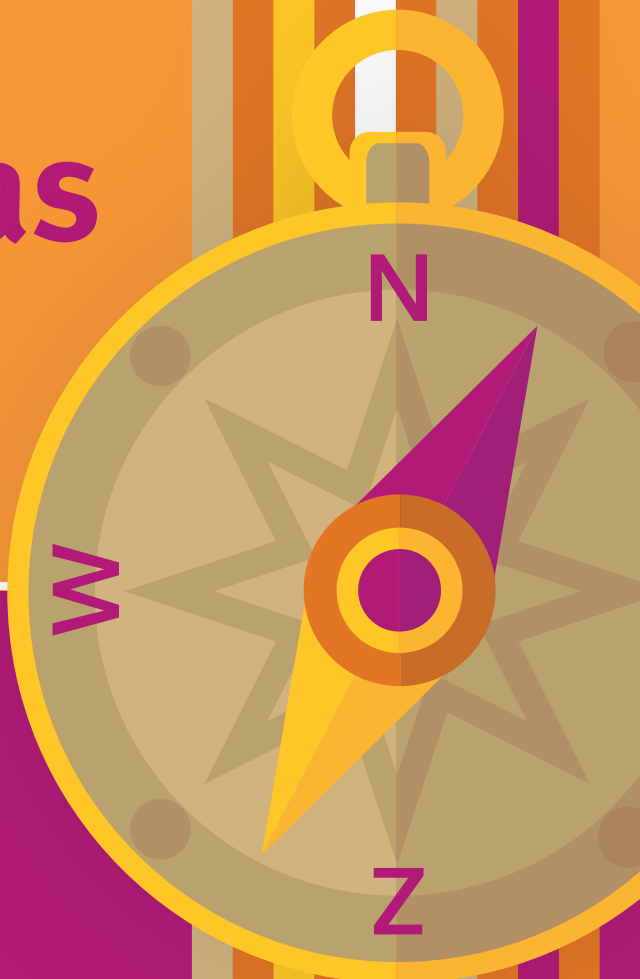
Cyberkompas

voor Ondernemend Nederland



Cybersecurity Alliantie

Voorwoord

Beste lezer,

Het is zover: het eerste Cyberkompas voor Ondernemend Nederland ligt voor u. Een kompas dat u zicht geeft op digitale ontwikkelingen in de komende twee jaar die van invloed kunnen zijn op uw cyberveiligheid. Met dit inzicht biedt de Cybersecurity Alliantie (CSA) u perspectief waardoor het ontwikkelen van een daadkrachtig en effectief beleid voor uw cyberweerbaarheid afgestemd kan worden op de toekomst voor uw onderneming.

De digitale transitie in Nederland gaat razendsnel. Maatschappelijke, economische en technologische ontwikkelingen gaan in een snel tempo vooruit en geven daarmee vorm aan onze digitale toekomst. Hierdoor ontstaan ook nieuwe uitdagingen. Het is daarom van groot belang dat ondernemend Nederland zicht krijgt op deze ontwikkelingen, zich op de toekomst kan voorbereiden en, waar nodig en mogelijk, tijdig kan bijsturen. Uiteindelijk willen we allen een veilige digitale samenleving.

In een periode waarin de hele maatschappij gebukt ging onder de pandemie, is het de Cybersecurity Alliantie toch gelukt de juiste mensen bijeen te brengen om dit kompas te realiseren. Via virtuele expertmeetings is alle kennis bij elkaar gebracht door enthousiaste leden van de Alliantie.
Af en toe dreigden de verscherpte corona-maatregelen het proces ernstig te vertragen, maar het doorzettingsvermogen van alle betrokkenen heeft toch overwonnen en geleid tot de eerste versie van dit levende document.

Ik wil dan ook graag alle betrokken adviseurs en experts (Michelle de Boer, Marjolijn Bonthuis, Janet Cadel, Margreet Drijvers, Elif Duru, Liesbeth Holterman, Diederik van Luijk, Jeroen Kasbergen, Marnix Korlaar, Liebeth Kruizinga, Iris Koster, Nicole Mallens, Sjaak Schouteren, Jelle Niemantsverdriet, Julia Peeters, Eleonora Petridou, Kees Plas, Serge van der Schaft, Jeroen Steenbakkers, Stephanie Teeuwen, Mieke van Ulden, Martin Vliem, Michael Vos, Esther van der Weide en Rosa van Zijl Jansen) enorm bedanken voor hun waardevolle bijdragen aan dit kompas.

Voor u veel leesplezier en succes met uw cyberweerbaarheid strategie.

Met vriendelijke groet,

Evert van Zanten (PvIB)
Voorzitter werkgroep Cyberkompas voor Ondernemend Nederland

Inhoud

Inleiding

In deze snel veranderende maatschappij is het belangrijk om digitaal weerbaar te blijven. Ontwikkelingen in het digitale domein gaan razendsnel en de complexiteit neemt toe. Juist voor ondernemend Nederland is het van belang om niet alleen zicht te hebben op de uitdagingen die op ons afkomen, maar vooral ook perspectief te hebben hoe hier adequaat mee om te gaan.

