligheid van organisaties in de LSH-sector over de gehele linie moet worden verhoogd. Een belangrijk deel van de organisaties lijkt hierbij behoefte te hebben aan ondersteuning. De uitkomsten van het onderzoek laten zien dat digitale veiligheid in veel organisaties nog niet goed is georganiseerd en dat IT- en OT-systemen vaak nog onvoldoende veilig zijn ingericht. Het vergroten van expertise binnen de organisaties door middel van scholing of workshops, maar ook ondersteuning bij het inrichten van een managementsysteem voor digitale veiligheid kan een bijdrage aan het verbeteren ervan leveren.

4 Aanbevelingen

Op basis van de inzichten die volgen uit de vorige hoofdstukken doen we in dit hoofdstuk enkele aanbevelingen om de digitale veiligheid van organisaties in de LSH-sector te verbeteren. Hierbij richten we ons op (1) het verbeteren van het risicobewustzijn, (2) het vergroten van de expertise van de mensen die invulling moeten geven aan de digitale veiligheid van de organisaties en (3) het inrichten van ondersteuning aan organisaties in de LSH-sector voor de digitale veiligheid.

Verscheidene activiteiten die hieronder genoemd worden, kunnen geïnitieerd, gerealiseerd, of ondersteund worden door een centraal kennis- en ondersteuningspunt voor digitale veiligheid, bijvoorbeeld een sectoraal cyberweerbaarheidscentrum (CWC).

4.1.1 Risicobewustzijn verbeteren

Om het risicobewustzijn van hoger management en bestuur van organisaties in de LSH-sector te verbeteren, kunnen de volgende activiteiten worden ingezet:

1. **Zoek 'ambassadeurs' om het belang van digitale veiligheid uit te dragen:** Mensen kunnen vooral goed door 'gelijken' worden overtuigd om zaken anders te zien of anders aan te pakken. Mensen uit directie en management kunnen vooral goed worden overtuigd door andere directieleden en managers, ook vanuit andere vergelijkbare organisaties. Zoek naar mensen in het LBSP en de Medical Delta die overtuigd zijn van het belang om digitale veiligheid op te pakken en die anderen daarvan willen overtuigen.
2. **Organiseer risicobewustzijnsworkshops:** Door middel van korte workshops over de kenmerken en het belang van digitale veiligheid voor managers, stafmedewerkers en bestuurders, waar mogelijk toegespitst op de LSH-sector. Dit heeft tot doel om het risicobewustzijn met betrekking tot digitale veiligheid te vergroten en de mensen handelingsperspectieven te geven.

4.1.2 Expertise vergroten

Om de expertise op organisatieniveau te vergroten, kunnen de volgende activiteiten worden ingezet:

1. **Leg contact met cybersecurity-opleidingen in de regio:** de beschikbaarheid van expertise in de LSH-sector wordt bepaald door verschillende factoren, waaronder de instroom van nieuwe digitale veiligheidsprofessionals, de aansluiting tussen cybersecurity-opleidingen en de praktijk, bijscholing op het gebied digitale veiligheid voor professionals. In contact met cybersecurity-opleidingen in de regio kunnen bijvoorbeeld afspraken worden gemaakt over de inzet van stagiairs en afstudeerders en het inbrengen van sectorkennis in opleidingen.
2. **Spreek met relevante vakinhoudelijke opleidingen in de regio over een minimaal kennisniveau van digitale veiligheid voor afgestudeerden:** In veel mbo/hbo-laboratoriumopleidingen en wetenschappelijke opleidingen zoals geneeskunde en biomedische wetenschappen is nauwelijks aandacht voor digitale veiligheid. Vanuit de behoefte van de sector aan een minimaal kennisniveau van medewerkers op het gebied van digitale veiligheid kunnen mogelijkheden voor het aanbrengen van accenten in de curricula van relevante opleidingen in de regio worden verkend.
3. **Organiseer kennissessies en bijscholing op het gebied van digitale veiligheid:** Door middel van korte groepsgewijze kennissessies gericht op directie/management en bijscholing gericht op digitale veiligheidsspecialisten kan het kennisniveau op het gebied van digitale veiligheid van mensen die werkzaam zijn in de LSH-sector worden verhoogd.
4. **Organiseer workshops gericht op de elementaire digitale veiligheidsmaatregelen:** Voor organisaties op beginnersniveau kunnen workshops voor managers zich onder meer richten op een stappenplan voor het implementeren van de elementaire maatregelen voor digitale veiligheid. Voor meer gevorderde organisaties kan een workshop worden aangeboden voor digitaal veiligheidsspecialisten, 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.
5. **Ondersteun de inrichting van een managementsysteem voor de digitale veiligheid:** Bied een cursus aan waarin organisaties praktische handvatten wordt geboden voor het inrichten van een managementsysteem voor de digitale veiligheid van de organisatie.
6. **Ondersteun goed gebruik van risicoanalyse, monitoring, testen en audits:** Organiseer workshops voor digitale veiligheidsspecialisten gericht op de toepassingsmogelijkheden bij deze instrumenten en organiseer een aanbod van risicoanalysemethoden en van aanbieders van monitoring, testen en audits toegespitst op organisaties in de LSH-sector.

