Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Cyberkompas 2019

Toegestane verspreiding TLP: WHITE
(Traffic Light Protocol)

Het Cyberkompas heeft het label TLP:White en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Ligth Protocol (TLP) om eenduidig te definiëren wat er met informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard van First (www.first.org/tlp). Ontvangers mogen de informatie uit het Cyberkompas delen binnen en buiten hun organisatie, daarnaast mag informatie publiek gemaakt worden.

Uw reacties zijn welkom op info@ncsc.nl.

Cyberkompas

Inleiding

In deze snel veranderende maatschappij is het belangrijk om digitaal weerbaar te blijven. Ontwikkelingen in het digitale domein gaan razendsnel plus de complexiteit neemt toe. Het is daarom cruciaal zicht te hebben op de uitdagingen die op ons af komen.

Om dit weer te kunnen geven hebben we het Cyberkompas ontwikkeld. Hiermee geven we organisaties richting op basis van acht thema's en bijbehorende verwachtingen. Het is een interactief instrument waarmee inzicht, bewustwording en handelingsperspectief gerealiseerd wordt.

Organisaties kunnen zo zelf anticiperen op de digitale uitdagingen die voor hen liggen en de cybersecurity vraagstukken die voor hun organisatie een rol gaan spelen.

Het Cyberkompas onderscheidt acht thema's die toekomstrichting aangeven. Deze thema's zijn onderverdeeld in een aantal concrete verwachtingen. Voor ieder thema zijn een omschrijving en versnellers en vertragers geformuleerd.

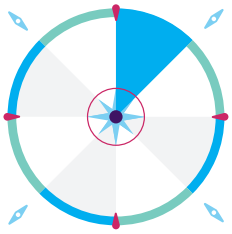
Ook de verwachtingen worden verder omschreven. Per verwachting zijn mogelijke gevolgen, verwachte relevantie en een verwacht doorbraakmoment geïdentificeerd. Tot slot zijn er indicatoren aangewezen die wijzen op een doorbraak.

U vindt een grafische weergave van het Cyberkompas in de achterflap van deze publicatie.

Thema

Digitalisering tot in haarvaten maatschappij

Alledaagse processen zoals wonen, werken, recreëren, reizen, transporteren en communiceren worden steeds meer afhankelijk van digitale technologie. De verwachting is dat dit nog verder zal toenemen. Vaak zijn er geen alternatieven meer voorhanden. Ook kent de toepassing van gedigitaliseerde processen geen landsgrenzen meer.



Voorbeelden

Slimme apparaten en toepassingen met sensoren. Bankieren en reizen met wearables. Off the shelf apps en toepassingen op mobiele telefoons. Het gebruik van internationale clouddiensten.

Versnellers

Druk vanuit potentiele commerciële belangen, schaalvoordelen.

Vertragers

Fragiele infrastructuur, privacyoverwegingen, wetgeving.

Verwachtingen

Afhankelijkheid van Streaming

Streamingdiensten nemen steeds meer de plaats in van opgeslagen data. Dit vergroot de afhankelijkheid van elektriciteit en digitale infrastructuur. Beschikbaarheid en vertrouwelijkheid staan hiermee onder druk. Data van gebruikers wordt gebruikt voor profilering en veel informatie bevindt zich buiten de landsgrenzen.

- Mogelijke gevolgen: persoonlijke data op andermans hardware zorgt voor het risico van verlies van controle over data. Bij een publieke cloud, een standaard dienst die aangeboden wordt voor een breed publiek, is het meestal niet precies duidelijk wie toegang heeft tot jouw data. Zeker wanneer deze data bewaard wordt in landen waar wettelijke verplichtingen bestaan om stilzwijgend toegang te verschaffen aan politie- en opsporingsdiensten.
- Verwachte relevantie: laag.
- Verwachte doorbraak(moment): 2021.
- Indicatoren die wijzen op doorbraak: mediaberichten over profiling door streamingsdiensten.