Om dit goed weer te geven, heeft de Cybersecurity Alliantie (CSA) het **Cyberkompas voor Ondernemend Nederland** ontwikkeld. Het kompas heeft dezelfde thema's, basis- en uitgangspunten als het Cyberkompas van het Nationaal Cyber Security Centrum (NCSC) voor de vitale sector, maar verschilt daarvan door zich meer te richten op een kortere termijn en het aanreiken van voorbeelden en acties die ondernemers in Nederland kunnen toepassen.

Het Cyberkompas voor Ondernemend Nederland is opgebouwd rond acht thema's die toekomstige richtingen aangeven. Voor ieder thema zijn een omschrijving van het thema, versnellers en vertragers beschreven. Ook de concrete verwachtingen worden verder omschreven. Per verwachting zijn mogelijke gevolgen, verwachte relevantie en een verwacht doorbraakmoment opgesteld. Tot slot zijn er aanwijzingen vastgesteld die wijzen op een doorbraak.

Het kompas biedt ook de mogelijkheid om met een scherpe blik naar de toekomst te kijken. Het Cyberkompas voor Ondernemend Nederland heeft als doel om op termijn te dienen als een interactief instrument waarmee onder andere inzicht en bewustwording kan worden gerealiseerd. Organisaties kunnen zo zelf rekening houden met de voor hen geldende digitale uitdagingen en de vraagstukken op het gebied van cybersecurity.

Bij het opstellen van dit document is ervoor gekozen om geen verdiepingsslag te maken naar een specifieke branche of waardeketen. Het kompas is zo opgesteld dat het een handvat biedt aan intermediairs om deze vertaalslag te maken naar voor hun specifieke branchegerelateerde ontwikkelingen. Hierdoor kunnen zij hun achterban van informatie voorzien en ondersteunen bij passende maatregelen. Wilt u direct aan de slag met één van de thema's dan kunt u ondersteuning vinden op de website van het Digital Trust Center (www.digitaltrustcenter.nl) en kennispartners vinden via de Wegwijzer voor cybersecurity initiatieven.

De digitale wereld is continu in beweging. Het Cyberkompas beweegt hierin mee en wordt met enige regelmaat voorzien van een update. Uw input hiervoor is uiteraard onmisbaar. Heeft u daarom toevoegingen, aanvullingen of correcties op het Cyberkompas? Geef deze dan vooral door via: csa@ecp.nl.

Thema

Digitalisering tot in haarvaten maatschappij

Doordat bijna elke organisatie afhankelijk is van technologie, kan in zekere mate worden vastgesteld dat organisaties - naast hun dagelijkse werkzaamheden - tegenwoordig ook actief zijn als IT-bedrijf. Ondernemers zijn afhankelijk van digitale technologie en de verwachting is dat deze afhankelijkheid nog verder zal toenemen. De toepassing van deze gedigitaliseerde processen loopt naadloos over naar de bedrijfsprocessen van ondernemingen. Verder kent deze vervlechting ook geen landsgrenzen meer doordat bijvoorbeeld data wordt opgeslagen in de clouddiensten van buitenlandse partijen of vanuit andere landen benaderd wordt.

Voorbeelden

- Een volledig digitaal betaalproces voor winkels.
- Online klantenservices met mail en chat opties.
- Het gebruik van online reserveringssystemen.
- Organisaties waar processen zijn geautomatiseerd op basis van ‘make to order’ door de consument.

Versnellers

- Continue verbetering van producten en diensten en de digitale toegankelijkheid daartoe.
- Toestroom nieuwe diensten die online en real life verder integreren, gebaseerd op nieuwe technologie.
- Toename populariteit van het hybride werken.
- Maatschappelijke problemen waarvoor alleen oplossingen met nieuwe technologie voldoen (controleren van vaccinatie- of testbewijs via QR-codes in de CoronaCheck-app).

Vertragers

- Privacy- en veiligheidsoverwegingen.
- Verminderende toegankelijkheid voor mensen die minder digitaal onderlegd zijn.
- Maatschappelijke discussie.

Verwachtingen:

Meer nadruk op omgang met klantgegevens en privacy

Door de toenemende digitalisering van informatieverstrekking wordt er meer nadruk gelegd op hoe ondernemers op een verantwoorde manier omgaan met de gegevens en privacy van klanten. Door deze toename kunnen ondernemers het gevoel krijgen dat ze mee moeten met de ontwikkelingen om zo bij te blijven. Hierdoor is het mogelijk dat ze minder doorhebben wat de risico’s of voordelen van dataverzameling zijn. De vraag die ook actueel blijft is of het opslaan van teveel klantgegevens wel noodzakelijk is.