4.1.3 Ondersteuning inrichten

Om organisaties in de LSH-sector te ondersteunen bij het verbeteren van de digitale veiligheid kan worden gedacht aan de volgende activiteiten:

1. **Organiseer de beschikbaarheid van informatie over digitale veiligheid:** Actuele informatie over dreigingen, kwetsbaarheden en incidenten kan de slagkracht van organisaties vergroten. Dergelijke informatie wordt door specialistische organisaties aangeboden. Het distribueren van deze informatie kan bijvoorbeeld binnen het LBSP ingericht worden.
2. **Maak afspraken met aanbieders van dienstverlening op het gebied van risicoanalyse, testen en audits:** Maak afspraken met deze dienstverleners op het gebied van risicoanalysemethoden, testen en audits, toegespitst op organisaties in de LSH-sector.
3. **Organiseer samenwerking en kennisdeling tussen LSH-organisaties:** Vergelijkbare organisaties kampen vaak met vergelijkbare vraagstukken op het gebied van digitale veiligheid en kunnen profiteren van elkaars inzichten en ervaringen. Ook kan het delen van informatie over actuele dreigingen, kwetsbaarheden en incidenten in collectief verband bijdragen aan risicobewustzijn en organisaties beter voorbereiden op cyberincidenten.

5 Conclusie

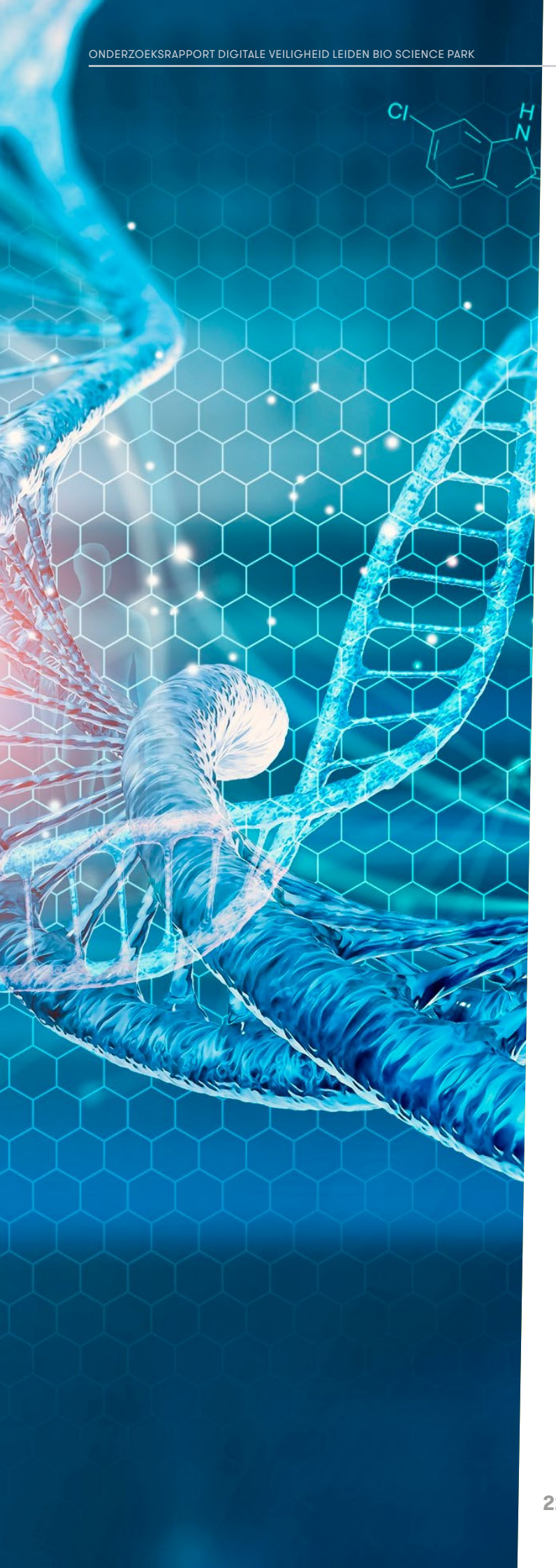
Dreigingslandschap
Het dreigingslandschap voor organisaties in de LSH-sector komt in belangrijke mate overeen met het dreigingslandschap dat geldt voor vitale sectoren in Nederland. Met de kanttekening dat een deel van de organisaties in de LSH-sector wordt gekenmerkt door hoog-innovatieve processen, een belangrijke rol voor intellectueel eigendom en internationale exposure. Dit maakt dit type organisatie een interessanter doelwit voor (bedrijfs)spionage, al dan niet door statelijke actoren of criminele organisaties. In het algemeen is ons beeld dat organisaties in de LSH-sector relevante dreigingen voor de digitale veiligheid van hun organisatie onderschatten. Voor een reëlere inschatting van het dreigingslandschap is het van belang dat het risicobewustzijn van bestuur, hoger management en staf wordt verhoogd en de beschikbare expertise binnen organisaties in de LSH-sector wordt uitgebreid.