Eigenaarschap van data wordt gecompliceerd vraagstuk

Door de nieuwe manieren waarop data wordt verwerkt en opgeslagen, is het lastiger om controle te houden over de toegang tot informatie. Gegevens die opgeslagen zijn op bijvoorbeeld clouddiensten staan feitelijk op andermans hardware. Daarnaast wordt data over de hele wereld opgeslagen en heeft de eigenaar van de data daar niet altijd controle over.

- Mogelijke gevolgen: een verlies van vertrouwen in digitale technologie. Toename van het aantal rechtszaken tegen grote technologiebedrijven. Nieuwe wet- en regelgeving.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2020.
- Indicatoren die wijzen op doorbraak: toenemende maatschappelijke onrust over dataverwerking door apps en onderliggende diensten.

Mogelijkheden voor 24 uurs toegang tot kennis en diensten nemen toe.

Door toegenomen digitalisering van informatie wordt kennis breder en gemakkelijker toegankelijk en goedkoper. Informatiebronnen die voorheen alleen fysiek toegankelijk waren (bijvoorbeeld in een archief of bibliotheek) zijn nu voor meer mensen beschikbaar. Daarnaast is er ook toegang tot kennis in de vorm van MOOC's (Massive Open Online Courses) voor een breed publiek.

- Mogelijke gevolgen: nieuwe ontwikkelmogelijkheden voor groepen die van oudsher geen toegang hadden tot informatie. Anderzijds groei van de kloof tussen have's, hen die toegang tot internet en informatie achter paywalls hebben, en have not's, de internetlozen.
- Verwachte relevantie: laag.
- Verwachte doorbraak(moment): 2021.
- Indicatoren die wijzen op doorbraak: groei van het aantal online diensten. Groei van betaalde diensten. Afname van hoogwaardige informatie die gratis toegankelijk is.

Toename gebruik wearables voor medische hulpverlening

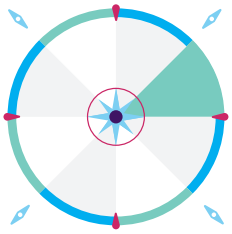
Wearables worden steeds meer gebruikt en bieden meer mogelijkheden voor het in kaart brengen van de gezondheid. Op basis van bepaalde indicatoren wordt het normaal dat hulpdiensten worden ingeschakeld en dat indicatoren gezamenlijk de medische status geven van een gebruiker.

- Mogelijke gevolgen: eigen interpretatie van de medische status zonder tussenkomst van een medisch specialist. Dit kan leiden tot verkeerde diagnoses. Patiënten kunnen op afstand continu gemonitord worden. Zorgverzekeraars kunnen lagere premies gaan bieden in ruil voor informatie uit wearables.
- Verwachte relevantie: laag.
- Verwachte doorbraak(moment): 2022.
- Indicatoren die wijzen op doorbraak: inzet van wearables door zorgverzekeraars en zorgverleners.

Thema

Toename wet- en regelgeving

Wet- en regelgeving die toeziet op cybersecurity aspecten neemt toe. Doordat cybersecurity een steeds grotere plaats inneemt in de maatschappij, wordt de urgentie van bijbehorende problemen steeds groter. Hiermee neemt de behoefte aan kaders, richtlijnen en dus regulering ook toe. Deze wetten kunnen buiten hun werkingsgebied ook een rol spelen als gevolg van marktmechanismen. De meeste multi- of internationale bedrijven zullen ervoor kiezen om toe te werken naar de vereisten van de hoogste standaarden wanneer ze geconfronteerd worden met regelgevingssystemen in meerdere landen.



Voorbeelden

Wetten en regelgeving zoals PSD2, Wbni, EU Cybersecurity-act, Wet CCIII, GDPR.

Versnellers

Internationaal draagvlak en consensus.

Vertragers

Verschillen in inzicht, tegengestelde belangen, lobbykracht.

Verwachtingen

Internationale regulering blijft verder achter bij technologische ontwikkeling

De digitale mogelijkheden nemen snel toe, denk aan Internet of Things toepassingen of toepassingen waarbij feit en fictie steeds moeilijker van elkaar te onderscheiden zijn. Misbruik van deze mogelijkheden moet beperkt worden. De roep om internationale regulering wordt groter. Omdat kwaadwillenden altijd nieuwe mogelijkheden vinden om misbruik te maken van kwetsbaarheden, zal wetgeving steeds verder achterlopen en zal de kloof groeien.