Mogelijke gevolgen: Bedrijven verzamelen meer data dan ze daadwerkelijk nodig hebben en realiseren zich niet meer welke data ze allemaal van hun klanten hebben. Door weinig voorbereiding op de mogelijke gevaren van dataverzameling, kunnen zij als gevolg kwetsbaar zijn voor ransomware-aanvallen en datalekken. Verder ontstaat er een verkrampte houding ten aanzien van het verzamelen van relevante data, waardoor de concurrentiepositie mogelijk verslechtert.

Verwachte relevantie: hoog

Verwachte doorbraak(moment): 2021-2022

Indicatoren die wijzen op doorbraak:
Gezondheidschecks waar nu al om wordt gevraagd. Meer bedrijven gaan sinds de lockdown online ondernemen. Verplichtingen vanuit de overheid tot het gebruik van specifieke digitale middelen, zoals de CoronaCheck app.

Internet of Things (IoT) nemen risico’s met zich mee

De continue verbetering van slimme IoT-producten zorgt ervoor dat digitalisering weliswaar meer fysieke vormen krijgt, maar ook minder zichtbaar wordt. Daarnaast wordt het ook vanzelfsprekend dat producten en diensten met elkaar verbonden zijn. Gebruikers kunnen zo minder begrijpen hoeveel techniek er achter een product, zoals een slimme deurbel, zit.

Mogelijke gevolgen: Mensen die minder digitaal onderlegd zijn, kunnen ontmoedigd raken voor het gebruik van slimme online diensten en producten.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2022

Indicatoren die wijzen op doorbraak: Toenemende ontwikkelingen rond bedrijven die onderdeel zijn van de online-platformeconomie. Structureel toenemend gebruik van IoT producten door consument.

Toename wet- en regelgeving

De wet- en regelgeving die toeziet op cybersecurity neemt toe. Cybersecurity wordt steeds belangrijker in de huidige maatschappij, waardoor ook het belang van bijbehorende problemen groter wordt. Hiermee neemt de behoefte aan heldere wetgeving omtrent dit onderwerp toe. Als gevolg van (toekomstige) ontwikkelingen in de economie, kunnen deze wetten ook buiten hun werkingsgebied een rol spelen. Veel multinationals zullen ervoor kiezen om toe te werken naar de vereisten van de hoogste standaarden wanneer ze geconfronteerd worden met deze wetgeving in meerdere landen.

Voorbeelden

- Kaderstellende wet- en regelgeving, zoals de AVG.
- Verschil tussen regelgeving en wat ondernemers moeten doen aan cybersecurity.
- Achterlopende wet- en regelgeving.
- Privacy overschrijdende wet- en regelgeving vanuit de noodzaak van toezicht en opsporing.

Versnellers

- Impactvolle gebeurtenissen in de maatschappij, zoals de coronacrisis en terreurdreiging, die gebreken huidige aanpak blootleggen.
- Het meer en meer grensoverschrijdende karakter van digitale producten en diensten.
- Internationale inmenging in nationale aangelegenheden.

Vertragers

- Concurrentiestrijd in diverse sectoren.
- Verschil in inzicht van noodzaak en impact cyberweerbaarheid.
- (Internationale) bestuurlijke besluitvorming.
- Gebrek aan tijdig goede alternatieve producten en diensten.
- Onmogelijkheid tot brede implementatie, naleving en toezicht.

Verwachtingen:

Wetgeving en branche regelgeving omtrent cybersecurity blijft achter lopen[1]

Cybersecurity standaarden zijn nog te weinig gemeengoed. Ondernemers maken er geen prioriteit van, omdat er niet naar wordt gevraagd. Dit komt voornamelijk omdat de wet- en regelgeving op het gebied van cybersecurity achterloopt.

Mogelijke gevolgen: Zonder duidelijk wet- en regelgeving vanuit de overheid kunnen grote Europese bedrijven zelf hun eigen regelgeving instellen en deze eventueel opleggen aan leveranciers of afnemers in de keten. De mogelijkheid bestaat dat het lastiger wordt voor kleinere ondernemers om aan de door grote bedrijven opgestelde regelgeving te voldoen.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2021 - 2022

Indicatoren die wijzen op doorbraak:
De bewustzijn van het gevaar van cyberaanvallen is nog niet op hetzelfde niveau als wat er op dit moment gebeurt. Bewustzijn omtrent cyberaanvallen is algemeen aanwezig, maar dat deze aanvallen de bedrijfsvoering van ondernemers kunnen treffen is minder bekend.

Belangrijkere rol voor brancheverenigingen en waardeketens

Brancheverenigingen kunnen een grote rol spelen om bewustzijn en regelgeving te creëren omtrent de cyberweerbaarheid van ondernemers. Goede afspraken voor een veilige omgeving zijn daarvoor nodig. Brancheverenigingen zijn echter vaak te klein van omvang om veel aandacht aan cyberweerbaarheid te besteden.