Impact van cyberincidenten
Organisaties in de LSH-sector zijn in belangrijke mate afhankelijk van hun digitale systemen. Verstoring van IT- en OT-systemen leidt tot stilvallen van productie en logistieke processen, maar kan ook leiden tot aansprakelijkheidskwesties, reputatieschade, of verlies van concurrentiegevoelige data. Toch lijken de organisaties de impact van incidenten nog te onderschatten. Hierin speelt mee dat risicoanalyses vaak niet of niet goed worden gebruikt. Ook lijkt de invloed die de verwevenheid van de gebruikte IT- en OT-systemen heeft op mogelijke doorwerking van cyberincidenten onvoldoende te worden meegewogen. Voor een reëlere inschatting van de impact van cyberincidenten is het van belang dat het risicobewustzijn van bestuur, hoger management en staf wordt verhoogd en dat organisaties in de LSH-sector onderling informatie uitwisselen over actuele dreigingen, kwetsbaarheden en incidenten.

Niveau van informatiebeveiliging
Voor vrijwel alle deelnemende organisaties ligt er nog een opgave om het niveau van de digitale veiligheid te verbeteren. De uitkomsten van de enquête laten zien dat de meeste deelnemende organisaties zelfs de elementaire maatregelen voor de digitale veiligheid nog niet op orde hebben. Dit beeld wordt bevestigd door de volwassenheidsmetingen en technische metingen die voor dit onderzoek zijn uitgevoerd. Bovendien blijkt dat maar weinig organisaties gebruik maken van instrumenten zoals een beveiligingsbaseline, risicoanalyses en toetsing van de digitale veiligheid van de IT- en OT-systemen door middel van penetratietesten en audits.

Al met al wijzen de uitkomsten van dit onderzoek erop dat de deelnemende organisaties in de LSH-sector een lager niveau van digitale veiligheid hebben dan passend is.