- Mogelijke gevolgen: het blijft aantrekkelijk voor kwaadwillenden om kwetsbaarheden te misbruiken. Dit kan een toename van cybercrime (in brede zin) tot gevolg hebben. Doordat wettelijke kaders ontbreken voelen organisaties onvoldoende noodzaak om hun weerbaarheid verder te verhogen.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2020.
- Indicatoren die wijzen op doorbraak: Europese en zelfs mondiale samenwerkingen komen steeds moeilijker tot stand door tegengestelde belangen waardoor internationale regulering ook moeilijker gerealiseerd wordt.

Positie van Cybersecurity professionals wordt versterkt

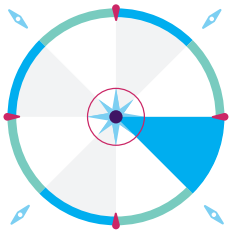
Doordat (nationale) regulering de afgelopen jaren is toegenomen, moeten meer organisaties sturen op het voldoen aan regelgeving. Hiervoor worden, ook in de toekomst, extra professionals ingezet op het gebied van bescherming van gegevens.

- Mogelijke gevolgen: cybersecurityprofessionals worden meer betrokken bij strategische beslissingen omdat erkend wordt dat cybersecurity een rol speelt met betrekking tot de continuïteit van de organisatie.
- Verwachte relevantie: hoog.
- Verwachte doorbraak(moment): 2020.
- Indicatoren die wijzen op doorbraak: Cybersecurity als onderdeel van het organisatiecontinuïteitsvraagstuk staat steeds vaker op de agenda van de hoogste managementlagen en toezichthouders. Dit zorgt voor een grotere vraag naar cybersecurityprofessionals. Handhaving van cybersecurity wordt steeds meer geformaliseerd, bijvoorbeeld in de vorm van wettelijke bevoegdheden van overheidsorganisaties om in te grijpen bij organisaties die onvoldoende compliant zijn.

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 een centrale rol samen met sociale, maatschappelijke, juridische en ethische aspecten.



Voorbeelden

Zelfvarende schepen, zelfrijdende auto's, zelfvliegende drones, zelfrijdende treinen, slimme infrastructuur etc.

Versnellers

Wettelijk kader, betere (veiligheids-)techniek en kostenbesparingen, maatschappelijke acceptatie.

Vertragers

Ongevallen, ontbreken van wettelijk kader, ethische vraagstukken. Het ontbreken van standaarden, communicatie- en protocolverschillen.

Verwachtingen

Volledige afhankelijkheid van elektriciteit voor internet en technologie leidt tot druk op kritieke infrastructuur

Intelligente mobiliteit is voor een steeds groter deel afhankelijk van elektriciteit als vervanging voor fossiele brandstoffen. Zolang er meer data opgeslagen wordt, zal ook het aandeel van datacenters in het energiegebruik steeds verder toenemen. De verwachting is dat ook nieuw te ontwikkelen producten afhankelijk zullen zijn van elektriciteit. Hierdoor neemt de behoefte aan elektriciteit verder toe. Het aanbod zal meer gaan fluctueren door de toenemende hoeveelheid van opgewekte zonne- en windenergie. Hierdoor neemt de belasting op het elektriciteitsnetwerk steeds verder toe en daarmee de kans op tekorten in de distributiecapaciteit en uitval.

- Mogelijke gevolgen: disrupties in kritieke infrastructuur met maatschappelijke impact: het uitvallen van (techniek in) voertuigen, storingen en/of tekorten bij auto-oplaadpalen en verkeersregelsystemen doordat er niet aan de vraag kan worden voldaan. Meer gebruik van alternatieve en duurzame energiedragers zoals waterstof, groengas, accu's en andere vormen van decentrale energieopslag.
- Verwachte relevantie: hoog.
- Verwachte doorbraak(moment): 2021.
- Indicatoren die wijzen op doorbraak: toename in frequentie en duur van verstoringen in elektriciteitsnetwerken.