Mogelijke gevolgen: Er is een toenemende behoefte aan schaalbare en begrijpelijke ondersteuning op het gebied van cybersecurity voor ondernemers. Hierdoor kunnen er in branches een zelf-regulerend en coördinerend principe ontstaan, waarbij ondernemers kennis kunnen overdragen.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2021-2022

Indicatoren die wijzen op doorbraak:
Er wordt structureel informatie gedeeld met branches en ondernemers over cyberdreigingen. Verder vermeldt Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in het Cybersecuritybeeld Nederland 2021 (CSBN, 2021, p. 29) dat ransomware als maatschappij ontwrichtend kan worden gezien en steeds meer ondernemers last hebben van ransomware-aanvallen.

Belemmering door complexiteit en snelheid cyberaanvallen

De mate en snelheden van cyberaanvallen nemen in een snel tempo toe. Het gevolg hiervan is dat de core business van ondernemers bedreigd wordt wanneer zij niet cyberweerbaar zijn.

Mogelijke gevolgen: Doordat cyberaanvallen krachtiger van aard worden, kan dat als gevolg leiden tot financiële-, bedrijfs- en/of imagoschade. In het ergste geval kan dit zorgen voor faillissementen, omdat de verwachting is dat zulke aanvullen door de meeste verzekeringsmaatschappijen niet meer worden gedekt. De aansprakelijkheid komt daardoor op het bordje van ondernemers terecht. Er is daarom meer waakzaamheid en veerkracht nodig.

Verwachte relevantie: hoog

Verwachte doorbraak(moment): 2021

Indicatoren die wijzen op doorbraak:
Toename van cyberaanvallen bij internationale bedrijven en ondernemers. Er is ook meer aandacht voor de openheid van slachtoffers, waarbij zij zich ervan bewust worden dat reputatieschade mogelijk meevalt bij transparante, tijdige en eerlijke communicatie.

1 Minimumeisen aan digitale veiligheid slimme apparaten - Rijksoverheid: https://www.rijksoverheid.nl/actueel/nieuws/2021/10/29/minimumeisen-aan-digitale-veiligheid-slimme-apparaten

Thema

Intelligentere mobiliteit

Er vindt een grote ontwikkeling plaats op het gebied van systemen die mobiliteit autonoom maken en intelligente systemen die deze mobiliteit ondersteunen in bijvoorbeeld infrastructuur en verkeersregelsystemen. Techniek speelt hierbij, samen met onder andere de maatschappelijke en juridische aspecten, een centrale rol. De connectiviteit op de weg neemt ook toe. Voertuigen hebben onderling interactie, met de omgeving en met de infrastructuur. Deze ontwikkeling ondersteunt de verkeersveiligheid en zorgt voor een efficiënter gebruik van de weg. De vraag is wat deze ontwikkeling gaat betekenen voor de privacy van bestuurders, werknemers en reizigers.

Voorbeelden

- Timers die bijhouden hoe lang een vrachtwagenchauffeur aan het rijden is.
- Planningsystemen die aangeven waar vracht naartoe moet.
- Intelligente Ruimtelijke Informatie Technologie (RIT) Systemen, gebaseerd op tracking en tracing via IoT.
- Autofabrikanten komen/zijn in bezit van enorme hoeveelheden reis- en gebruiksdata.

Versnellers

- Regelgeving die (semi) autonoom rijden toestaat.
- Testen die aangeven dat dit soort systemen rijden veiliger maken.
- Stimulerende maatregelen overheid, zoals de lease-bijtelling voor schone auto's.
- Klimaatdiscussie wordt steeds meer gevoerd.
- Invoering van beprijzen van gebruik (rekeningrijden).

Vertragers

- Zorgen over fysieke veiligheid, incidenten met verstoring van dergelijke systemen.
- Ontbreken van regelgeving over data-eigenaarschap.
- Big Brother discussie die gevoerd wordt vanuit behoefte aan toezicht (overheid) en behoefte aan privacy (consument).

Verwachtingen:

Transitie van fossiel naar elektrisch rijden brengt nieuwe uitdagingen met zich mee

Elektrisch rijden wordt meer gestimuleerd door de overheid. Naast particulieren zijn er ook bezorgdiensten die een volledig elektrisch voertuig gebruiken om hun goederen aan klanten te leveren. De nieuwe uitdagingen van elektrisch rijden liggen vooral bij de vraag of er voldoende netcapaciteit is en of er aan de groeiende vraag naar laadinfrastructuur kan worden voldoen.

Mogelijke gevolgen: De afhankelijkheid van de beschikbaarheid van elektriciteit en systemen groeit, terwijl er geen 'analoog' alternatief meer is. Daarnaast zorgt het (semi) autonoom rijden voor meer veiligheid, maar is er tegelijkertijd wel de zorg over de aansprakelijkheid en software-eisen.