De vraag hoe het gesteld is met de digitale veiligheid in de LSH-sector kan worden beantwoord met de constatering dat er voor organisaties in de sector nog de nodige stappen te zetten zijn om hun digitale veiligheid op een passend niveau te brengen. Het inzetten van ‘ambassadeurs’ voor digitale veiligheid, het geven van risicobewustzijnsworkshops, het maken van afspraken met relevante opleidingen in de regio over het verhogen van de basiskennis over digitale veiligheid, het aantrekken van meer specialisten op het gebied van digitale veiligheid en het inrichten van ondersteuning voor en samenwerking tussen organisaties met betrekking tot digitale veiligheid en het veilig inrichten van hun digitale systemen kunnen hierin een bijdrage leveren.



Bijlage 1: Enquête

Geachte heer/mevrouw,

In opdracht van Security Delta voeren de Hogeschool Leiden, de Haagse Hogeschool en Reqon gezamenlijk een onderzoek uit naar digitale veiligheid in de organisaties in het Bio Science Park Leiden. Met dit onderzoek brengen we in kaart hoe het is gesteld met de digitale veiligheid in deze organisaties en in hoeverre deze verbeterd zou moeten worden.

In het onderzoek kijken we niet alleen naar de veiligheid van de IT, ofwel de informatietechnologie (denk aan kantoorautomatisering, administratieve automatisering, cloud-functies en netwerken), maar ook naar de veiligheid van de OT, ofwel de operationele technologie (denk aan automatisering van fysieke processen en systemen, zoals productie, logistiek, opslag, verpakking, etc.).

Wij willen u vragen om mee te werken aan dit onderzoek. Het onderzoek is volledig anoniem en de verwerking van de data voldoet uiteraard aan hoge veiligheidsstandaarden. Het invullen van de enquête neemt ongeveer 15 minuten in beslag. Wij ontvangen uw reactie graag uiterlijk vrijdag 13 mei 2022.

De uitkomsten van de enquête zijn niet herleidbaar tot personen of organisaties, en worden gebruikt in de onder-zoeksrapportage om uitdagingen en oplossingsrichtingen voor het verbeteren van digitale veiligheid in het Bio Science Park Leiden inzichtelijk te maken.

Organisaties die geïnteresseerd zijn kunnen zich aan het einde van de enquête aanmelden voor (1) een kosteloze volwassenheidsmeting voor de organisatie van de digitale veiligheid en/of (2) een meting van de technische veiligheid van uw netwerk.

Wij hopen op uw medewerking,
dr. Marcel Spruit, Lector Cyber Security and Safety,
dr. Emiel Kerpershoek, Senior Onderzoeker Cybersecurity,

Vragen

1. Onder welke branche/sector valt uw organisatie? *[Open vraag]*

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

3. Hoeveel werknemers heeft de vestiging waar u werkzaam bent? *[Open vraag]*

4. Hoe groot is de maximale impact als één of meer **IT-systemen** van uw organisatie (denk aan kantoorautomatisering, administratieve systemen, IT-netwerk, pc's, cloud-systemen, e.d.) 1 uur/1 dag/1 week niet beschikbaar zijn, verkeerd functioneren, of gegevens lekken? *[Open vraag]*

5. Indien uw organisatie gebruik maakt van **OT-systemen** (denk aan automatisering van machines, logistieke automatisering, robots, drones, etc.), hoe groot is dan de maximale impact als één of meer van deze OT-systemen 1 uur/1 dag/1 week niet beschikbaar zijn, verkeerd functioneren, of gegevens lekken? *[Open vraag]*

6. Voor welke doeleinden maken uw IT-systemen en/of OT-systemen gebruik van het internet?
   [Meerdere antwoorden mogelijk: Voor beheer op afstand / Voor clouddienstverlening / Voor gegevensuitwisseling / Niet / Weet ik niet / Anders, namelijk: …]

7. In hoeverre is het beheer van uw IT- en OT-systemen uitbesteed?
   [Alle IT en OT / Een deel van de IT en OT / Niet / Weet ik niet / Anders, namelijk: …]

8. Zijn er met de IT- en/of OT-leveranciers expliciet afspraken gemaakt over, of normen gesteld aan digitale veiligheid?
   [Alle leveranciers / Een deel van de leveranciers / Nee / Weet ik niet]