Meer aandacht voor cybersecurity intelligente mobiliteitssystemen

Het maatschappelijke belang van cybersecurity maatregelen in mobiliteitssystemen wordt steeds duidelijker voor leverancier en consument. Hierdoor ontstaat er onder andere een behoefte aan het signaleren van kwetsbaarheden in de hierbij toegepaste technologie.

- Mogelijke gevolgen: toename aan R&D-beleid, meer wettelijke eisen aan beveiliging bij mobiliteit, toename aan certificering voor informatiebeveiligingssystemen in mobiliteitssystemen, meer mobiliteitssystemen die *security by design* toepassen.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2021.
- Indicatoren die wijzen op doorbraak: grotere vraag naar cybersecurity professionals, hogere bugbounties, aandacht voor het hacken van auto's.

Standaardisatie biedt kansen voor betere bescherming van kritieke infrastructuur

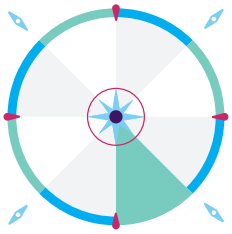
Doordat autonome voertuigen gemeengoed worden treedt er standaardisatie op in de gebruikte technieken. Dit biedt mogelijkheden om technieken toe te passen die rekening houden met de kwetsbaarheid van de infrastructuur.

- Mogelijke gevolgen: veiligere (autonome) voertuigen.
- Verwachte relevantie: laag.
- Verwachte doorbraak(moment): later.
- Indicatoren die wijzen op doorbraak: meer wet -en regelgeving, het toepassen van standaardtechnieken in de mobiliteitsindustrie.

Thema

Homogenisering van digitale landschap

Er wordt op grote schaal gebruik gemaakt van steeds meer dezelfde (technische) oplossingen.



Voorbeelden

Bepaalde soorten chips en referentiearchitecturen worden veel gebruikt in diverse toepassingen waardoor de impact groot kan zijn bij een kwetsbaarheid in een dergelijke bouwsteen.

Versnellers

Off the shelf is goedkoper dan nieuw te ontwikkelen technieken of oplossingen.

Vertragers

Door incidenten komt er meer vraag naar alternatieve oplossingen. Geopolitieke spanningen kunnen zorgen voor heterogeniteit.

Verwachtingen

Behoefte aan het verminderen van wederzijdse afhankelijkheid (van machtsblokken) zorgt voor meer verschillende technieken

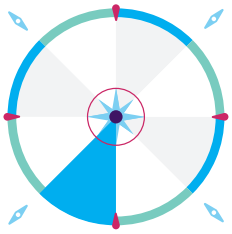
Om de afhankelijkheid van machtsblokken, zoals bijvoorbeeld veel gebruikte software van grote marktpartijen te verminderen, wordt bewust een afweging gemaakt om andere soorten technieken in te zetten.

- Mogelijke gevolgen: hogere kosten.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2021.
- Indicatoren die wijzen op doorbraak: voorschriften die wederzijdse afhankelijkheid en daarmee homogeniteit trachten te verminderen.

Thema

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.



Voorbeelden

We zijn vrijwel allemaal gebruiker van de diensten van de big five.

Versnellers

Lobby krachten en technology push waarbij technische mogelijkheden aanbod gedreven 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, opsplitsing. Geopolitieke ontwikkelingen.

Verwachtingen

Schaalvoordelen zorgen voor uniforme beveiligingsmechanismen

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

- Mogelijke gevolgen: door beveiligingsmechanismes af te dwingen, kan worden voorkomen dat simpele technieken effectief zijn voor het hacken van systemen.
- Verwachte relevantie: hoog.
- Verwachte doorbraak(moment): 2020.
- 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.
- Indicatoren die wijzen op doorbraak: effect op een aantal gebruikers na schandalen, waarbij de privacy van gebruikers geschaad werd.

Afhankelijkheid van een beperkt aantal partijen zet weerbaarheid onder druk

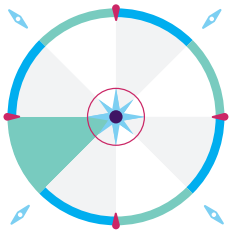
Door de centrale positie van een klein aantal partijen ondervindt een hele sector of zelfs de gehele vitale infrastructuur negatieve gevolgen wanneer die leverancier wordt getroffen door een cybersecurity-incident.

- Mogelijke gevolgen: meer regulering en wetgeving om de weerbaarheid van deze partijen te verhogen zodat een incident minder effect heeft. Maatregelen om de afhankelijkheid te verkleinen en alternatieven voorhanden te hebben.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2021.
- Indicatoren die wijzen op doorbraak: incidenten uit het verleden zoals het brandstofprobleem op Schiphol in 2019.

Thema

Toename complexiteit incident respons

Met de concentratie op kernactiviteiten en de verplaatsing van eigen servers naar software in de cloud, nemen het aantal betrokken organisaties en de gebruikte technieken in een keten toe. Daarmee stijgt de noodzaak tot afstemming van informatie en verantwoordelijkheden, evenals de toegang tot alle relevante informatie in het geval van incidenten.



Voorbeelden
Er wordt steeds meer encryptie toegepast in het dataverkeer.

Versnellers
Toename van encryptie, opkomst van desinformatie en nepnieuws, tekort aan goed opgeleid personeel.

Vertragers
Standaardisatie van security-oplossingen, betere afspraken in het stakeholder-landschap.

Verwachtingen

Root Cause Analyse en detectie wordt lastiger

Root cause analyse en detectie wordt lastiger omdat niet alle informatie uit de keten real-time beschikbaar is.

- Mogelijke gevolgen: meer kans op ontwrichtende incidenten omdat deze niet tijdig en juist gedetecteerd kunnen worden. Incidenten houden langer aan. Meer samenwerking tussen ketenpartijen. Respons zal meer maatwerk zal zijn.
- Verwachte relevantie: laag.
- Verwachte doorbraak(moment): 2020.
- Indicatoren die wijzen op doorbraak: herhaling van incidenten uit het verleden zoals (Not)Petya waarbij een lek in een buitenlands boekhoudprogramma zich razendsnel verspreidde en het primaire proces in de Rotterdamse haven deels stillegde.

Detectie wordt lastiger, er komen meer 'black boxes' in de keten

De keten is opgebouwd uit black boxes waarvan niet transparant is hoe ze werken en welke invloed ze hebben in de rest van de keten. Hierdoor wordt detectie complex omdat niet alle informatie beschikbaar is.

- Mogelijke gevolgen: meer kans op ontwrichtende incidenten omdat deze niet tijdig en juist gedetecteerd kunnen worden. Incidenten houden langer aan.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2021.
- Indicatoren die wijzen op doorbraak: grootschalige adoptie van technieken zoals DNS over HTTPS waarbij het proces van het opzoeken van de domeinnaam die bij een ip-adres hoort, versleuteld wordt

Door toename van gegevensbescherming wordt het lastiger om malafide activiteiten tegen te gaan

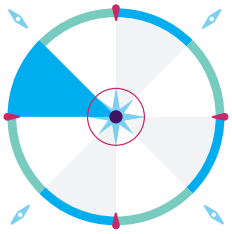
Organisaties zijn zich meer bewust van het belang van gegevensbescherming en zorgen voor maatregelen om deze gegevens beter af te schermen. Dit kan resulteren in aanvallen waarbij beveiligingstechnieken gericht op gegevensbescherming in het voordeel van de aanvaller worden ingezet. Deze aanvallen zijn moeilijker te traceren.

- Mogelijke gevolgen: securityproducten vergroten de onveiligheid.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment):: 2021.
- Indicatoren die wijzen op doorbraak: adoptie door kwaadwillenden van technieken zoals DNS en VPN over HTTPS waarbij de inzet van versleuteling het lastiger maakt de aanvaller te detecteren.

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 overgelaten aan kunstmatige intelligentie. Dit gebeurt met software op basis van algoritmes. De algoritmes zijn door de mens bedacht, hiermee worden de beslissingen zelfstandig gemaakt. 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

Bureaucratische processen zoals belastingen, subsidies, verzekeringen, betaalverkeer en logistieke processen.

Versnellers

Arbeidskosten, krapte op de arbeidsmarkt, menselijke tekortkomingen, concurrentie, marktvraag, technologische ontwikkelingen en betrouwbaarheidseisen.

Vertragers

Wetgeving, initiële investeringen, grote incidenten veroorzaakt door algoritmes, angst voor en wantrouwen jegens algoritmes en robots, ethische vraagstukken.

Verwachtingen

Reductie van het aantal beveiligingsincidenten veroorzaakt door menselijke fouten.

Processen die worden aangestuurd op basis van algoritmes zijn minder vatbaar voor fouten. Vanzelfsprekend hangt dit wel af van de gebruikte techniek en eventueel de kwaliteit van het gebruikte algoritme. Immers, op basis van gegevens maakt een computer deze beslissing, niet op basis van gevoel. Hiermee zou de beslissing die wordt gemaakt en de actie die hierop volgt altijd te voorspellen zijn. Die is dus minder foutgevoelig.

- Mogelijke gevolgen: er worden door de mens minder fouten gemaakt. Doordat software of machines die zelfstandig (en mogelijk zelflerend) beslissingen nemen, belangrijker zijn bij beslissingen dan de mens, zal een kwaadwillende zich meer gaan richten op het beïnvloeden van de gebruikte algoritmes of de hardware die betrokken is bij deze beslissingen. Deze ontwikkeling maakt schaalvergroting (relatief) eenvoudig mogelijk waardoor de impact toeneemt.
- Verwachte relevantie: hoog.
- Verwachte doorbraak(moment): 2021.
- Indicatoren die wijzen op doorbraak: meer incidenten als gevolg van algoritmes die niet juist zijn of die door kwaadwillenden bewust gemanipuleerd worden.

Menselijk improvisatievermogen om besluiten van computers te betwisten vermindert.

Doordat 'gesloten' algoritmes steeds meer worden gebruikt om beslissingen te nemen, wordt de totstandkoming van besluiten steeds meer een 'black box'. In deze black box zullen ook vooroordelen verwerkt zijn, omdat de algoritmes door de mens zijn bedacht. Onze democratie vereist dat er inzicht moet zijn in de wijze waarop de black box werkt. Door dit gebrek aan inzicht wordt de beoordeling door de mens van de juistheid van de beslissing moeilijker.

- Mogelijke gevolgen: er is meer behoefte aan transparantie over de gebruikte algoritmes; regelgeving of richtlijnen worden belangrijker. Vertrouwen in AI neemt af doordat het gevoel van controle verloren gaat.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2020.
- Indicatoren die wijzen op doorbraak: ontwikkelingen waarover in de media gediscussieerd wordt zoals een transparantielab, bedoeld om transparantie te verhogen. Wetten die gericht zijn op het waarborgen van gedetailleerd inzicht in de totstandkoming van besluiten.

Negatieve gevolgen van het gebrek aan menselijke oordelen wordt zichtbaar.

Doordat kunstmatige intelligentie (AI) gebaseerd is op het nemen van beslissingen op basis van gegevens in een bepaalde context, kan er niet meer bijgestuurd worden op basis van aanvullende gegevens die ook van belang blijken te zijn of menselijke inzichten. AI is makkelijker om de tuin te leiden met valse invoer dan de mensen die vervangen worden. Hierdoor kunnen beslissingen anders uitpakken.

- Mogelijke gevolgen: verkeerde beslissingen indien bezien vanuit een breder belang of vanuit ethisch oogpunt. Beslissingen worden vaker ter discussie gesteld.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2022 en verder.
- Indicatoren die wijzen op doorbraak: toename in het onderzoek naar de ethische bezwaren van AI.