Verwachte relevantie: hoog

Verwachte doorbraak(moment): 2021 - 2022

Indicatoren die wijzen op doorbraak:
Groeiend aantal laadpunten in de publieke ruimte. Toename elektrische en hybride auto's op het wegennet.

Groeiende kansen voor ondernemers om in te spelen op efficiënter goederen transport

Met digitale systemen die meten en registreren waar voertuigen zich bevinden, wordt het mogelijk om efficiënter en dynamischer ritten te plannen. Hierdoor kan de capaciteit van transport worden vergroot, omdat veel vrachtwagens nu nog met een lege inhoud de weg op gaan.

Mogelijke gevolgen: De distributieketen zal veranderen. Deze verandering creëert kansen voor het mogelijk sneller en goedkoper transporteren van goederen. Verder kan dit worden versterkt wanneer de logistieke sector data deelt, wat effectiviteit en efficiëntie bevorderd. Daarnaast kan de differentiatie in diensten tussen de stad en het platteland een rol spelen door mogelijke operationele belemmeringen. De transitie zorgt ervoor dat de ondernemer een keuze heeft om zelf mee te veranderen of zichzelf aan te sluiten op online platformen die de effectiviteit en efficiëntie bevorderd. Dit laatste creëert echter een nieuw soort afhankelijkheid wat kan leiden tot een gewijzigd businessmodel.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2021 - 2022

Indicatoren die wijzen op doorbraak:
Verandering van wijze waarop goederen worden getransporteerd, zoals Amazon Air.

Thema

Homogenisering van digitale landschap

Big Tech-bedrijven blijven in de maatschappij de dienst uitmaken. Op brancheniveau zijn er vaak geen alternatieve aanbieders. Het gevaar schuilt hierin dat er steeds gebruik wordt gemaakt van dezelfde technologische oplossingen, afkomstig van steeds dezelfde partijen. De impact voor ondernemers ligt voornamelijk bij de bewustwording van de afhankelijkheid van deze technische systemen voor hun dagelijkse werkzaamheden.

Voorbeelden

- Planningssysteem in de kinderopvang.
- Administratietool via de tandartsenvereniging.
- Data en locatie.
- Reissystemen die allemaal van dezelfde grote transactieplatformen gebruik maken.
- Betalingssystemen.
- Logistieke transactieplatformen.

Versnellers

- Gezamenlijke initiatieven om de afhankelijkheid van systemen te verminderen en de stabiliteit en beschikbaarheid te verhogen.
- Behoefte en gedrag consument eist versnelling op niveaus die steeds minder partijen kunnen bieden.

Vertragers

- In zee gaan met verkeerde partijen.
- Regelgeving (AVG) niet in acht nemen.
- Onbewustzijn cyberrisico's bij organisaties.
- Cyberweerbaarheid in de keten niet op orde.
- Grote partijen zijn regelmatig slachtoffer van onder andere ransomware-aanvallen.

Verwachtingen:

Verhogen bewustwording over afhankelijkheid en risico's Big Tech-diensten

Ondernemers zijn steeds vaker afhankelijk van enkele sleutelspelers op het digitale speelveld. Deze grote IT-bedrijven en aanbieders zijn vaak zichtbaar en de diensten zijn makkelijk te gebruiken door ondernemers. Veel ondernemers maken daarom gebruik van hun (online) diensten voor bijvoorbeeld de kantoorautomatisering, het voorraadbeheer of de administratie. Zelfs als ondernemers diensten afnemen van kleinere, nationale of regionale spelers, kunnen ze ongemerkt gebruik maken van grote aanbieders die de (cloud) technologie leveren aan deze kleine aanbieders.

Mogelijke gevolgen: Als brancheorganisaties geen actieve rol innemen, zal het zeker bij kleinere organisaties tot onnodige vertraging leiden om tot een effectief cyber risk management beleid te komen. Wanneer branchеverenigingen meer als één persoon/entiteit acteren en een gezamenlijk standpunt innemen, kunnen zij meer macht/controle uitoefenen op ICT-dienstverleners.

Verwachte relevantie: hoog

Verwachte doorbraak(moment): 2021 - 2022

Indicatoren die wijzen op doorbraak:
Er is een stijging van de penetratiegraad voor cyberverzekeringen. Verder is er aandacht voor de risico's bij (branche)organisaties en zijn er gerechtelijke uitspraken over de reikwijdte van de zorgplicht bij serviceproviders. het wegennet.

Ondernemer heeft inzicht nodig van de consequenties van een contract

De contracten die ondernemers sluiten, moeten op juridisch gebied zorgvuldig worden bestudeerd. Maar de vraag is of ondernemers de juridische bepalingen kunnen begrijpen. Met name contracten en Service Level Agreements (SLA's) van Big Tech-bedrijven zijn vaak goed dichtgetimmerd om op 'homogene wijze' een zo groot mogelijke digitale markt te bedienen, waardoor er voor een ondernemer weinig ruimte is om individueel afspraken te bespreken of te veranderen.