9. Welk rapportcijfer (1 – 10) geeft u de digitale veiligheid van uw organisatie op dit moment? *[Cijfer 1..10]*

10. Heeft uw organisatie de volgende beveiligingsmaatregelen getroffen?

    a. Het implementeren van veilige instellingen op alle apparatuur, software, netwerk en internetverbindingen
       [Alle systemen / Meeste systemen / Sommige systemen / Niet / Weet ik niet]

    b. Het regelmatig en tijdig implementeren van alle software- en beveiligingsupdates
       [Alle systemen / Meeste systemen / Sommige systemen / Sommige updates / Niet / Weet ik niet]

    c. Het beperken van de toegangsrechten tot systemen voor de eigen medewerkers en externe partijen, alsook het afdwingen ervan met behulp van multifactor authenticatie en autorisatie
       [Alle systemen / Meeste systemen / Sommige systemen / Alleen voor internen / Alleen voor externen / Niet / Weet ik niet]

    d. Het voorkomen van virussen en andere malware
       [Alle systemen / Meeste systemen / Sommige systemen / Niet / Weet ik niet]

    e. Maakt uw organisatie gebruik van monitoring van het netwerk om verdacht netwerkverkeer tijdig te kunnen detecteren?
       [Ja / Externe partij / Nee / Weet ik niet]

    f. Het regelmatig maken van back-ups van alle belangrijke gegevens en software en deze offline opslaan
       [Alle systemen / Meeste systemen / Sommige systemen / Online / In de cloud / Niet / Weet ik niet]

    g. Het compartimenteren van het netwerk om de reikwijdte van malware en penetraties te beperken
       [Ja / Enigszins / Niet / Weet ik niet]

11. Maakt uw organisatie gebruik van een standaard baseline voor de digitale veiligheid?
    [Ja / Nee / Weet ik niet]

12. Worden in uw organisatie voor alle kritische IT- en OT-systemen risicoanalyses uitgevoerd?
    [Periodiek / Incidenteel / Bij aanschaf / Nee / Weet ik niet]

13. Worden er voor uw organisatie testen uitgevoerd om zwakke plekken in de digitale veiligheid van uw organisatie op te sporen?
    [Meerdere antwoorden mogelijk: Penetratietesten / Social engineering testen / Red team testen / Andere testen / Nee / Weet ik niet]

14. Wordt de digitale veiligheid van uw organisatie geaudit?
    [Meerdere antwoorden mogelijk: Periodiek / Incidenteel / Nee / Weet ik niet]

Als deelnemer aan dit onderzoek bieden we uw organisatie kosteloos een volwassenheidsmeting voor de organisatie van de digitale veiligheid aan, alsook een meting van de technische veiligheid van uw netwerk.
Indien u geïnteresseerd bent in één van beide metingen, of allebei de metingen, dan kunt u dit aangeven in een mail aan **e.f.p.kerpershoek@hhs.nl.**

Hartelijk dank voor uw medewerking!

Bijlage 2: Interviewprotocol

Onderstaande vragen worden gebruikt bij de interviews van functionarissen uit de organisatie waarvoor het volwassenheidsniveau van de organisatie van de digitale veiligheid wordt bepaald.

De vragen zijn open vragen. De interviews worden afgenomen door ter zake deskundige interviewers. Voor veel vragen is het nodig om door te vragen om zeker te stellen dat de vraag goed is begrepen en met voldoende nuance is beantwoord.

Om kleuring door ondeskundigheid, bias en vooringenomenheid zoveel mogelijk te voorkomen, worden de interviews bij voorkeur separaat uitgevoerd met verschillende functionarissen, namelijk:

- iemand uit het management, bijvoorbeeld de CIO;
- iemand die de beveiliging van de automatisering goed kent;
- iemand die niet werkzaam is in een IT-, OT- of beveiligingsfunctie.

Vanzelfsprekend kan ieder van deze functionarissen andere ter zake deskundige collega's meenemen om de vragen vollediger en met meer nuance te kunnen beantwoorden.