Beïnvloeding van stuurgegevens en stamdata leidt tot AI wantrouwen

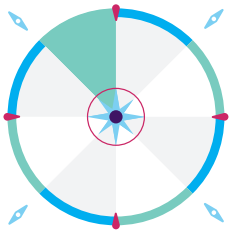
Er kunnen organisatie- of externe belangen zijn die beïnvloeding van stamdata waarschijnlijk maken. Hierdoor kunnen stuurgegevens en stamdata (on-)bewust vervuild worden om uiteindelijk uitkomsten te manipuleren.

- Mogelijke gevolgen: Het wantrouwen kan leiden tot weerstand tegen AI. Dat kan uiteindelijk tot gevolg hebben dat AI minder ingezet wordt bij processen waar discussie over de uitkomst vaker voorkomt (denk aan verzekeringen). Er komen steeds meer kunstmatig intelligente systemen die nep-content maken. Computational propaganda, deepfakes waarbij kunstmatige intelligentie ingezet wordt om nepvideo's te maken die echt lijken.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2021.
- Indicatoren die wijzen op doorbraak: schandalen zoals Cambridge Analytica: illegale manipulatie van de gegevens van miljoenen Facebook-gebruikers.

Thema

Afname vrijheid leverancierskeuze

Vanuit security-overwegingen zorgen verschillende factoren ervoor dat er een keuze is uit een beperkt aantal leveranciers.



Voorbeelden

In de telecomsector komt de vrijheid van leverancierskeuze steeds verder onder druk te staan.

Versnellers

Geopolitieke spanningen en security-eisen werken belemmerend voor nieuwe toetreders. Protectionisme, strengere wettelijke kaders. Industriepolitiek.

Vertragers

Security wordt als verkoopargument ingezet. Basisnormen voor securityvereisten zorgen voor een level playing field. Lobbymacht van bedrijven.

Verwachtingen

Door de nadruk op privacy- en andere wetgeving worden leveranciers kritischer getoetst op compliance (met deze kaders)

Europese wetgeving zet een hoge standaard neer op het gebied van privacy en dataprotectie. Daarnaast is er vanuit security oogpunt een groeiende onrust over het selecteren van leveranciers die zich hebben gevestigd in landen waarvan de nationale wetgeving bedrijven kan forceren om mee te werken aan offensieve cyberprogramma's, bijvoorbeeld cyberspionage en voorbereidingshandelingen voor sabotage.

- Mogelijke gevolgen: boetes door toezichthouders in verband met het niet voldoen aan wetgeving. Opkomst van nieuwe (kleinere) bedrijven die wel aan wetgeving kunnen voldoen. Uitsluiting van actoren.
- Verwachte relevantie: gemiddeld.
- Verwachte doorbraak(moment): 2020.
- Indicatoren die wijzen op doorbraak: meer wetten en regels die leveranciers uitsluiten dan wel voorschrijven.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Cyberkompas 2019

Om digitaal weerbaar te blijven is het noodzakelijk zicht te hebben op de uitdagingen die op ons af komen. Met de acht thema's en verwachtingen van het cyberkompas kunnen organisaties zelf anticiperen op de cybersecurity-vraagstukken die voor hun organisatie een rol kunnen gaan spelen.

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Totstandkoming

Dit product komt tot stand op basis van algemene trendverkenningen, openbaar toegankelijke bronnen en de tactische en operationele expertise van het NCSC.
Bij het opstellen heeft het NCSC dankbaar gebruik gemaakt van kennis die experts van de volgende partijen tijdens een expertmeeting hebben ingebracht:

Centric, Clingendael, Defensie Cyber Expertise Centrum, DNB, Fox-IT, The Hague Centre for Strategic Studies, Ministerie van EZK, NCTV, NFI, Privacycompany, Nationale Politie, Rathenau Instituut, SIDN, Surfnet, TNO, TU Delft

De inbreng van deze partijen, verenigd in het Analistennetwerk Nationale Veiligheid (ANV), heeft bijgedragen aan de inhoudelijke kwaliteit van het Cyberkompas 2019.

Uitgave
Nationaal Cyber
Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

november 2019