Mogelijke gevolgen: Wanneer ondernemers bekend zijn met de verschillende contracten, kunnen verwarringen of misverstanden tijdig worden voorkomen. Daarom is het belangrijk dat de afspraken en (onverwachte) kosten duidelijk op papier worden gezet en niet alleen mondeling worden overeengekomen. Daarnaast dienen bij het aandragen van meerdere oplossingen of alternatieven de voor- en nadelen duidelijk te zijn voor ondernemers. Hoe meer inzicht en interesse zij hebben in de materie, hoe groter de kans op bereidheid en medewerking zal zijn om risico's te verkleinen.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2021 - 2022

Indicatoren die wijzen op doorbraak:
Steeds meer incidenten vinden plaats, waarbij kwetsbaarheden bij een grote speler tot maatschappij ontwrichtende uitkomsten kunnen leiden. De storing waarbij Facebook, Instagram en WhatsApp lange tijd niet beschikbaar waren, zorgde ervoor dat ondernemers onder andere hun verkoop- en communicatiekanaal tijdelijk kwijt waren.

Monopolisering digitaal domein

Een beperkt aantal grote marktpartijen domineert vrijwel de gehele digitale markt. Een kleine groep leveranciers levert diensten die in vrijwel alle ketens terugkomen. In 2022 verwacht de Autoriteit Consument en Markt (ACM) hun conclusies te presenteren over de huidige stand van de markt. Naar aanleiding van dit onderzoek zal dit onderdeel van het kompas verder worden uitgewerkt. Daarom wordt vooralsnog dit thema geduid op basis van het Cyberkompas van het NCSC[2].

Voorbeelden

- We zijn vrijwel allemaal gebruiker van de diensten van de Big Tech.

Versnellers

- Lobby krachten en technology push waarbij technische mogelijkheden aanbodgedreven worden toegepast.
- Misbruik van bestaande monopolies, vendor lock-in waarbij de afnemer niet in staat is eenvoudig van leverancier te wijzigen.

Vertragers

- Ingrijpen door overheden via wetgeving en/of mededingingsmaatregelen en opsplitsing.
- Geopolitieke ontwikkelingen.

Verwachtingen:

Schaalvoordelen zorgen voor uniforme beveiligingsmechanismen

Grote organisaties kunnen nieuwe technologie met verbeterde beveiliging gemakkelijker ontwikkelen, maar ook afdwingen bij gebruik van de dienstverlening. Door hun omvang zijn de kosten voor de ontwikkeling van nieuwe beveiligingsmechanismen relatief laag. Het behaalde effect is door de schaalgrootte al snel interessant, omdat een kleine verbetering al winst oplevert.

Mogelijke gevolgen: Door beveiligingsmechanismen af te dwingen, kan worden voorkomen dat simpele technieken effectief zijn voor het hacken van systemen.

Verwachte relevantie: hoog

Verwachte doorbraak(moment): 2021 - 2022

Indicatoren die wijzen op doorbraak:
Toename gebruik van twee factor authenticatie en biometrie. Aanbod van Cybersecurity als onderdeel van de dienstverlening.

Bescherming van de gegevens is van belang voor de eigen concurrentiepositie

Het verzamelen en gebruiken van data is een belangrijke concurrentiefactor. Hoe unieker gegevens blijven, des te hoger de waarde voor deze marktpartijen. Beveiligingsincidenten hebben een negatief effect op het imago. Klanten laten de reputatie van de organisatie op het gebied van cybersecurity dan ook zwaarder meewegen in de keuze voor een bedrijf.

Mogelijke gevolgen: Organisaties investeren meer in cybersecurity en gaan concurreren op cybersecurity. Organisaties vallen elkaar actief aan om hun eigen concurrentiepositie te versterken.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2021 - 2022

Indicatoren die wijzen op doorbraak:
Effect op een aantal gebruikers na schandalen, waarbij de privacy van gebruikers geschaad werd.

2 De inhoud van dit thema komt uit Cyberkompas 2019 van het Nationaal Cyber Security Centrum (NCSC): https://www.ncsc.nl/documenten/publicaties/2019/november/27/ncsc-cyberkompas-2019

Toename complexiteit bij een cyber incident

Met de verplaatsing van eigen servers naar software in de cloud, nemen het aantal betrokken organisaties en de gebruikte technieken in de keten toe. Dit zorgt ervoor dat incidenten ook plaatsvinden binnen de eigen organisatie. De noodzaak tot afstemming van informatie en verantwoordelijkheid neemt toe, maar in de praktijk zijn ondernemers hier nog niet mee bezig en hebben ze basis nog niet geregeld.