De organisatie

1. In welke branche/sector valt uw organisatie?

2. Wat zijn de belangrijkste producten en/of diensten die uw organisatie levert?

3. Hoeveel werknemers heeft uw organisatie?

4. Over hoeveel vestigingen is de organisatie verdeeld?

5. Hoeveel werknemers werken op de vestiging waar u werkt?

6. Heeft uw organisatie één of meer functionarissen voor de digitale veiligheid?
   Zo ja, hoeveel (in fte)?
   Maakt één van deze functionarissen deel uit van directie/managementteam?
   Zo nee, rapporteert één van deze functionarissen direct aan directie/managementteam?

7. Is er voor uw vestiging een jaarlijks budget beschikbaar specifiek voor de digitale veiligheid?
   Zo ja, hoe groot is het budget?

8. Maakt de digitale veiligheid deel uit van de planning & control cyclus?
   Zo ja, waar blijkt dat uit?

Uw functie

9. Welke functie(s) bekleedt u in uw organisatie?
   Bent u lid van directie/managementteam?
   Zo nee, rapporteert u direct aan directie/managementteam?

10. In welke mate bent u betrokken bij digitale veiligheid in uw organisatie?

De automatisering

11. Gebruikt uw organisatie automatisering voor het aansturen of monitoren van een maatschappelijk vitaal proces?

12. Heeft u inzicht in de systemen waaruit de automatisering bestaat en de koppelingen die ze hebben, onderling en met het internet?
    Is hiervan een schematisch overzicht?

13. Wat is de maximale impact als één of meer IT-systemen van uw organisatie (denk aan kantoorautomatisering, administratieve systemen, IT-netwerk, pc's, cloud-systemen, e.d.) niet beschikbaar zijn, verkeerd functioneren, of gegevens lekken?
    Bij welke uitvalsduur en/of reikwijdte van verkeerd functioneren of gegevens lekken manifesteert deze impact zich?

14. Maakt uw organisatie naast de IT ook gebruik van operationele technologie (OT), denk aan automatisering van machines, logistieke automatisering, robots, drones, etc.?
    Zo ja, waarvoor worden OT-systemen gebruikt?
    Worden OT-systemen op afstand (via het internet) gemonitord en/of bestuurd?
    Zijn de netwerken voor IT-systemen en OT-systemen fysiek en/of logisch van elkaar gescheiden?

15. Wat is de maximale impact als één of meer OT-systemen van uw organisatie niet beschikbaar zijn, verkeerd functioneren, of gegevens lekken?
    Bij welke uitvalsduur en/of reikwijdte van verkeerd functioneren of gegevens lekken manifesteert deze impact zich?

16. In hoeverre is het beheer van de IT- en OT-systemen uitbesteed?
    Maakt uw organisatie gebruik van cloud-diensten, of levert ze cloud-diensten?

17. Is de digitale veiligheid van nieuw te bouwen of aan te schaffen IT- en OT-systemen vanaf het begin al een vast bespreekpunt (security-by-design en privacy-by-design)?

18. Is uw organisatie de afgelopen twee jaren getroffen door één of meer ernstige incidenten op het gebied van digitale veiligheid?

Volwassenheid digitale veiligheid

19. Waar ligt in uw organisatie de verantwoordelijkheid voor digitale veiligheid?
    Geldt dit voor zowel de IT als de OT?
    En op welke manier blijkt de betrokkenheid van de directie?
    Hoe vaak is de digitale veiligheid een bespreekpunt voor de directie?

20. In hoeverre maakt u zich zorgen over mogelijke incidenten op het gebied van digitale veiligheid in uw organisatie?

21. Heeft de organisatie een beleid voor digitale veiligheid, bijvoorbeeld een informatiebeveiligingsbeleid?
    En is dit beleid voldoende bekend bij alle werknemers?

22. Is voor elk (kritisch) proces, systeem en dataverzameling bekend wie de 'eigenaar' is?
    Geldt dit ook voor de OT-systemen?

