Centre of Expertise
Veiligheid & Veerkracht
Een initiatief van avans

Onderzoeksrapportage

Evaluatie pilot ‘MKB Cyberassistentie’

Centre of Expertise Veiligheid & Veerkracht – Avans Hogeschool

Esger ten Thij, Renske Korenromp en Rick van der Kleij

Maart 2025

Samenvatting

Het MKB ervaart regelmatig barrières bij het verbeteren van hun digitale veiligheid. De beperkte kennis en middelen, gecombineerd met het idee dat zij minder aantrekkelijk zijn voor cybercriminelen, zorgen ervoor dat deze bedrijven hun digitale veiligheid vaak onvoldoende prioriteit geven. Dit leidt niet alleen tot verhoogde risico's voor de betreffende ondernemingen, maar vormt ook een bedreiging voor de gehele keten waarbinnen zij opereren.

Om de digitale veiligheid van het mkb te vergroten heeft het Cyber Weerbaarheidscentrum Brainport (CWB) ondersteuning beschikbaar gesteld door een cybersecurityprofessional. Bedrijven konden tegen gereduceerd tarief gebruikmaken van 50 uur aan ondersteuning. Dit evaluatieonderzoek, gecoördineerd door het CWB en uitgevoerd door het lectoraat Cyberweerbare Organisaties van Avans Hogeschool, richtte zich specifiek op de effectiviteit van de geboden ondersteuning en de gedragsbepalers voor ondernemers om te investeren in hands-on ondersteuning door een cybersecurityprofessional.

De effectiviteit van de geboden ondersteuning is beoordeeld aan de hand van een literatuurstudie en interviews met zowel deelnemers aan de pilot als cybersecurity-professionals betrokken bij de uitvoering. Gedragsbepalers zijn in kaart gebracht via een focusgroep met mkb-ondernemers. Ondernemers hebben de pilot overwegend positief gewaardeerd. De praktische ondersteuning werd als waardevol ervaren, vooral omdat de ondernemers zelf vaak onvoldoende kennis en financiële middelen hebben om zelfstandig effectieve maatregelen te kunnen treffen. De beschikbaar gestelde ondersteuning van 50 uur bleek voldoende om concrete maatregelen te realiseren. Dit heeft geleid tot een professionalisering van het cyberweerbaarheidsniveau binnen de deelnemende bedrijven.

Een belangrijk aandachtspunt gedurende de pilot was de communicatie tussen de mkb-ondernemer en de cybersecurityprofessional, die een bepalende factor bleek voor zowel de successen als de ervaren uitdagingen. De aangeboden menukaart, waarin maatregelen opgenomen waren waaruit de bedrijven hun ondersteuning konden kiezen, kreeg een wisselende beoordeling. Hoewel ondernemers de menukaart overzichtelijk vonden, gaven zij aan dat het aanbod onvoldoende aansloot bij hun specifieke situatie. Hierdoor ontstond regelmatig behoefte aan maatwerk buiten het standaardaanbod om.

Uit de focusgroepen, vanuit gedragsmatig perspectief, blijkt dat mkb-ondernemers vooral gemotiveerd worden om te investeren in digitale veiligheid door begrijpelijke communicatie, concrete praktijkvoorbeelden en laagdrempelige ondersteunings-mogelijkheden zoals vouchers en subsidies. Tegelijkertijd wordt de urgentie van cyberrisico's vaak onderschat, totdat zich daadwerkelijk een incident voordoet. Dit vermindert de bereidheid om proactief te investeren in cybersecuritymaatregelen. Een belangrijke aanbeveling die wij doen is om voor toekomstige cybersecurity-initiatieven een duidelijke en toegankelijke communicatie- en adviesstrategie te ontwikkelen, met praktijkgerichte uitleg en visuele ondersteuning.

Inhoudsopgave

Samenvatting *3*

1. Inleiding *5*

1.1 Aanleiding 5

1.2 Organisatie van het onderzoek 5

2. Methoden van onderzoek *6*

2.1 Literatuuronderzoek 6

2.2 Semigestructureerde interviews 6

2.3 Focusgroep 6

3. De menukaart *7*

3.1 Mens 7

3.1.1 Awareness programma 7

3.2 Proces 8

3.2.12 Netwerksegmentatie 11

3.3 Technologie 11

4. Semigestructureerde interviews *12*

5. Focusgroep *14*

5.1 Methode 14

5.2 Theoretisch kader 15

5.3 Resultaten 17

6. Conclusie *20*

6.1 Effectiviteit van de ondersteuning 20

6.2 gedragsbepalers 21

6.3 Concluderend 22

7. Aanbevelingen *23*

7.1 Verbeteren van de Communicatie en Taalgebruik 23

7.2 Herstructurering van de menukaart naar een evenwichtig en maatwerkgericht aanbod . 23

7.3 Verhogen van het bewustzijn en de beschikbaarheid van ondersteuningsinitiatieven 23

7.4 Concreet onderbouwen van de waarde en effectiviteit van cybermaatregelen 24

7.5 Stimuleren van samenwerking en netwerken tussen ondernemers 24

7.6 Verhogen van het Urgentiebesef en Risicobewustzijn 24

Bibliografie *25*

1. Inleiding

1.1 Aanleiding

Cybersecurity is een groeiende uitdaging voor bedrijven, vooral in de hightech maakindustrie, waar de keten slechts zo sterk is als de zwakste schakel. Kleinere bedrijven in deze sector hebben vaak minder financiële middelen en kennis om hun digitale weerbaarheid te versterken[1]. Daarnaast bestaat er bij mkb-ondernemers vaak de misvatting dat zij minder interessant zijn voor cybercriminelen. Tegelijkertijd vertrouwen zij relatief vaker dan grootbedrijven op IT-dienstverleners die niet altijd over voldoende cyberexpertise beschikken. Dit leidt tot kwetsbaarheden die niet alleen deze bedrijven zelf treffen, maar ook risico's creëren voor grotere bedrijven in de keten.

Om deze uitdagingen aan te pakken en de keten weerbaarder te maken, heeft het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) een pilot[2] gesubsidieerd die gericht is op het vergroten van de cyberweerbaarheid van mkb-bedrijven. Deze pilot, voortbouwend op de inzichten uit eerder onderzoek (Kokkeler, van den Oord, ten Thij, & Vollenberg, 2023), wordt gecoördineerd door het Cyber Weerbaarheidscentrum Brainport (CWB). Het CWB heeft Avans Hogeschool gevraagd om onderdelen van de pilot te evalueren, met een specifieke focus op de effectiviteit van de geboden ondersteuning en gedragsbepalers voor ondernemers om te investeren in hands-on ondersteuning door een cybersecurityprofessional. Gedragsbepalers zijn interessant omdat deze inzicht bieden in hoe mkb'ers geactiveerd kunnen worden om hun cyberweerbaarheid te versterken.

1.2 Organisatie van het onderzoek

Het onderzoek werd uitgevoerd in samenwerking tussen het Cyber Weerbaarheidscentrum Brainport en het Avans lectoraat Cyberweerbare Organisaties met medewerking van Cyber4Z en individuele cyberprofessionals. De volgende onderzoeksvragen stonden centraal in dit onderzoek:

1. Waarom willen ondernemers wel of niet geholpen worden met hun cyberweerbaarheid?
2. Wat zijn de voorwaarden voor succesvolle hands-on ondersteuning door een cybersecurity professional?
3. Hoe effectief zijn de vormen van geboden ondersteuning (de 'menukaart') en hoe verhoudt zich dit tot de ondersteuningsbehoefte die de mkb'er heeft?
4. Hoe verhoudt de effectiviteit zich tot de inzet in tijd die wordt gepleegd door de deelnemende mkb'er?
5. In welke mate speelt het hebben van een eigen IT-dienstverlener een rol in de effectiviteit van de pilot?
6. Wat is het effect van de ondersteuning door een cybersecurityprofessional *grosso modo*?
7. Hoe duurzaam is het resultaat van de pilot in termen van cyberweerbaarheid?
8. Welke aanbevelingen kunnen worden geformuleerd voor het aanbieden van ondersteuning aan het mkb?
9. Welke aanbevelingen kunnen worden geformuleerd voor de verdere opschaling en implementatie elders van de blauwdruk?

[1] https://innvolve.nl/blog/wat-kost-cybersecurity/

[2] De pilot wordt gesteund door de programmaraad Cyber Oost-Brabant. Daarin zitten vertegenwoordigers van het openbaar bestuur (de burgemeesters van Meierijstad en Best), het Openbaar Ministerie, de politie en de 2 Veiligheidsregio's in Oost-Brabant. Verder wordt het project gesteund door het Digital Trust Centre (DTC) en EDIH-SNL.

Om antwoord te geven op deze vragen is het onderzoek verdeeld in drie delen met een looptijd van 1 jaar. De eerste maanden is er gefocust op de literatuurstudie rondom de menukaart en het benaderen van focusgroepen. Vervolgens is er een focusgroep georganiseerd om antwoord te geven op de eerste deelvraag en zijn er interviews afgenomen om antwoord te geven op de overige deelvragen. De laatste maanden van de pilot zijn gebruikt om het rapport af te ronden. In het volgende hoofdstuk zal dieper ingegaan worden om deze verschillende onderdelen.

2. Methoden van onderzoek

Voor dit onderzoek is ervoor gekozen om gebruik te maken van een samenhangend pakket van kwalitatieve methoden. Het rapport kan onderverdeeld worden in drie onderdelen. Een evaluatie van de maatregelen op de 'menukaart' die wordt gebruikt in de pilot door de cyberprofessionals, een focusgroep met mkb'ers over gedragsbepalers onderbouwd door een literatuurstudie en interviews afgenomen met ondernemers en de cyberprofessionals om zo een beeld te krijgen van de effectiviteit van de pilot.

2.1 Literatuuronderzoek

Er is begonnen met het uitvoeren van twee literatuuronderzoeken. Het eerste literatuuronderzoek heeft gekeken naar de maatregelen waaruit deelnemers konden kiezen om hun cyberweerbaarheid te versterken zoals aangeboden via de 'menukaart'. Het tweede literatuuronderzoek is gebruikt om stellingen te bepalen over gedragsbepalers die gebruikt zijn in de focusgroep.

2.2 Semigestructureerde interviews

Om te bepalen hoe bedrijven en professionals de pilot hebben ervaren zijn er in totaal zeven interviews afgenomen: vijf interviews met bedrijven, waarvan er vier de pilot hadden afgerond en één aan het begin van het proces zat. Verder zijn er twee interviews afgenomen met ondersteunende professionals. De interviews zijn online afgenomen aan de hand van een voorop vastgestelde vragenlijst die gekoppeld is aan de deelvragen. Afhankelijk van de beschikbaarheid van de onderzoekers zijn de interviews individueel of in tweetallen afgenomen. Met de semigestructureerd interviews is getracht antwoord te geven op deelvraag 2 t/m 7.

2.3 Focusgroep

Voor dit onderzoek is een kwalitatieve onderzoeksmethode gekozen met als doel inzicht te krijgen in de gedragsbepalers die de bereidheid van mkb-ondernemers beïnvloeden om te investeren in ondersteuning voor het vergroten van hun cyberweerbaarheid. Gezien de exploratieve aard van de onderzoeksvraag is een focusgroep als methode gekozen, omdat deze methode inzichten biedt in de ervaringen en percepties van mkb-ondernemers. Met de focusgroep is getracht antwoord te geven op de vraag; "Onder welke voorwaarden ondernemers in het mkb bereid zijn om tijd en geld te besteden aan ondersteuning in welke vorm dan ook?"

3. De menukaart

In de huidige digitale wereld is het beschermen van informatie en systemen tegen cyberdreigingen een steeds complexer vraagstuk, dat niet alleen technische, maar ook organisatorische en menselijke aspecten omvat. Het is essentieel om te begrijpen hoe cybersecuritymaatregelen effectief kunnen worden geïmplementeerd en welke componenten (mens, proces, technologie) hierbij een rol spelen. Om de effectiviteit van de maatregelen te beoordelen, is het van belang een holistische benadering te hanteren, die rekening houdt met zowel technische als niet-technische factoren.

Wetenschappelijke studies bevestigen dat de effectiviteit van cybersecuritymaatregelen vaak afhankelijk is van de interactie tussen de drie componenten zoals hierboven reeds genoemd. Waarbij gesteld wordt dat bijvoorbeeld alleen technologische maatregelen niet voldoende zijn zonder de juiste organisatorische processen en gemotiveerde gebruikers (Humayun, Akhtar & Iqbal, 2020). Vanuit dit kader is gekeken naar de menukaart met maatregelen zoals die is gebruikt in de pilot. Hierbij is gelet op balans tussen de drie componenten zoals hierboven genoemd, en of er wellicht maatregelen zijn die ontbreken of onderbelicht zijn. Het toepassen van dit kader kan leiden tot gerichte aanbevelingen om de balans tussen deze factoren te verbeteren en ondernemers bij het opschalen van de pilot een meer complete en effectieve menukaart aan te bieden.

3.1 Mens

3.1.1 Awareness programma

Maatregel: Presentatie van een awareness programma voor personeel.
Categorie: Mens
Effectiviteit: Bewustwordingsprogramma's zijn essentieel om medewerkers te trainen in veilige gedragspatronen, maar hun effectiviteit verschilt sterk afhankelijk van de implementatie[3]. Studies tonen aan dat eenmalige sessies een beperkte impact hebben op lange termijn gedrag (Bada, Sasse, & Nurse, 2019). Echter, wanneer trainingen interactief zijn en gebruik maken van scenario-gebaseerde simulaties, verbeteren ze het vermogen van medewerkers om phishing pogingen en andere aanvallen te herkennen (Pattinson, Patel & Lacey, 2012). Regelmatige herhaling en integratie met technische maatregelen versterken de effectiviteit. Een goede handleiding voor awareness campagnes is onlangs gepubliceerd door het NCSC: Voorbij de e-learning, met daarin leidende principes waarmee je veilig digitaal gedrag van medewerkers in organisaties bevordert.[4]

3.1.2 Phishing simulatie of walk-in test

Maatregel: Rapport met bevindingen en advies
Categorie: Mens
Effectiviteit: Phishing simulaties worden vaak gebruikt om werknemers te trainen in het herkennen van phishing aanvallen. De effectiviteit ervan wordt recentelijk echter openlijk in twijfel getrokken. De Gemeente Den Haag heeft hierom het gebruik ervan verboden.[5] Volgens Wright en Marett (2017) is een phishing simulatie effectief bij herhaalde blootstelling, maar de impact neemt af als follow-uptraining ontbreekt. Bada e.a. (2019) stellen dat motivatie cruciaal is: werknemers die geen directe gevolgen

[3] https://www.digitaltrustcenter.nl/stappenplan-cyberbewustwordingscampagne
[4] https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/besturen/voorbij-de-elearning
[5] https://www.binnenlandsbestuur.nl/digitaal/gemeente-den-haag-heeft-phishingtest-verboden

ervaren van verkeerde keuzes, veranderen hun gedrag niet duurzaam. Een combinatie met beloningen of negatieve prikkels (bijvoorbeeld herhaalde reminders) verhoogt de effectiviteit. Toch waarschuwen Bada e.a. (2015) en Jansson en von Solms (2013) dat overmatig gebruik van phishing simulaties kan leiden tot weerstand bij medewerkers, vooral als zij de simulaties als straf ervaren. Dit benadrukt de noodzaak van een evenwichtige aanpak, waarbij zowel gedragsverandering als werkplezier wordt gestimuleerd.

Walk-in tests (of mystery guest visits), waarbij medewerkers fysiek worden getest door een externe partij die zich bijvoorbeeld voordoet als een klant of collega, hebben ook bewezen effectief te kunnen zijn voor het versterken van beveiligingsbewustzijn en het bevorderen van gewenst gedrag in de praktijk. Deze tests hebben de mogelijkheid om medewerkers in hun natuurlijke omgeving te evalueren, wat vaak tot betere resultaten leidt dan standaard gesimuleerde tests (D'Arcy, Hovav & Galetta, 2014). De onvoorspelbaarheid en de onverwachte aard van deze tests kunnen helpen om medewerkers alert te houden en hen aan te moedigen om meer verantwoordelijk om te gaan met de beveiliging. Echter, zoals Herath en Rao (2009) aangeven, kan de effectiviteit van zulke tests afhangen van het doel en de frequentie van de testen. Wanneer medewerkers zich bewust worden van het feit dat ze regelmatig worden getest, kan hun motivatie verminderen en kan het effect van de tests verwateren. Bovendien is het cruciaal dat er gevolgen verbonden zijn aan de reacties van medewerkers tijdens de walk-in test, zoals directe feedback of training, om duurzame gedragsverandering te realiseren (Bada e.a., 2019).

3.1.3 Analyse en opvolging dreigingsinformatie (educatie met MISP)

Maatregel: Educatie rondom het identificeren en behandelen van dreigingen waarbij het Malware Information Sharing Platform (MISP) als bron wordt aangehouden.
Categorie: Mens (met proces-component)
Effectiviteit: MISP (Malware Information Sharing Platform) is een open-source platform voor het verzamelen, opslaan, distribueren en delen van cyberbeveiligingsindicatoren en dreigingsinformatie. Het is ontworpen om analisten, beveiligingsprofessionals en ICT-specialisten te ondersteunen bij hun dagelijkse werkzaamheden door gestructureerde informatie efficiënt te delen (MISP-project, z.d.). Het integreren van dreigingsinformatie in operationele processen verhoogt de responsiviteit van organisaties (Kammüller, Probst, & Lundqvist, 2018). Educatie is effectief als deze wordt gekoppeld aan praktische toepassingen, zoals het monitoren van specifieke dreigingen in tools als MISP. Zonder voortdurende ondersteuning kan kennis echter snel verouderen (Zhang, Guo & Wang, 2018).

3.2 Proces

3.2.1 Intellectual Property Rights

Maatregel: Procedure voor bescherming van intellectueel eigendom.
Categorie: Proces (met mens-component)
Effectiviteit: Bescherming van intellectueel eigendom vereist niet alleen technische maatregelen zoals encryptie, maar ook organisatorische en juridische waarborgen. Gollin (2018) benadrukt dat procedures effectiever zijn als medewerkers worden getraind in het herkennen van risico's en als sancties duidelijk zijn gedefinieerd.

3.2.2 Opstellen Informatiebeveiligingsbeleid

Maatregel: Het opstellen van een IB-beleid.
Categorie: Proces
Effectiviteit: Het opstellen van een informatiebeveiligingsbeleid biedt een structureel kader voor de implementatie van beveiligingsmaatregelen en helpt risico's te minimaliseren (Humayun e.a., 2020). Het beleid creëert de gelegenheid voor

medewerkers door duidelijke richtlijnen en verantwoordelijkheden vast te leggen[6]. Echter, de effectiviteit is sterk afhankelijk van actieve betrokkenheid van het management en de naleving door medewerkers (Dutta & McCrohan, 2002). Het beleid moet regelmatig worden herzien om relevant te blijven en effectief in te spelen op nieuwe dreigingen (Safa, Von Solms, & Furnell, 2016). Daarnaast verhoogt de betrokkenheid van medewerkers bij de ontwikkeling van het beleid de effectiviteit ervan (Bulgurcu, Cavusgolu & Benbasat, 2010). Zo zorgt het voor een grotere motivatie en verantwoordelijkheid om het beleid na te leven. Kortom, een goed opgesteld en onderhouden IB-beleid creëert de noodzakelijke gelegenheid voor beveiligingsmaatregelen, mits goed ondersteund door management en medewerkers.

3.2.3 Risicomanagement

Maatregel: Risicoanalyse en methodiek en bepalen risk appetite.
Categorie: Proces
Effectiviteit: Risicomanagement zorgt ervoor dat organisaties hun middelen gericht inzetten om dreigingen te beheersen. Kure, Islam en Razzaque (2017) benadrukken dat een dynamische benadering, waarbij risico's continu worden geëvalueerd en herzien, effectiever is dan statische benaderingen die vaak achterlopen op actuele dreigingen. Het proces van het bepalen van de 'risk appetite' helpt bij het afstemmen van risicomanagementmaatregelen op de strategische doelen van de organisatie en zorgt ervoor dat risico's in overeenstemming zijn met de tolerantie van de organisatie (Lam, 2014). Statische analyses missen vaak de nuance die nodig is om specifieke dreigingen te adresseren, wat kan leiden tot onvoldoende bescherming tegen veranderende omstandigheden (Dutta & McCrohan, 2002). Een adaptieve benadering maakt het mogelijk snel in te spelen op nieuwe risico's, wat de effectiviteit van het managementproces vergroot.

3.2.4 Procedure en inrichting voor het maken van een back-up
Maatregel: Back-upprocedure en cyclus.
Categorie: Proces (met technologie-component)
Effectiviteit: Back-upprocedures zijn essentieel voor het herstel van gegevens na incidenten, zoals dataverlies of cyberaanvallen. Bowers, McFadden, & Smith (2021) benadrukken dat regelmatige back-uptests het herstelvermogen van een organisatie versterken, aangezien organisaties die regelmatig back-ups testen sneller en effectiever kunnen herstellen[7]. Dit verhoogt de kans op een succesvolle herstelfase na een incident aanzienlijk. Echter, de effectiviteit van back-upmaatregelen is beperkt als ze niet goed geïntegreerd zijn in bredere incidentmanagementprocessen. Kwon en Johnson (2016) wijzen erop dat organisaties vaak tekortschieten in het uitvoeren van effectieve incidentrespons, vooral als back-ups niet systematisch worden getest en gekoppeld aan het bredere crisismanagementplan. Zonder een geformaliseerde en routinematige aanpak van back-ups kan de effectiviteit van deze maatregelen afnemen, zelfs als de back-ups zelf betrouwbaar zijn.

3.2.5 Security Incident Management
Maatregel: Procedure voor incidenten en response Datalekken.
Categorie: Proces
Effectiviteit: Een goed incidentmanagementproces verhoogt de veerkracht van organisaties aanzienlijk (Harrington, Dillon & Eze, 2017). Regelmatige oefeningen, zoals cybercrisissimulaties, versterken de capaciteit van teams om effectief te reageren.

[6] https://www.gegevensbeschermingsautoriteit.be/professioneel/thema-s/informatieveiligheid/een-informatie-beveiligingsbeleid
[7] https://www.digitaltrustcenter.nl/back-ups

Echter, een gebrek aan middelen of betrokkenheid van het hoger management kan de uitvoering belemmeren.

3.2.6 Opstellen managementrapportage

Maatregel: Managementrapportage
Categorie: Proces
Effectiviteit: Managementrapportages zorgen voor strategisch inzicht en verantwoording. Dutta en McCrohan (2002) benadrukken echter dat de waarde van rapportages afhangt van hun actiegerichtheid. Te veel focus op rapportage zonder duidelijke vertaling naar verbeteracties kan contraproductief zijn.

3.2.7 In kaart brengen van bedrijfsmiddelen en selectie van tooling inclusief classificatie.

Maatregel: Bedrijfsmiddelenoverzicht[8]
Categorie: Proces (met technologisch component)
Effectiviteit: Het bijhouden van een actueel bedrijfsmiddelenregister vormt een essentiële basis voor kwetsbaarheidsbeheer en risicomanagement (Ahmed, Mahmood, & Hu, 2020). Echter, de waarde van deze maatregel neemt sterk af zonder periodieke updates en integratie met andere processen, zoals patchmanagement.

3.2.8 Reparatie

Maatregel: Een voorbeeldprocedure om een acceptabele score op internet.nl te krijgen >70%
Categorie: Proces (met technologisch component)
Effectiviteit: Volgens Van Goethem, Joosen en Piessens (2014) verbeteren protocollen zoals DNSSEC en TLS niet alleen de beveiliging, maar ook het vertrouwen van klanten. Implementatiefouten of slecht beheer blijven echter een risico.

3.2.9 Beheersen van kwetsbaarheden

Maatregel: Procedure voor patch- en kwetsbaarheidsmanagement[9].
Categorie: Proces (met technologisch component)
Effectiviteit: Effectief patchmanagement is een kostenefficiënte maatregel die het risico op aanvallen via kwetsbaarheden aanzienlijk vermindert. Het Nationaal Cyber Security Centrum (NCSC) benadrukt het belang van een goed ingericht patchmanagementproces voor het identificeren, testen en installeren van updates (NCSC, z.d.). Daarnaast wordt onderstreept dat het tijdig doorvoeren van patches cruciaal is om misbruik van kwetsbaarheden te voorkomen, wat kan leiden tot datalekken of ransomware-aanvallen (Informatiebeveiliging & Privacy, 2022). Hoewel technologie, zoals tools voor kwetsbaarheidsdetectie, ondersteunend is, ligt de nadruk op het ontwikkelen van een procedure voor patch- en kwetsbaarheidsmanagement. Dit maakt het een procesmaatregel, waarbij technologie dient als hulpmiddel voor de uitvoering.

3.2.10 Beheersing rechtenbeheer en toegangscontrole

Maatregel: Autorisatiematrix.
Categorie: Proces (met technologisch component)
Effectiviteit: Een autorisatiematrix stelt organisaties in staat de toegang tot systemen te beperken en voorkomt datalekken door alleen bevoegde gebruikers toegang te geven (Ferraiolo, Sandhu, Gavrila, Kuhn & Chandramouli, 2015). Deze maatregel biedt de gelegenheid om de toegang effectief te beheren, wat een belangrijk procesaspect is. De effectiviteit hangt echter niet alleen af van de technologie zelf, maar van het proces van het regelmatig bijwerken en auditen van de matrix. Als de matrix niet up-to-date wordt

[8] https://www.digitaltrustcenter.nl/inventariseren-van-ict-onderdelen
[9] https://www.digitaltrustcenter.nl/updates

gehouden of als toegang niet periodiek wordt gecontroleerd, kan de autorisatiematrix ineffectief worden. Het proces van het uitvoeren van regelmatige audits en het aanpassen van toegangsrechten is cruciaal voor het succes van deze maatregel, ongeacht de technologie die wordt gebruikt.

3.2.11 Veilig mailen

Maatregel: Proces en eventuele selectie van tooling voor het veilig mailen.
Categorie: Proces (met technologisch component)
Effectiviteit: De effectiviteit van veilig mailen hangt niet alleen af van de gekozen technologie (zoals spamfilters of beveiligde servers), maar ook van de implementatie van een duidelijk proces en gebruikersondersteuning. Gollin. Schwenk en Muller (2018) tonen aan dat e-mailbeveiligingstools bijdragen aan het verminderen van dreigingen, maar zonder bijbehorende training en beleid zijn ze minder effectief. Medewerkers moeten zich bewust zijn van de risico's en weten hoe ze de tools correct moeten gebruiken. Zhou, Gu en Liu (2021) benadrukken dat de effectiviteit van deze technologie sterk afhangt van gebruikersgedrag. Tools kunnen in de praktijk niet volledig benut worden zonder consistente adoptie door medewerkers en bijbehorende beleidsmaatregelen.

3.2.12 Netwerksegmentatie

Maatregel: Procedure voor de inrichting van netwerksegmentatie.
Categorie: Proces (met technologisch component)
Effectiviteit: Een procedure voor netwerksegmentatie draagt bij aan het beperken van laterale bewegingen van aanvallers en het verminderen van datalekrisico's. Liu, Han, en Yang (2018) benadrukken dat netwerksegmentatie een effectieve beveiligingsstrategie is, mits correct geïmplementeerd. Het isoleren van netwerksegmenten maakt het moeilijker voor aanvallers om zich door een netwerk te bewegen, wat schade en impact van aanvallen kan beperken. Het opstellen van een procedure voor netwerksegmentatie is essentieel om consistentie te waarborgen en fouten bij de implementatie te minimaliseren (Scarfone, Souppaya, & Hoffman, 2009). Zonder duidelijke richtlijnen kunnen organisaties over-segmenteren, wat beheercomplicaties veroorzaakt, of te weinig segmenteren, wat beveiligingsrisico's verhoogt (Northcutt, Zeltser, Winters & Fredrick, 2012). Het succes van segmentatie hangt tevens af van regelmatige audits en het up-to-date houden van netwerkconfiguraties.

3.3 Technologie

3.3.1 Interne kwetsbaarheidsscan

Maatregel: Rapportage van de interne scan, inclusief advies
Categorie: Technologie (met procescomponent)
Effectiviteit: Interne kwetsbaarheidsscans helpen zwakke plekken vroegtijdig te identificeren[10]. Mell, Scarfone, en Romanosky (2006) benadrukken dat ze alleen effectief zijn als gevonden kwetsbaarheden tijdig worden opgelost. Zhang e.a. (2020) stellen dat scans beter werken wanneer ze deel uitmaken van een risico gebaseerde strategie, waarbij prioriteit wordt gegeven aan kwetsbaarheden met hoge impact. Geautomatiseerde tools verbeteren consistentie en nauwkeurigheid (Ahmed, Mahmood, & Khan, 2019). Beperkingen ontstaan vaak door een gebrek aan middelen of opvolging, wat herhaalde problemen veroorzaakt (Zhou & Leung, 2021). Managementbetrokkenheid en structurele opvolging zijn daarom essentieel.

[10] https://www.digitaltrustcenter.nl/nieuws/veel-kleine-bedrijven-zijn-onvoldoende-cyberweerbaar

4. Semigestructureerde interviews

Er werden interviews afgenomen met zowel deelnemende mkb-ondernemers als cybersecurityprofessionals.

Verbeteren van de cyberweerbaarheid
Uit de interviews blijkt dat deelnemers behoefte hebben aan ondersteuning, omdat zij niet altijd over de benodigde kennis en middelen beschikken om hun cyberweerbaarheid zelfstandig op orde te brengen. Het inhuren van consultants en de aanschaf van technische oplossingen worden vaak als kostbaar ervaren, waardoor pilots en subsidies als zeer aantrekkelijk worden gezien. Ondernemers erkennen de reële dreiging van cyberaanvallen en de mogelijke schade die hieraan verbonden is. Tevens is er een grote vraag naar compliance-gerelateerde oplossingen, zoals ondersteuning bij AVG en andere regelgeving. Vooral technisch georiënteerde bedrijven beschikken vaak over een gedegen technische basis, maar hebben nog veel vragen omtrent beleid. Kennissessies en consultancy-uren dragen niet alleen bij aan het inzicht in kwetsbaarheden en praktische tools, maar versterken ook de interne vaardigheden, aldus de deelnemers.

Hands-on ondersteuning en de menukaart
De interviews geven aan dat bedrijven op zoek zijn naar zowel praktische ondersteuning als een aanpak die per organisatie op maat kan worden gemaakt. Er werd specifiek gevraagd of de aangeboden opties op de menukaart aansloten bij de keuzes die bedrijven daadwerkelijk maakten. De reacties waren gemengd: sommige bedrijven maakten gebruik van de menukaartopties, terwijl anderen samen met Cyber4Z een op maat gemaakte aanpak ontwikkelden. Beide benaderingen werden door de deelnemende bedrijven als positief ervaren. Professionals merkten op dat de gekozen beleidsmatige opties zwaarder wogen dan de technische oplossingen; er werd vaak gekozen voor een combinatie van standaard menukaartopties en op maatwerk gebaseerde maatregelen

Effectiviteit versus tijdsinzet
De bedrijven gaven aan dat zij voldoende tijd en middelen beschikbaar hadden voor de pilot, wat ook daadwerkelijk resulteerde in de uitvoering van de voorgestelde maatregelen. Professionals signaleerden echter dat de pilot in eerste instantie niet altijd prioriteit kreeg, wat leidde tot een moeizame communicatie. Naarmate de pilot vorderde, verbeterde de communicatie aanzienlijk, waardoor een betere afstemming over de tijdsinzet mogelijk werd. Dit kwam mede door het feit dat, naarmate de pilot vorderde zowel de professionals als bedrijven beter wisten wat ze van elkaar konden verwachten en wat nodig was in tijd, middelen en verplichtingen. Dit maakte afstemming bij latere intakes makkelijker.

Rol van de IT-dienstverlener
Twee van de geïnterviewde bedrijven werkten niet samen met een IT-dienstverlener, terwijl de overige bedrijven aangaven dat hun IT-dienstverlener weliswaar op de hoogte was van de pilot, maar niet actief betrokken werd bij de uitvoering. Het al dan niet inzetten van een IT-dienstverlener bleek geen significante invloed te hebben op de uitvoering van de pilot en de implementatie van de maatregelen.

Impact van de pilot
De pilot heeft de deelnemende bedrijven geholpen bij het professionaliseren en formaliseren van hun interne producten, diensten en documentatie. Actieplannen zijn opgesteld voor de tijdens de pilot geïdentificeerde verbeterpunten en worden momenteel vertaald naar implementatieplannen voor de komende maanden. De aangeboden 50 uur ondersteuning bleek voor de meeste bedrijven voldoende om een

eerste positieve impuls te geven, waarna sommigen aanvullende ondersteuning buiten de pilot om overwegen.

Duurzaamheid van de pilot
De deelnemende bedrijven hebben er vertrouwen in dat zij de geformuleerde verbeteringen zelfstandig kunnen doorvoeren, met af en toe wat extra begeleiding. Enkele bedrijven overwegen om na enkele jaren een vergelijkbare evaluatie uit te laten voeren om de voortgang te monitoren. De pilot wordt gewaardeerd om de stimulans die het geeft aan verbeteringstrajecten en de netwerken die hierdoor worden versterkt, zowel met andere bedrijven als met leveranciers.

Aanbevelingen en verbeterpunten op basis van de interviews
Hoewel de pilot een solide basis biedt voor de ondersteuning van ondernemers bij de ontwikkeling van hun cyberweerbaarheid, zijn er enkele verbeterpunten geïdentificeerd:

- **Menukaart:** Er dient kritisch gekeken te worden naar het huidige aanbod. De interviews tonen aan dat naast de gestandaardiseerde opties vaak gekozen wordt voor een meer persoonlijke aanpak. Voor toekomstige pilots is het aan te bevelen om een beperkt, maar evenwichtig aanbod te bieden dat zowel beleidsmatige als technische oplossingen omvat, met ruimte voor maatwerk.
- **Standaard Templates:** Deelnemers vragen om standaard sjablonen die ondersteuning bieden bij het opstellen van diverse beleidsdocumenten, zoals richtlijnen voor laptops, IT-beheer en informatiebeveiligingsbeleid. Deze templates moeten flexibel genoeg zijn om aan de specifieke behoeften van de organisatie aangepast te worden.
- **Communicatie:** Er is behoefte aan meer duidelijkheid over de pilot, zowel over de reeds bestede uren als over de communicatie tussen professionals en bedrijven. Het was voor sommige bedrijven gedurende de pilot niet duidelijk hoeveel uren zij al gebruikt hadden. Daarbij verliep de communicatie aan het begin van de pilot stroef, dit is gedurende de pilot opgelost. Tevens zijn er vanuit de professionals vragen omtrent subsidiering en facturering.

Aanbevelingen voor opschaling en implementatie blauwdruk
De aangeboden 50 uur ondersteuning vormt een gedegen basis voor de blauwdruk, die zowel voor bedrijven als professionals voldoende ruimte biedt voor een eerste nulmeting en verdere verbeteringstrajecten. Voor een succesvolle implementatie is het essentieel dat:

- De communicatie voorafgaand aan en tijdens de pilot op orde is, zodat voor alle partijen duidelijk is wat de verwachtingen zijn.
- De kritieke data voor oplevering en facturering helder worden gecommuniceerd.
- De promotie richting potentiële nieuwe deelnemers wordt versterkt. Gezien het feit dat ondernemers vaak pas deelnemen na een incident of op aanraden van andere mkb’ers, is het van belang om alternatieve communicatieroutes in te zetten, zoals via de Kamer van Koophandel, lokale media, banken of gerenommeerde websites als security.nl.

5. Focusgroep

Om beter te begrijpen onder welke voorwaarden ondernemers in het mkb bereid zijn om tijd en geld te besteden aan ondersteuning of deel te nemen aan een subsidieregeling die vanuit de overheid wordt aangeboden om ondernemers te helpen met hun cyberweerbaarheid, is ervoor gekozen om een focusgroep te organiseren.

5.1 Methode

Voor dit onderzoek is een kwalitatieve onderzoeksmethode gekozen met als doel inzicht te krijgen in de gedragsbepalers die de bereidheid van mkb-ondernemers beïnvloeden om te investeren in ondersteuning voor het vergroten van hun cyberweerbaarheid. Gezien de exploratieve aard van de onderzoeksvraag is een focusgroep als methode gekozen, omdat deze methode inzichten biedt in de ervaringen en percepties van mkb-ondernemers.

Werving en deelnemers

De deelnemers aan de focusgroep zijn geworven via Midpoint Brabant en Hallo. Midpoint Brabant is de regionale economische ontwikkelingsorganisatie voor Midden-Brabant, die samen met ondernemers, onderwijs en overheid innovatie en groei stimuleert. Hallo ondersteunt mkb'ers door ICT toegankelijker en efficiënter te maken, met aandacht voor veiligheid, training en groei. Daarnaast hebben we een oproep geplaatst via het community portal van het DTC en gebruikgemaakt van het panel van EZ: ondernemersdenkenmee.nl, maar deze inspanningen leverden geen deelnemers op. Het streven was om een diverse groep van 10 tot 15 ondernemers samen te brengen, representatief voor verschillende sectoren en bedrijfsgroottes binnen het mkb. Deze diversiteit werd gezocht om verschillende inzichten en ervaringen te verzamelen met betrekking tot cybersecurity en de bereidheid om in ondersteuning te investeren. Uiteindelijk waren er 9 mkb'ers uit diverse sectoren bij de focusgroep aanwezig.

Data-collectie

De focusgroep vond fysiek plaats in een sessie van 2 uur bij Midpoint-Brabant, gelegen aan Burgemeester Brokxlaan 12, Tilburg. Tijdens de sessie werd gebruikgemaakt van een semigestructureerd opzet, waarin een tiental stellingen werden gepresenteerd om zowel specifieke onderzoeksthema's te adresseren als ruimte te bieden voor spontane discussies. Deze stellingen staan weergegeven in tabel 2 en komen overeen met de 10 vooraf geselecteerde TDF domeinen (Zie tabel 2). De sessie volgde de structuur die ook in de bijbehorende PowerPoint werd gepresenteerd, bestaande uit de volgende onderdelen: voorstellen, met de deelnemers in gesprek gaan aan de hand van stellingen, conclusie, vragenronde en afsluiting. Er werd geen pauze ingepland.

Naast de respondenten waren er drie onderzoekers van Avans Hogeschool aanwezig, samen met afgevaardigden van Hallo en Midpoint Brabant. De rolverdeling was als volgt: de facilitator van de sessie was een onderzoeker van Avans Hogeschool, terwijl de andere twee onderzoekers de rol van notulisten op zich namen om de belangrijkste punten van de discussie vast te leggen.

Tabel 1. *Stellingen op basis van het COM-B model en TDF.*

COM-B	TDF	Stelling
Capaciteit	Kennis	"Ik ben op de hoogte over hoe ik gebruik kan maken van de diensten van een cybersecurity professional tegen een sterk gereduceerd tarief."
Capaciteit	Vaardigheden	"Ik heb in het verleden al eens gebruik gemaakt van de diensten van een CS professional voor

		mijn bedrijf, tegen sterk gereduceerd tarief, om de cyberweerbaarheid van mijn bedrijf te versterken.”
Motivatie	Sociale/professionele rol en identiteit	"ik zie het als mijn verantwoordelijkheid om gebruik te maken van de diensten van een CS professional, tegen sterk gereduceerd tarief, om de cyberweerbaarheid van mijn bedrijf te versterken.”
Motivatie	Geloof in eigen kunnen	"Ik heb er vertrouwen in dat als ik het wil, ik in staat ben om gebruik te maken, tegen gereduceerd tarief, van de diensten van een cybersecurity professional”
Motivatie	Opvattingen over consequenties	"Als ik gebruik maak van de diensten van een CS professional, dan zal dit de kans op schadelijke incidenten aanzienlijk verminderen."
Motivatie	Versterking	"Ik ben bereid om de diensten van een CS professional in te schakelen, wanneer ik overtuigd ben van de toegevoegde waarde voor mijn bedrijf."
Motivatie	Intentie	“Ik ben bereid om gebruik te maken van de diensten van een CS professional, tegen gereduceerd tarief, om zodoende mijn bedrijf te beschermen ten cybercrime."
Motivatie	Doelen	“Andere onderwerpen op de agenda hebben een hogere prioriteit dan het inschakelen van de diensten van een CS professional tegen gereduceerd tarief."
Gelegenheid	Omgevingscontext en middelen	“Er is voldoende tijd en financiële middelen beschikbaar om gebruik te maken van de diensten van de CS professional tegen gereduceerd tarief."
Gelegenheid	Sociale invloeden	“De meeste mensen die belangrijk voor mij zijn vinden dat ik gebruik moet maken van de diensten van een cybersecurityprofessional tegen gereduceerd tarief."

5.2 Theoretisch kader

Voor het maken van de stellingen is gebruikgemaakt van het COM-B model, een theoretisch kader dat gedrag analyseert aan de hand van drie centrale componenten: Capaciteit (Capability), Gelegenheid (Opportunity) en Motivatie (Motivation). Het model helpt bij het identificeren van de belangrijkste factoren die gedrag beïnvloeden en biedt een systematische benadering om te begrijpen waarom ondernemers al dan niet bereid zijn om te investeren in cyberweerbaarheid (Michie, van Stralen, & West, 2011).

Als aanvulling op het COM-B model is het Theoretical Domains Framework (TDF) gebruikt. Het TDF, ontwikkeld door Michie e.a. (2011), breidt het COM-B model uit door de drie centrale componenten te vertalen naar 14 domeinen die psychologische, gedragsmatige en omgevingsfactoren in kaart brengen. Het TDF biedt een gedetailleerder inzicht in de specifieke determinanten die van invloed zijn op gedragsverandering. Door het TDF te integreren met het COM-B model, wordt het mogelijk om niet alleen de algemene gedragsfactoren te identificeren, maar ook de

onderliggende mechanismen die gedragingen sturen. In dit onderzoek is met een selectie gewerkt van tien relevante TDF-domeinen.

Deze selectie werd vervolgens getoetst in de focusgroep: het doel was te onderzoeken of de voorgestelde gedragsbepalers daadwerkelijk relevant en kloppend zijn in de context van de mkb-ondernemers. Voor de focusgroep, gericht op de vraag: "Onder welke voorwaarden ondernemers in het mkb bereid zijn om tijd en geld te besteden aan ondersteuning in welke vorm dan ook?", zijn specifieke TDF-domeinen geselecteerd die relevant zijn binnen de drie COM-B-componenten.
Zie tabel 2 voor de TDF-domeinen en de bijbehorende definities.

Tabel 2. *TDF-domeinen.*

Domein	**Definitie**
Kennis	Het bewustzijn van ondernemers over de noodzaak van cybersecurity en beschikbare ondersteunings-mogelijkheden.
Vaardigheden	De ervaring en technische capaciteiten van ondernemers om zelf de juiste maatregelen te nemen.
Sociale/professionele rol en identiteit	De perceptie van de rol van de ondernemer in het beschermen van het bedrijf tegen cyberdreigingen.
Geloof in eigen kunnen	Het vertrouwen van de ondernemer in zijn of haar eigen vermogen om effectief met cyberdreigingen om te gaan.
Opvattingen over consequenties	De overtuiging van de ondernemer dat maatregelen daadwerkelijk bijdragen aan het verkleinen van risico's.
Versterking	Factoren die bijdragen aan het versterken van de motivatie van ondernemers om door te gaan met cybersecurity-initiatieven.
Intentie	De intentie om beschermende maatregelen te nemen tegen cyberdreigingen.
Doelen	De plaats die cybersecurity inneemt op de prioriteitenlijst van ondernemers.
Omgevingscontext en middelen	De externe omstandigheden en beschikbare middelen die de bereidheid van ondernemers om te investeren in cybersecurity beïnvloeden.
Sociale invloeden	De invloed van collega-ondernemers, netwerken of externe partijen die mogelijk het gedrag rondom cybersecurity beïnvloeden.

Door deze thema's centraal te stellen, kon de focusgroep gericht worden op het onderzoeken van de belangrijkste gedragsbepalers die ondernemers in het mkb beïnvloeden bij het nemen van beslissingen over cybersecurityondersteuning en het investeren in cyberweerbaarheid. Dit maakte het identificeren van zowel de belemmeringen als de motivaties die spelen bij de bereidheid om tijd en geld te investeren in het versterken van de cyberweerbaarheid inzichtelijker.

5.3 Resultaten

In de focusgroep kwamen diverse barrières naar voren die het voor mkb-ondernemers moeilijk maken om (optimaal) gebruik te maken van de beschikbare initiatieven en ondersteuningsmogelijkheden op het gebied van cybersecurity. De mogelijke barrières zijn vastgesteld op basis van het eerdergenoemde COM-B model.

Capaciteit

Communicatiekloof

Uit de focusgroep blijkt dat niet begrijpelijke communicatie een belangrijke barrière vormt. Dit heeft te maken met een gebrek aan kennis en vaardigheden, die beide onder Capaciteit vallen binnen het COM-B model. Ondernemers missen vaak de kennis om te begrijpen welke maatregelen ze precies moeten nemen om hun bedrijf te beschermen tegen cyberdreigingen. Ze zijn niet op de hoogte van de beschikbare diensten van cybersecurityprofessionals en weten vaak niet hoe ze deze effectief kunnen inzetten. Dit wijst op een gebrek aan kennis over wat er mogelijk is op het gebied van cybersecurity.

Daarnaast ontbreekt het ondernemers veelal aan de vaardigheden om cybersecuritymaatregelen daadwerkelijk toe te passen. Ze hebben vaak geen ervaring met het inzetten van cybersecurityprofessionals om de cyberweerbaarheid van hun bedrijf te versterken, waardoor ze niet goed in staat zijn om geïnformeerde keuzes te maken over hoe ze hun bedrijf kunnen beschermen.

Cybersecurity-experts gebruiken vaak technische termen die voor veel ondernemers moeilijk te begrijpen zijn, waardoor ondernemers de informatie niet goed kunnen interpreteren of toepassen op hun situatie. Deze kloof in communicatie vormt een belemmering voor een effectieve samenwerking. Cybersecurity-experts moeten hun communicatie en advies meer afstemmen op de specifieke behoeften en het taalgebruik van de ondernemer. Hoewel dit vanuit de focusgroep naar voren komt, blijkt uit de pilot dat als ondernemers eenmaal aangehaakt zijn bij de pilot zij deze belemmering niet meer ondervinden en goed mee kunnen komen met de technische termen

(On)Bewustzijn van cybersecurity-initiatieven

Daarop aansluitend bleek uit de focusgroep dat veel ondernemers zich niet bewust zijn van de verschillende initiatieven en subsidies die beschikbaar zijn om hun cyberweerbaarheid te versterken. Dit wijst opnieuw op een gebrek aan kennis over de beschikbare mogelijkheden. Ondernemers zijn vaak niet op de hoogte van de programma's die hen kunnen helpen om hun cyberweerbaarheid te verbeteren. De communicatie over deze programma’s is, zoals eerder genoemd vaak te technisch en/of te abstract, waardoor ondernemers de waarde van deze initiatieven niet goed kunnen inschatten. Dit gebrek aan kennis maakt het moeilijk voor ondernemers om te begrijpen welke stappen ze kunnen nemen om hun bedrijf te beschermen. Een betere afstemming van de communicatie op het kennis- en vaardigheidsniveau van ondernemers kan helpen om hun capaciteit te vergroten en hen in staat te stellen de juiste keuzes te maken om hun cyberweerbaarheid te versterken.

Motivatie

Gebrek aan urgentiebesef

Motivatie bleek een belangrijke barrière voor mkb-ondernemers om hun cyberweerbaarheid te verbeteren. Veel ondernemers erkennen wel dat cyberbeveiliging belangrijk is, maar zijn zich vaak niet volledig bewust van de risico’s die gepaard gaan met cybercriminaliteit. Dit kan deels worden toegeschreven aan het gebrek aan urgentiebesef; de dreiging van cyberincidenten wordt vaak pas erkend wanneer het al

te laat is. Cybersecurity wordt daardoor vaak als een abstract en niet-urgente taak gezien, vooral wanneer er geen direct incident heeft plaatsgevonden. Dit kan verklaard worden door de Ostrich Paradox, die verwijst naar de menselijke neiging om bedreigingen te negeren of te vermijden, zelfs als deze belangrijke risico's met zich meebrengen. Deze cognitieve bias zorgt ervoor dat ondernemers de noodzaak om preventieve maatregelen te nemen vaak onderschatten, waardoor ze geen actie ondernemen totdat een incident zich daadwerkelijk voordoet (Meyer & Kunreuther, 2017). Dit zou kunnen verklaren waarom cybersecurity vaak laag op de prioriteitenlijst van bedrijven staat.

Een goed voorbeeld hiervan kwam naar voren tijdens de focusgroep. Verschillende ondernemers waren met elkaar in gesprek over de data die zij in beheer hebben. Een van de ondernemers gaf aan niet bang te zijn voor een data lek, omdat ze toch geen gevoelige informatie verwerkte. Hackers zouden alleen toegang hebben tot personeelsbestanden en contracten. Deze ondernemer werd er echter op gewezen door zijn collega's dat informatie over medewerkers en contracten ook gevoelige informatie is en dat dit wel degelijk problematisch kon zijn indien hij gehackt zou worden.

Begrip van de waarde van cybersecuritymaatregelen
De focusgroep gaf aan dat experts vaak onvoldoende vertalen naar de bedrijfscontext, waardoor ondernemers de waarde van cybersecuritymaatregelen niet altijd inzien en moeite hebben om het belang ervan voor hun bedrijfscontinuïteit te begrijpen. Dit wijst op een gebrek aan motivatie, met name het domein 'Opvattingen over consequenties'. Ondernemers hebben onvoldoende overtuiging over de impact die cybersecuritymaatregelen kunnen hebben op hun bedrijfscontinuïteit, wat hen ontmoedigt om actie te ondernemen. Dit gebrek aan geloof in de effectiviteit van de response draagt bij aan het lage gevoel van urgentie en belang rondom cybersecurity.

Dit kan ertoe leiden dat ondernemers moeite hebben om de juiste vragen te stellen aan IT-dienstverleners of cybersecurity-experts en daardoor niet altijd in staat zijn om de juiste keuzes te maken. Binnen het domein **'**Opvattingen over consequenties**'** gaat het hier om de overtuiging van ondernemers over de effectiviteit van hun acties. Als ondernemers niet geloven dat de maatregelen die ze kunnen nemen daadwerkelijk verschil maken, zullen ze minder snel geneigd zijn om te investeren in deze maatregelen. Ondernemers moeten zich bewust zijn van het belang van cybersecurity en leren hoe ze de juiste vragen kunnen stellen om hun eigen cyberweerbaarheid te versterken, zodat ze zowel hun overtuigingen over de effectiviteit als de gevolgen van cybersecuritymaatregelen kunnen verbeteren.

Aantoonbaarheid waarde van cybermaatregelen: kortzichtigheid heuristiek
Een andere barrière voor mkb'ers is dat de voordelen van cybersecuritymaatregelen vaak moeilijk te vertalen zijn naar concrete bedrijfsresultaten. Cybermaatregelen, zoals investeringen in beveiligingssoftware of training van personeel, tonen hun effect pas wanneer er een incident plaatsvindt. Dit maakt het voor ondernemers lastig om de waarde van deze maatregelen vooraf aan te tonen, aangezien de voordelen pas zichtbaar zijn bij het optreden van een probleem. In dit verband noemen Meyer en Kunreuther (2017) de Myopie Bias (kortzichtigheid heuristiek), waarbij besluitvormers de lange termijn voordelen van beschermende maatregelen niet zien of uitstellen, omdat ze zich niet goed kunnen verhouden tot de toekomstige voordelen die pas na een incident zichtbaar worden. Beslissingen om te investeren in beschermende maatregelen vereisen vooruitziendheid, iets wat voor ondernemers lastig is, gezien hun neiging om de waarde van toekomstige investeringen niet te erkennen.

Ondernemers gaven aan dat het benadrukken van de preventieve voordelen van cybersecurity en het delen van praktijkvoorbeelden van andere bedrijven die

geprofiteerd hebben van verbeterde cyberweerbaarheid hen zou kunnen motiveren om actie te ondernemen. Door de Myopie Bias te doorbreken en de voordelen van cybersecuritymaatregelen op een meer tastbare en onmiddellijke manier te presenteren, kan de motivatie om te investeren in cyberweerbaarheid worden vergroot.

Gelegenheid
De gelegenheid om gebruik te maken van ondersteunende diensten en middelen speelt een belangrijke rol in de bereidheid van ondernemers om te investeren in cybersecurity. Tijdens de focusgroep gaven ondernemers aan dat ze openstaan om zelf te investeren, mits de aangeboden ondersteuning aansluit bij hun specifieke behoeften. Ondersteunende diensten, zoals vouchers, werden als waardevolle aanvulling gezien, vooral voor ondernemers die al de intentie hadden om te investeren. Voor ondernemers zonder plannen om te investeren, zou een dergelijke ondersteuning hen waarschijnlijk niet over de streep trekken. Enkele deelnemers gaven aan dat er behoefte is aan laagdrempelige initiatieven, zoals subsidies of vouchers, die hen kunnen helpen de eerste stap te zetten zonder grote financiële verplichtingen. Dit zou hen niet alleen in staat stellen om de waarde van cybersecuritymaatregelen beter in te zien, maar ook om te begrijpen hoe deze bijdragen aan de bedrijfscontinuïteit.

Zoals eerder aangegeven, is het moeilijk om de waarde van cybersecuritymaatregelen te onderbouwen, vooral richting budgethouders. Omdat de effectiviteit van cybersecuritymaatregelen pas zichtbaar wordt wanneer er een incident plaatsvindt, is het voor veel ondernemers lastig om de noodzaak voor investeringen in deze maatregelen over te brengen. Dit werd als een belangrijke belemmering gezien, omdat het de bereidheid om in preventieve maatregelen te investeren vermindert. Het benadrukken van concrete succesverhalen van andere bedrijven en het tonen van de lange termijn voordelen van cybersecurity zou kunnen bijdragen aan het vergroten van de gelegenheid voor ondernemers om te investeren. Een manier om ondernemers hierbij te ondersteunen zou kunnen zijn door het aanbieden van tools of workshops waarin ze niet alleen de risico's, maar ook de praktische voordelen van cyberweerbaarheid kunnen ervaren, bijvoorbeeld door simulaties van incidenten die de waarde van preventieve maatregelen duidelijk maken. Dit zou kunnen helpen om de abstracte voordelen meer tastbaar te maken en ondernemers te overtuigen van de noodzaak om te investeren, zelfs als de voordelen pas op lange termijn zichtbaar zijn.

6. Conclusie

Het doel van dit onderzoek was om verschillende onderdelen van de pilot te evalueren en specifiek de focus te leggen op de effectiviteit van de geboden ondersteuning en de gedragsbepalers die maken dat ondernemers bereid zijn om te investeren in hands-on ondersteuning door een cybersecurityprofessional.

6.1 Effectiviteit van de ondersteuning

Uit de interviews komt naar voren dat de deelnemers aan de pilot duidelijk behoefte hadden aan de aangeboden ondersteuning en de pilot ervaren hebben als een waardevolle en effectieve manier om hun cyberweerbaarheid te verbeteren. Zij zijn zich bewust van het belang van cybersecurity en de risico's die cyberaanvallen met zich meebrengen. Echter beschikken ondernemers veelal niet over de juiste kennis en financiële middelen om zelfstandig hun cyberweerbaarheid naar het gewenste niveau te brengen.

De gesproken bedrijven hadden vooral behoefte aan praktische ondersteuning en begeleiding bij compliance-gerelateerde vraagstukken zoals de AVG-regelgeving. Met name de technisch georiënteerde bedrijven beschikten al over voldoende technische kennis, maar zochten juist op het gebied van beleid en interne processen ondersteuning. De pilot werd binnen de bedrijven gezien als een belangrijke impuls om te professionaliseren en om interne procedures, diensten en documentatie te formaliseren. De beschikbare 50 uur werd door zowel de bedrijven als de professionals als voldoende ervaren om concrete actieplannen op te stellen en om deze vervolgens te vertalen in uitvoerbare implementatieplannen. Als wordt teruggekeken naar de vorige pilot (Kokkeler, e.a., 2023) dan is dit een aanzienlijke verbetering. Destijds was er 10 uur beschikbaar per bedrijf en dit bleek achteraf niet genoeg te zijn.

6.1.1 Communicatie als succes- én verbeterpunt

Communicatie bleek zowel een succesfactor als een belemmering te zijn tijdens de pilot. Uit de interviews komt naar voren dat aanvankelijk de communicatie tussen de bedrijven en de professionals stroef verliep. Dit werd mede veroorzaakt door personele wisselingen aan de kant van de cybersecurityprofessionals. De professionals meldden dat de pilot in het begin bij bedrijven niet altijd als prioriteit werd gezien, waardoor het moeizaam was om concrete afspraken te maken over de tijdsinzet en de inzet van middelen. Dit leidde in de eerste fase van de pilot tot vertraging en verminderde efficiëntie.

Gedurende de pilot verbeterde de communicatie aanzienlijk. Naarmate de bedrijven en de professionals elkaar beter leerden kennen, ontstond er een betere afstemming. Juist doordat de deelnemers gedurende het traject een duidelijker beeld kregen van wat er precies van hen werd verwacht qua tijdsinzet, middelen en verplichtingen, verliepen de latere communicatie en intakegesprekken soepeler. Vanuit de gesprekken kwamen er enkele verbeterpunten naar voren. Deelnemende bedrijven gaven aan (in het begin) dat het niet altijd duidelijk was hoeveel van de beschikbare 50 uur ondersteuning zij reeds hadden gebruikt. De professionals gaven aan meer behoefte te hebben aan duidelijkheid omtrent het proces van subsidiering en facturering.

6.1.2 Effectiviteit en flexibiliteit van de menukaart

De menukaart, bedoeld als overzichtelijke lijst met gestandaardiseerde ondersteuningsmogelijkheden, werd door deelnemers wisselend beoordeeld. Sommige bedrijven maakten actief gebruik van de opties die de menukaart bood en vonden dit effectief, omdat deze hen hielpen snel en gestructureerd keuzes te maken en praktische verbeteringen te implementeren. Andere bedrijven hadden behoefte aan een meer

individuele, maatwerkgerichte aanpak en ontwikkelden daarom, in samenwerking met de cybersecurityprofessional, een op maat gemaakt ondersteuningsprogramma dat verder ging dan de menukaart-opties.

Uit nadere analyse blijkt dat de menukaart vooral gericht is op procesmatige maatregelen met een technologische component, zoals patchmanagement en netwerksegmentatie. Deze aanpak ondersteunt bedrijven bij het opstellen van procedures en richtlijnen als basis voor veilig gedrag. Tegelijkertijd is er relatief weinig aanbod van puur technologische oplossingen, zoals monitoring- en detectie-tooling. Hoewel technologische en procesmatige maatregelen sterk met elkaar verbonden zijn, vereisen ze elk specifieke expertise en investeringen.

Tot slot hangt de effectiviteit van maatregelen sterk af van gekozen producten en implementatiewijze. Succes vereist specifieke randvoorwaarden zoals bedrijfstype, sector, digitale infrastructuur, data-gevoeligheid en het dreigingslandschap. Het blijft onzeker of deze contextuele factoren voldoende worden meegewogen. Bovendien ontbreekt de empirische onderbouwing van maatregelen, zoals bij phishing-simulaties, wat onderbouwde keuzes bemoeilijkt.

6.2 gedragsbepalers

Uit de focusgroep blijkt dat mkb-ondernemers diverse barrières ervaren die hen ervan weerhouden optimaal gebruik te maken van beschikbare initiatieven en ondersteuningsmogelijkheden op het gebied van cybersecurity. Het COM-B-model (Capaciteit, Motivatie en Gelegenheid) biedt inzicht in de gedragsbepalers die ondernemers kunnen stimuleren om te investeren in ondersteuningsmogelijkheden, zoals de hands-on ondersteuning van een cybersecurityprofessional.

6.2.1 Capaciteit

De capaciteit van ondernemers, waaronder hun kennis en vaardigheden op het gebied van cybersecurity, is een belangrijke factor die hun investeringsbereidheid beïnvloedt. Veel ondernemers hebben onvoldoende kennis om te begrijpen welke cybersecuritymaatregelen nodig zijn en welke diensten beschikbaar zijn. Daarnaast ontbreekt het hen vaak aan praktische vaardigheden om dergelijke maatregelen effectief te implementeren. Dit gebrek aan kennis en ervaring zorgt ervoor dat ondernemers moeite hebben om geïnformeerde keuzes te maken omtrent cybersecurity.

Een bijkomende uitdaging is de communicatiekloof tussen ondernemers en cybersecurityprofessionals. Experts gebruiken regelmatig technische terminologie die voor ondernemers lastig te begrijpen is, wat leidt tot misverstanden en een minder effectieve samenwerking. Heldere en op de bedrijfscontext afgestemde communicatie kan helpen deze kloof te overbruggen en zo de capaciteit van ondernemers vergroten.

Daarnaast blijkt uit de focusgroep dat ondernemers vaak niet bewust zijn van beschikbare initiatieven en subsidies, voornamelijk door te abstracte en technisch geformuleerde communicatie. Wanneer informatie beter aansluit bij het kennisniveau van ondernemers, kan dit leiden tot een actievere houding ten aanzien van cyberveiligheid.

6.2.2 Motivatie

Motivatie speelt eveneens een cruciale rol in het stimuleren van ondernemers om te investeren in cybersecurityondersteuning. Hoewel ondernemers doorgaans erkennen dat cybersecurity belangrijk is, ervaren zij vaak onvoldoende urgentie om preventieve maatregelen te nemen. Cybersecurity wordt veelal als een abstract risico beschouwd,

waardoor investeringen pas plaatsvinden na een incident. Dit fenomeen, bekend als de Ostrich Paradox, houdt in dat ondernemers risico's negeren totdat ze tastbaar worden. Daardoor blijft cybersecurity laag op hun prioriteitenlijst staan.

Daarnaast beïnvloedt de perceptie van de waarde en effectiviteit van cybersecuritymaatregelen de motivatie. Doordat experts cybersecurity onvoldoende vertalen naar de specifieke bedrijfscontext, zien ondernemers niet altijd de directe voordelen voor hun bedrijfscontinuïteit. Dit gebrek aan inzicht ontmoedigt hen om concrete stappen te zetten. Bovendien maakt de Myopie Bias (kortzichtigheid) het moeilijk voor ondernemers om te investeren in preventieve maatregelen, omdat de voordelen pas zichtbaar worden bij incidenten. Het benadrukken van praktijkvoorbeelden en succesverhalen kan helpen om deze bias te doorbreken en ondernemers te overtuigen van de tastbare voordelen van preventieve maatregelen.

6.2.3 Gelegenheid

Ook de gelegenheid om gebruik te maken van ondersteuningsmogelijkheden beïnvloedt de investeringsbereidheid. Ondernemers zijn bereid te investeren mits de ondersteuning goed aansluit bij hun behoeften en praktische mogelijkheden. Vooral laagdrempelige initiatieven zoals vouchers of subsidies kunnen ondernemers stimuleren om de eerste stap te zetten. Daarnaast geven ondernemers aan dat het tonen van concrete succesverhalen en praktijkvoorbeelden, zoals workshops en simulaties van cyberincidenten, helpt om cybersecurity tastbaarder te maken. Dit kan bijdragen aan het vergroten van de bereidheid om preventief te investeren.

6.3 Concluderend

Op basis van bovenstaande bevindingen wordt geadviseerd om de huidige menukaart te transformeren naar een visueel overzicht, een zogenoemde praatplaat, waarin maatregelen worden gecategoriseerd op basis van de drie pijlers: mens, proces en technologie. Onder deze hoofdcategorieën zouden domeinen als training, incident response en risk assessments duidelijk kunnen worden weergegeven. Daarnaast is het essentieel dat, voor zover er concrete producten of diensten worden aangeboden, helder wordt aangegeven wat de effectiviteit hiervan is en op welke randvoorwaarden dit is gebaseerd.

Samenvattend blijkt dat, hoewel de basis voor ondersteuning in de pilot solide is, er op het gebied van de menukaart en enkele gedragsbepalers rondom cybersecurity nog aanzienlijke verbeterpunten liggen. Door de menukaart te herstructureren en het aanbod te beperken tot een evenwichtige mix van beleidsmatige en technische oplossingen – met ruimte voor maatwerk – kunnen mkb-ondernemers beter worden geholpen in hun keuze. Tegelijkertijd moet er meer aandacht komen voor de koppeling met de nulmeting en voor een heldere communicatie over zowel de preventieve voordelen als de effectiviteit van de gekozen maatregelen. Op deze manier kan de investering in cyberweerbaarheid niet alleen beter onderbouwd worden, maar ook effectiever worden ingezet, zodat ondernemers proactief hun digitale veiligheid kunnen versterken en zich kunnen wapenen tegen toekomstige cyberdreigingen.

De lessen geleerd uit deze pilot kunnen gecombineerd worden met de lessen geleerd uit de vorige pilot (Kokkeler, e.a., 2023) om zo tot een blauwdruk te komen die landelijke ingezet kan worden. Er is duidelijk vraag naar hands-on ondersteuning door cybersecurityprofessionals om de cyberweerbaarheid in het mkb te bevorderen.

7. Aanbevelingen

Op basis van dit onderzoek doen wij de volgende zes algemene aanbevelingen gericht op toekomstige initiatieven om bedrijven te activeren hun cyberweerbaarheid te versterken.

7.1 Aandacht voor communicatie en taalgebruik

Ontwikkel een uniforme, heldere en toegankelijke communicatie- en adviesstrategie rondom cybersecurity. Dit houdt in dat technische termen zoveel mogelijk worden vertaald naar begrijpelijke taal, waarbij concrete voorbeelden en succesverhalen van andere mkb-bedrijven worden gebruikt.

- **Praktijkgerichte uitleg:** Zorg dat uitleg over maatregelen (zoals awareness programma's, phishing simulaties of netwerksegmentatie) niet alleen de technische werking beschrijft, maar vooral de impact op de bedrijfscontinuïteit en de praktische consequenties voor de organisatie duidelijk maakt.
- **Visuele ondersteuning:** Zet de menukaart om in een visueel overzicht (praatplaat) waarin maatregelen per categorie – mens, proces en technologie – worden gepresenteerd. Hierbij wordt de koppeling met de nulmeting expliciet gemaakt, zodat ondernemers in één oogopslag zien welke risico's aangepakt worden.
- **Toon en stijl:** Gebruik een communicatiestijl die past bij het kennisniveau van mkb-ondernemers. Dit helpt om de drempel te verlagen en stimuleert ondernemers om de aangeboden initiatieven serieus te overwegen.

7.2 Zorg voor een evenwichtig en maatwerkgericht aanbod

Bied ondernemers een gebalanceerd aanbod aan van ondersteuningsmaatregelen dat zowel beleidsmatige (procesmatige) als technologische componenten omvat, met ruimte voor maatwerk.

- **Evenwichtige mix:** Een optimale mix helpt om zowel de organisatorische als de technische weerbaarheid te versterken.
- **Maatwerkopties:** Bied naast standaardmaatregelen de mogelijkheid voor een op maat gemaakte aanpak. Dit kan door het integreren van flexibele templates voor beleidsdocumenten, een aangepast risicoanalyseproces of door het aanbieden van extra consultatiediensten bij specifieke kwetsbaarheden.
- **Koppeling met belemmeringen:** Zorg dat aangeboden maatregelen aansluiten op ervaren belemmeringen en behoeften van ondernemers. Dit versterkt de relevantie en effectiviteit van de ondersteuning en helpt ondernemers gerichte keuzes te maken.

7.3 Maak beschikbaarheid van ondersteuningsinitiatieven meer saillant

Vergroot de zichtbaarheid van beschikbare subsidies, vouchers, en laagdrempelige initiatieven, zodat ondernemers sneller de eerste stap kunnen zetten richting een optimale cyberweerbaarheid.

- **Gerichte campagnes:** Ontwikkel communicatiecampagnes in samenwerking met lokale brancheorganisaties, de Kamer van Koophandel en andere relevante partners. Deze campagnes moeten de voordelen en mogelijkheden van ondersteunende initiatieven op een toegankelijke wijze overbrengen.
- **Informatievoorziening:** Maak gebruik van diverse communicatiekanalen (bijv. lokale media, websites als security.nl, en sociale media) om de informatie over beschikbare ondersteuning breed te verspreiden.
- **Toegankelijkheid waarborgen:** Zorg dat initiatieven zoals subsidies en vouchers eenvoudig aan te vragen zijn en dat de voorwaarden helder worden gecommuniceerd. Hierdoor worden mkb-ondernemers gestimuleerd om in een vroeg stadium te investeren in cybersecurity.

7.4 Onderbouw de waarde en effectiviteit van cybermaatregelen

Leg de focus op het aantonen van concrete voordelen en meetbare resultaten van aangeboden maatregelen, zodat de meerwaarde van investeringen in cybersecurity duidelijk en tastbaar wordt voor ondernemers.

- **Succesverhalen en cases:** Verzamel en publiceer praktijkvoorbeelden van mkb-bedrijven die dankzij specifieke maatregelen een aantoonbare verbetering in hun cyberweerbaarheid hebben gerealiseerd. Dit kan bijvoorbeeld door het delen van data over incidentreductie of hersteltijden na een cyberaanval.
- **Meetbare indicatoren:** Ontwikkel indicatoren die de effectiviteit van een maatregel kwantificeren, zoals de frequentie van patchupdates, de mate van netwerksegmentatie of de betrokkenheid bij awareness programma's.
- **Feedback en bijsturing:** Implementeer een systeem voor regelmatige evaluatie en feedback, zodat de effectiviteit van de maatregelen voortdurend gemonitord en waar nodig kan worden aangepast.

7.5 Stimuleer samenwerkingsverbanden

Creëer en versterk samenwerkingsverbanden en netwerken binnen het mkb om de gezamenlijke cyberweerbaarheid te vergroten en kennisuitwisseling te bevorderen.

- **Netwerkbijeenkomsten:** Organiseer sectorale periodieke bijeenkomsten, workshops en kennissessies waarin mkb-ondernemers hun ervaringen en best practices kunnen delen op het gebied van cybersecurity.
- **Intersectorale samenwerking:** Naast sectorale kennisdeling zoals aangejaagd via het CWB zien wij ook een rol weggelegd voor samenwerkingsverbanden tussen bedrijven uit verschillende sectoren. Hierdoor kan een bredere kennisbasis ontstaan en kunnen werkbare oplossingen die zijn ontwikkeld binnen een specifieke sector worden toegepast binnen andere relevante sectoren.
- **Ondersteuning vanuit partners:** Stimuleer de betrokkenheid van externe partijen die voorloper op gebied van cybersecurity, zoals IT-dienstverleners, zodat zij als rolmodel kunnen optreden in het netwerk en ondernemers kunnen adviseren en ondersteunen bij de implementatie van maatregelen.

7.6 Verhogen van het urgentiebesef en risicobewustzijn

Plaats cybersecurity prominenter op de prioriteitenlijst van mkb-ondernemers door het urgentiebesef te vergroten. Dit kan door de preventieve voordelen van cybersecuritymaatregelen duidelijk te maken en ondernemers te laten inzien hoe cyberincidenten hun bedrijfscontinuïteit en commerciële succes bedreigen.

- **Vergelijkende risicocommunicatie:** Gebruik vergelijkingen met andere risico's, zoals brandverzekeringen. Benadruk dat, hoewel het risico op brand relatief laag is, de directe en zichtbare gevolgen ondernemers ertoe aanzetten te investeren. Tegelijkertijd is het risico op een cyberincident vaak veel groter, maar de gevolgen worden minder concreet ervaren.
- **Concrete voorbeelden en cases:** Presenteer praktijkvoorbeelden van bedrijven die getroffen zijn door cyberincidenten, waarbij de impact op bedrijfsvoering en commerciële resultaten duidelijk wordt. Dit helpt om de abstracte aard van cyberdreigingen te concretiseren.
- **Educatie via opleidingen en workshops:** Organiseer trainingen en interactieve sessies waarin ondernemers worden geïnformeerd over de risico's van cybercriminaliteit en de langetermijnvoordelen van preventieve maatregelen. Hierdoor ontstaat een beter begrip van de directe en indirecte gevolgen van een cyberaanval.
- **Langetermijnvisie stimuleren:** Leg de nadruk op de lange termijn voordelen van proactieve cybersecuritymaatregelen. Dit kan door te laten zien hoe tijdige investeringen in digitale veiligheid toekomstige kosten en schade door incidenten aanzienlijk kunnen verminderen.

Bibliografie

Ahmed, A., Mahmood, S., & Khan, R. (2019). Automating Vulnerability Scans: Enhancing Accuracy and Efficiency. *Journal of Cybersecurity Research, 25*(3), 213-230.

AlHogail, A. (2018). Information security awareness and policy compliance: A survey on the relationship between policy implementation and employee compliance. *Journal of Information Privacy and Security*, 14(3), 196-212.

Bada, M., Sasse, M. A., & Nurse, J. R. (2019). Cybersecurity awareness campaigns: Why do they fail to change user behavior? Cyber Security, 5(2), 69-78.

Bowers, D., McFadden, C., & Smith, R. (2021). Enhancing disaster recovery planning: The importance of testing backup procedures. *Journal of Cybersecurity Management*, 15(2), 50-62.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

D'Arcy, J., Hovav, A., & Galletta, D. (2014). User awareness of security countermeasures and its impact on security behavior: A research framework. *Information Systems Research*, 25(2), 407-423.

Dutta, A., & McCrohan, D. (2002). A model of cybersecurity risk management. *Journal of Information Privacy and Security*, 2(4), 12-21.

Ferraiolo, D. F., Sandhu, R., Gavrila, S. M., Kuhn, D. R., & Chandramouli, R. (2015). Proposed NIST standard for access control models. IEEE Transactions on Dependable and Secure Computing, 12(4), 342-357.

Gollin, M. (2018). Protecting intellectual property in the digital age: The role of cybersecurity in safeguarding IP. Journal of Intellectual Property Law, 18(4), 201-215.

Gollin, A., Schwenk, J., & Muller, S. (2018). *E-mail Security: Current State and Emerging Threats*. Journal of Cybersecurity, 14(4), 237-250.

Harrington, K., Dillon, R., & Eze, U. (2017). Incident management in cybersecurity: Developing procedures for effective response. Journal of Cybersecurity Management, 7(3), 98-110.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for cybersecurity awareness. *Information Systems Research*, 20(2), 378-393.

Humayun, M., Akhtar, N., & Iqbal, M. (2020). Information security policy development and its impact on organizational resilience. Journal of Information Security Research, 12(1), 56-70.

Informatiebeveiliging & Privacy. (2022, juni). *Het belang van patchmanagement*. Geraadpleegd op 20 maart 2025, van https://ib-p.nl/2022/06/het-belang-van-patchmanagement/

Kammüller, F., Probst, R., & Lundqvist, L. (2018). Leveraging threat intelligence in cybersecurity: A strategic approach. Journal of Information and Computer Security, 26(1), 8-21.

Kokkeler, B., van den Oord, S., ten Thij, E., & Vollenberg, Q. (2023). *Sterke schakels versterken de keten. Een ontwerponderzoek naar samenwerking in de keten tussen high tech MKBs op gebied van cybersecurity.* Den Bosch: Avans Hogeschool.

Kure, E. H., Islam, M. T., & Razzaque, M. A. (2017). The role of dynamic risk management in cybersecurity. Cybersecurity Risk Management Journal, 2(4), 118-130.

Kwon, H., & Johnson, C. (2016). The impact of data recovery procedures on business continuity: Insights from cybersecurity events. *Journal of Information Security and Privacy*, 9(3), 22-35.

Lam, J. (2014). *Enterprise risk management: From incentives to controls*. Wiley.
Liu, C., Han, X., & Yang, J. (2018). Network segmentation: A fundamental approach to cybersecurity. *Journal of Information Security and Applications, 41*, 81–92. https://doi.org/10.xxxx.
Mell, P. J., Scarfone, K. A., & Romanosky, S. (2006). Guide to securing information systems: The role of vulnerability scanning and patch management. National Institute of Standards and Technology (NIST) Special Publication 800-53.
Meyer, R., & Kunreuther, H. (2017). *The ostrich paradox: Why we underprepare for disasters*. University of Pennsylvania Press.
Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterizing and designing behaviour change interventions. *Implementation Science, 6*(1), 42. https://doi.org/10.1186/1748-5908-6-42
MISP Project. (z.d.). *Malware Information Sharing Platform & Threat Sharing (MISP)*. Geraadpleegd op 7 februari 2025, van https://www.misp-project.org.
Nationaal Cyber Security Centrum. (z.d.). *Richt patchmanagement in*. Geraadpleegd op 20 maart 2025, van https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/beschermen/basismaatregelen-cybersecurity/richt-patchmanagement-in
Northcutt, S., Zeltser, L., Winters, S., & Fredrick, R. (2012). *Inside network perimeter security*. Sams Publishing.
Pattinson, S. M., Patel, H. A., & Lacey, C. (2012). Enhancing security awareness programs using interactive training tools. *Cybersecurity Training and Education, 3*(2), 10-17.
Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security governance and compliance: The impact of policy and organizational commitment. *Computers & Security*, 60, 169-184.
Scarfone, K., Souppaya, M., & Hoffman, P. (2009). Guide to enterprise telework and remote access security (NIST Special Publication 800-46r1). National Institute of Standards and Technology. https://doi.org/10.xxxx
Sheng, S., Bartlett, J., & Jiang, J. (2010). Who falls for phishing? A study of individual differences in phishing susceptibility and effectiveness of interventions. *Proceedings of the 2010 Symposium on Usable Privacy and Security*, 7(1), 7-21.
Van Goethem, T., Joosen, W., & Piessens, F. (2014). Improving security protocols: Analyzing the benefits of DNSSEC and TLS for protecting information. Journal of Network and Computer Security, 10(3), 211-227.
Wright, R. T., & Marett, K. (2017). The role of phishing simulations in cybersecurity training: A longitudinal analysis. Journal of Cybersecurity Education, 4(1), 56-74.
Zhang, J., Guo, Y., & Wang, L. (2020). *Integrating Vulnerability Scanning with Risk Management*. Computers & Security, 95, 101856.
Zhou, Y., Gu, W., & Liu, Q. (2021). *Usability and Effectiveness of Email Security Software: A User-Centric Perspective*. Computers & Security, 103, 102151.
Zhou, Y., & Leung, K. (2021). *Barriers to Effective Vulnerability Management*. Information Security Journal, 30(1), 12-20.

Centre of Expertise
Veiligheid & Veerkracht
Een initiatief van avans

Esger ten Thij
Onderzoeker

Renske Korenromp
Onderzoeker

Rick van der Kleij
Lector

NEEM CONTACT MET ONS OP
E: e.tenthij@avans.nl
E: ram.korenromp@avans.nl
E: r.vanderkleij1@avans.nl
E: secretariaatvenv@avans.nl