Voorbeelden

- Afhankelijkheid van leveranciers.
- IT-landschap complexer.

Versnellers

- Snellere adoptiegraad consumenten.
- Eisen vanuit overheid en toezichthouders.

Vertragers

- Angst voor reputatieschade.
- Onbewust van olievlekwerking van een incident.

Verwachtingen:

Meer aanbieders van een managed service dienst

Door de toename van het aantal aanbieders is het IT-landschap complexer geworden. Hierdoor wordt het lastiger om als ondernemer goed voorbereid te zijn op mogelijke incidenten. Om de complexiteit behapbaar te maken, moeten de rollen en verantwoordelijkheden op dit gebied goed worden gedefinieerd. Door de toename van deze diensten moeten ondernemers duidelijke afspraken maken met leveranciers.

Mogelijke gevolgen: Meer complexiteit op het gebied van incident respons zorgen mogelijk voor hogere kosten. Wanneer bedrijven dit goed regelen, ontstaat er voor bedrijven een kans om zaken te doen binnen een keten. Hierdoor kan het mogelijk zijn dat er minder inzicht is in de feitelijke kosten die worden gemaakt. Door de toename van deze complexiteit, wordt innovatie bij ondernemers ook lastiger en kan de gevolgschade onverwacht op ondernemers worden verhaald.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2022

Indicatoren die wijzen op doorbraak:
Consumenten hebben een hogere en snelle adoptiegraad door de opmars van IoT. DIt kan direct impact hebben op de bedrijfsvoering.

Thema

Afname rol van de mens

Er worden steeds meer geautomatiseerde beslissingen genomen in processen. Waar vroeger de mens een afweging maakte op basis van beschikbare informatie en eigen inzicht, wordt dat nu soms overgelaten aan of ondersteund door kunstmatige intelligentie. Dit gebeurt met software op basis van algoritmes, die door de mens worden bedacht, waardoor beslissingen zelfstandig gemaakt kunnen worden. Ook kan software zelflerend zijn (machine learning) op basis van patroonherkenning. De rol van de mens wordt hiermee steeds kleiner in ketens van besluitvormings- en productieprocessen.

Voorbeelden

- Algoritme neemt beslissing bij aanvraag vergunning of verlening subsidies.
- Geautomatiseerde matchingplatformen voor het aannemen van personeel.
- Klanten werven via social media platformen.
- AI algoritmes in acceptatieprocessen bij banken.
- Gebruikmaking van automatisch gegenereerde ‘blacklists’.

Versnellers

- Brede discussie over verantwoorde inzet van Artificial Intelligence (AI).
- Kennisvergroting op dit specifieke thema bij ondernemers.
- (Korte termijn) winst in efficiëntere processen.

Vertragers

- Groeiende kenniskloof tussen ondernemers.
- Toenemende invloed van gebruikers en inzet door ondernemers.
- Maatschappelijke discussie na onethisch gebruik AI.

Verwachtingen:

Artificial Intelligence (AI) zorgt voor objectieve en snellere beslissingen, maar ook voor zorgen vanwege de ondoorzichtigheid van de techniek

Door kunstmatige intelligentie kunnen er objectiever en sneller beslissingen worden genomen. Er zijn echter ook zorgen over deze techniek, wat met name komt door de ondoorzichtigheid van het proces.

Mogelijke gevolgen: De ondoorzichtigheid kan het wantrouwen richting deze ontwikkeling stimuleren. Dit is voornamelijk gebaseerd op de angst voor het verdwijnen van banen. Er ontstaat een digitale bubbel rond ondernemers zonder dat zij daar zelf bewust van zijn.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2021 - 2022

Indicatoren die wijzen op doorbraak:
Samenwerkingsinitiatieven zoals de Nederlandse AI-Coalitie en plannen van de Europese Commissie[3].

Maatwerk wordt steeds moeilijker omdat systemen een groot deel overnemen

Door toenemende standaardisatie wordt het moeilijker om maatwerk te leveren. Dit wordt versterkt wanneer ondernemers niet zo veel kennis hebben over de geautomatiseerde systemen die zij binnen hun bedrijf gebruiken. Aan de andere kant kunnen mensen ook effectiever maatwerk leveren doordat grote delen van het werk worden geautomatiseerd. Hiervoor is het wel essentieel dat de juiste kennis proces- en automatiseringskennis aanwezig is binnen de onderneming en op basis hiervan gekozen wordt voor de ‘menselijke maat’ op de juiste plek.

Mogelijke gevolgen: Een digitaal systeem waarbij een vorm van kunstmatige intelligentie aan de pas komt, zou ondernemers moeten ondersteunen in hun bedrijfsvoering. Hiermee wordt voorkomen dat deze systemen te bepalend worden, waardoor de afhankelijkheid toeneemt. In plaats daarvan kunnen ondernemers beter niet-essentiële werkzaamheden over laten aan computersystemen, zodat mensen binnen een organisatie zich op meer maatwerk gerelateerde werkzaamheden kunnen richten.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2023

Indicatoren die wijzen op doorbraak:
Binnen de keten van ondernemers is er meer discussie met IT-leveranciers over de invulling van digitale systemen. Verder vindt de (ethische) discussie rond AI vervolg in standaarden en regelgeving.

3 EU Legal framework on Artificial Intelligence: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0005.02/DOC_1&format=PDF

Afname vrijheid leveranciers-keuze

Door wet- en regelgeving, de maatschappij en de noodzaak tot voldoende digitale veiligheid zijn op korte termijn een beperkt aantal leveranciers in staat om aan securitywensen en -eisen te voldoen. Daardoor wordt de keuze voor een betrouwbare leverancier ernstig beperkt.

Voorbeelden

- Uitsluiting van ondernemers in bepaalde sectoren.
- Vergrote afhankelijkheid van een besturingssysteem of platform.

Versnellers

- Grotere organisaties ontwikkelen zich sneller in dienstverlening.
- Groeiende kloof tussen grotere en kleinere bedrijven.
- Acceptatie beperkte keuzevrijheid vanwege realiseerbare voordelen korte termijn voor veiligheid en compliancy.

Vertragers

- Verandering in producten van leveranciers.
- Incidenten die laten zien dat beveiliging niet zoveel met landsgrenzen te maken heeft.

Verwachtingen:

Opschaling producten & diensten bij bedrijven zodat ze cyberweerbaarder worden

Wanneer ondernemers beter begrijpen wat ze willen van leveranciers, kunnen ze de juiste vragen stellen en zo een duidelijke keuze hebben. De voordelen hiervan zijn een hoger niveau van standaarden en betere prijstechnische afspraken.

Mogelijke gevolgen: Door standaardisatie in producten en diensten kan het onderscheidend vermogen van ondernemers in gevaar komen. Daarnaast zijn de kosten die worden gemaakt onoverzichtelijk wanneer en in hoeverre zij met hun data willen overstappen naar een ander systeem.

Verwachte relevantie: gemiddeld

Verwachte doorbraak(moment): 2023

Indicatoren die wijzen op doorbraak:
Toenemende standaardisatie op nationaal en Europees niveau, zoals GAIA-X. Er is verder ook meer bewustzijn voor cyberweerbaarheid.

Over de Cybersecurity Alliantie

De Cybersecurity Alliantie biedt een netwerk voor partijen om samen te werken aan een digitaal weerbaar Nederland en biedt partijen een steun in de rug. Door uitvoering van kortlopende cybersecurityprojecten met een concreet resultaat, door inzicht in en overzicht van het Nederlandse cybersecuritylandschap, en door je netwerk te vergroten. Want de veiligheid van één, zorgt voor meer veiligheid voor iedereen.

De Cybersecurity Alliantie werkt samen via publiek-private samenwerking om zo het Cyberkompas voor Ondernemend Nederland te verspreiden. Op deze manier worden het denken over toekomstig cybersecuritybeleid en het verhogen van de cyberweerbaarheid gestimuleerd.

Totstandkoming
Het Cyberkompas voor Ondernemend Nederland komt tot op stand op basis van trendonderzoek binnen diverse branches en ketens, openbare bronnen en de expertise op het gebied van cybersecurity van de Cybersecurity Alliantie. Daarnaast is er bij het opstellen van het Cyberkompas beroep gedaan op kennis die de volgende personen tijdens de expertmeetings hebben ingebracht:

Michelle de Boer (NCTV), Marjolijn Bonthuis (ECP), Janet Cadel (CIO Platform), Margreet Drijvers (Platform Zelfstandige Ondernemers), Elif Duru (Ordina), Liesbeth Holterman (Cyberveilig Nederland), Diederik van Luijk (NCSC), Jeroen Kasbergen (DTC), Marnix Korlaar (NCTV), Liebeth Kruizinga (DTC), Iris Koster (ECP), Nicole Mallens (VNO NCW), Sjaak Schouteren (Marsh), Jelle Niemantsverdriet (Microsoft), Julia Peeters (NCTV), Eleonora Petridou (Booking), Kees Plas (BDO), Serge van der Schaft (NCSC), Jeroen Steenbakkers (Drechtsteden), Stephanie Teeuwen (ECP), Mieke van Ulden (ECP), Martin Vliem (Microsoft), Michael Vos (Microsoft), Esther van der Weide (TNO), Evert van Zanten (PvIB) en Rosa van Zijl Jansen (NCSC)

Uitgave:
Cybersecurity Alliantie (CSA)

Meer informatie:
www.cybersecurityalliantie.nl
csa@ecp.nl

December 2021

Cyberkompas
voor Ondernemend Nederland

cybersecurityalliantie.nl