23. Weten de verantwoordelijken voor digitale veiligheid van elkaar wie waarvoor verantwoordelijk is?
    Zo ja, hoe is dat geregeld?
    En als één van deze mensen tijdelijk is uitgeschakeld, worden diens taken dan overgenomen?

24. Op welke wijze worden medewerkers bewust gemaakt van het belang van digitale veiligheid en de van hun gevraagde inzet?

25. Als een medewerker een beveiligingsincident constateert, moet deze dan gemeld worden?
    Zo ja, aan wie?
    Geldt dit ook voor minder veilige of verdachte omstandigheden op de werkvloer of onverwacht of ongewenst gedrag in de automatisering?

26. Heeft de organisatie een calamiteitenplan/continuïteitsplan voor de primaire processen?
    Zo ja, hoe volledig en actueel is het, hoe vaak worden er calamiteitenoefeningen gedaan en in hoeverre dekt het plan IT- en OT-calamiteiten?

27. Heeft de organisatie elementaire beveiligingsmaatregelen getroffen voor de IT en, voor zover van toepassing, de OT? Het betreft onder meer:

    a. Het implementeren van veilige instellingen op alle apparatuur, software, netwerk en internetverbindingen.

    b. Het regelmatig en tijdig implementeren van alle benodigde software- en beveiligingsupdates.

    c. Het beperken van de toegangsrechten tot systemen voor de eigen medewerkers en externe partijen, alsook het controleren en afdwingen ervan.

    d. Het voorkomen van virussen en andere malware.

    e. Het regelmatig maken van back-ups van alle belangrijke gegevens en software en deze (ook) offline opslaan.

    f. Het compartimenteren van het netwerk om het verspreiden van malware en penetraties te beperken.

    g. Het monitoren van de kritische systemen en het interne netwerk om beveiligingsinbreuken vroegtijdig te signaleren.

    h. Het maken van expliciete afspraken met de IT- en/of OT-leveranciers en relevante ketenpartners over digitale veiligheid.

28. Maakt uw organisatie gebruik van een gecontroleerd basisniveau (baseline) voor digitale veiligheid?
    Zo ja, is dit gebaseerd op een externe standaard of baseline (bijv. ISO 27002, BIO, IEC 62443)?
    Geldt deze ook voor de OT?
    In welke mate is het basisniveau geïmplementeerd?

29. Worden risicoanalyses uitgevoerd voor de kritische IT- en OT-systemen?
    Hoe vaak worden deze analyses geactualiseerd?
    Wanneer is de laatste risicoanalyse voor een kritisch systeem uitgevoerd?
    Wordt er na een risicoanalyse een gap-analyse uitgevoerd en bijgehouden?
    Wie autoriseert de risico- en gap-analyses voor kritische systemen?

30. Worden regelmatig penetratietests en/of andere tests uitgevoerd?

31. Wordt regelmatig een self-assessment uitgevoerd op het geïmplementeerde niveau van digitale veiligheid (door een IT-auditor en niet alleen door een accountant)?

32. Wordt (een deel van) de IT en/of de OT van uw organisatie regelmatig (bijv. jaarlijks) geaudit en/of getest?
    Zo ja, gebeurt dit door, of in opdracht van, een externe toezichthouder?
    Is de toetsing ten behoeve van een certificatie gedaan (bijv. ISO 27001)?
    Maakt de OT deel uit van de audit?
    Wanneer heeft de laatste audit plaatsgevonden?
    Wanneer heeft de laatste penetratietest plaatsgevonden?
    In hoeverre zijn de aanbevelingen uit de audits en testen geïmplementeerd?

33. Maakt uw organisatie gebruik van een standaard op het gebied van digitale veiligheid of risicomanagement (bijv. COSO, ISO 27001, ISO 27005)?
    Zo ja, welke is/zijn dit en in welke mate is/zijn deze geïmplementeerd?
    In welke mate wordt dit gecontroleerd?
    Is er sprake van een Information Security Management System?

34. Zijn er nog zaken die voor het onderzoek relevant kunnen zijn en nog niet aan bod zijn geweest?

Hartelijk dank voor uw medewerking.

Adres- en contactgegevens

Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl