Voor het BGP Cybersecurity zijn 7 thema's geïdentificeerd

Security by design
Het verhogen van de cyberweerbaarheid door security by design (of 'by default') is een stip op de horizon die door alle Topsectoren benoemd is. Een selectieve maatregel kan voldoende bescherming bieden voor een select proces, maar houdt geen rekening met of biedt onvoldoende bescherming met de andere (operationele) processen. Cybersecurity dreigingen richten zich op de hele organisatie en netwerken. Daarom uiten de Topsectoren de behoefte aan normen en een referentiearchitectuur voor te ontwikkelen hardware en software. Een afsprakenstelsel voor minimale eisen van hard- en software en de werking ervan (denk aan identificatie, authenticatie en autorisatie van datastromen). Door een security by design aanpak willen de Topsectoren ervoor zorgen dat processen en apparaten veiliger worden én dat de uitval ervan minder schade teweegbrengt in de organisatie.[1] Ook de governance binnen en tussen organisaties hoort bij dit vraagstuk: hoe worden de normen of afspraken toegepast en geborgd gedurende de levenscyclus van systemen en hun bijbehorende fysieke platforms?! Technologie en toepassing.

Veilig datagedreven werken
Dit is een vaak genoemd thema. De maatschappelijke transities van de Topsectoren worden namelijk in hoge mate ondersteund door het gebruik van data science en AI. Data staat centraal. Daarom zijn er kennis- en innovatievragen over het gebruik en totstandkoming ervan en is men benieuwd naar de mogelijke risico's. Topsectoren zijn op zoek naar manieren om geautomatiseerd data te delen en analyseren en deze data op te werken naar bedrijfs- en sectorspecifieke voorspellingen. Men is onvoldoende op de hoogte en geëquipeerd om veilig data uit te wisselen tussen bedrijven en tussen bedrijven en publieke instellingen. Daarnaast is onvoldoende bekend hoe de betrouwbaarheid en veiligheid van datastromen die input leveren aan cruciale modellen en systemen gegarandeerd kunnen worden (authenticiteit en betrouwbaarheid van de bron, integriteit en vertrouwelijkheid van data gedurende opslag, transport en verwerking). Samenwerking, digitalisering en lange bewaartermijnen stellen speciale eisen aan cybersecurity, aan digitaal data delen en aan borging van intellectueel eigendom en kroonjuwelen. Er moeten toekomstbestendige afspraken (technische) gemaakt worden over wie wel of niet bij welke data en modellen mogen komen, digitaal gezekerd is, zonder dat dit een efficiënte samenwerking in de weg staat.

Het is een onderwerp dat speelt in vrijwel alle Topsectoren, bijvoorbeeld bij het veilig aansturen en monitoren van industriële controlesystemen op afstand, maar ook bij het vertrouwen van sensordata van open (GPS- en weerdata) en gesloten (bedrijfsinterne) bronnen. De authenticiteit van (digitale)media is b.v. ook een punt van zorg. Welke bronnen zijn nog te vertrouwen en zijn daar technologische waarborgen voor te ontwikkelen? Ook spelen juridische ethische vraagstukken een rol in de maatschappelijke uitdagingen van de Topsectoren. Men vraagt zich af of de huidige manier van dataeigenaarschap en dataverzameling nog wel mag en moet. Welke Privacy Enhancing Technologies (PET) moeten (door)ontwikkeld worden om klaar te zijn voor de toekomst? Vernieuwende toepassingen worden op dit moment ondersteund door technieken zoals Federated Learning en multi-party computation. Cryptografie (quantum-safe) als hulpmiddel voor authenticatie, integriteit en vertrouwelijkheid is eveneens een ondersteunende technologie. Idem automatisch kunnen labelen van (gevoelige) data. Is

[1] Inspiratie o.a. bij NCSC UK cyberstrategie voor 2030, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049345/cyber-security-strategy-2022.pdf

Nederland in staat om een afsprakenstelsel te ontwikkelen of beïnvloeden dat als blauwdruk kan dienen voor meerdere sectoren? Hoe werkt een dergelijke technologie in samenwerking met bestaande diverse groepen van actoren en andere afsprakenstelsels? Een voorbeeld hiervan is een blauwdruk die de transportsector kan gebruiken voor zowel leveranciers, als met de bloemenveilig Flora Holland, en de digitale systemen van de douane in binnen- en buitenland. Technologie en toepassing.

Veilige en robuuste connectiviteit
Een toekomstbestendig innoverend Nederland is afhankelijk van een veilige digitale infrastructuur. Datagedreven werken valt of staat met connectiviteit. Dat wil zeggen; vertrouwen in de draadloze en bekabelde verbindingen, én in de protocollen en standaarden die de functionaliteit, beschikbaarheid en veiligheid van verbindingen waarborgen. De vraag naar (veilige) connectiviteit blijft groeien, mede door de aanstaande breed uit te rollen technieken zoals 5G en 6G. Topsectoren zijn benieuwd naar de beveiliging van de fysieke infrastructuur maar ook naar het afsprakenstelsel dat daar een cruciale rol in speelt. Welke rol gaat het kwantuminternet spelen, hoe blijven netwerken van de toekomst synchroon (synchronisatie van atoomklokken)?Gezamenlijk optrekken voorkomt dat elke sector een eigen wiel gaat uitvinden, waardoor connectiviteit tussen systemen en data uit verschillende sectoren geborgd wordt op de lange termijn. Cross-sectorale samenwerkingen zijn vereist voor de volgende stadia van de ontwikkelingen; mobiliteit van de toekomst vereist bijvoorbeeld dat stedenbouwkundigen en de telecomindustrie met elkaar ontwikkelen. Connectiviteit maakt gegevensoverdracht, gegevensopslag en gegevensuitwisseling mogelijk als onderdeel van de voortgaande digitalisering.

Veilige OT en IoT en integratie met IT
De verwevenheid van IT en OT neemt in toenemende mate toe bij kritische (productie)processen. Apparaten en systemen praten met elkaar, lezen sensoren uit en worden door externen onderhouden en gemonitord. Topsectoren hebben onvoldoende grip op de risico's en dreigingen die deze integratie oplevert. Daarnaast is er onvoldoende begrip van beschikbare en inzicht in te ontwikkelen beheersmaatregelen. De verwevenheid van IT en OT is organisaties veelal ingeslopen vanuit het oogpunt van efficiëntie en functionaliteit. Topsectoren hebben behoefte aan kennis over deze integratie. Bij de uitwerking van use cases is dit o.a. verder verdiept naar het goed in kaart kunnen brengen van de risico's in complexe IT/OT omgevingen, modeleren en simuleren van dit soort omgevingen. Er liggen ook raakvlakken met de thema's cyberrisicomanagement en systeem en ketenveiligheid

Cyberrisicomanagement
Meerdere Topsectoren hebben aangegeven grote behoefte te zien voor innovatie op effectief en adequaat cyberrisicomanagement. Om te weten welke risico's van toepassing zijn is er meer kennis en toepassing nodig van (IT) asset management. Tevens zijn data en modellen nodig over de impact van cybersecurity dreigingen, de beschikbare maatregelen en de afhankelijkheid van ketens (b.v. de supply chain).[2]Het gaat hierbij om intern risicomanagement. Voor de nabije toekomst zou innovatie een rol kunnen spelen om real-time data te gebruiken voor risicomanagement (in tegenstelling tot statische gegevens). Een grote uitdaging is dat risico indicatoren en maatregelen niet kwantificeerbaar zijn, waardoor het profijt van investeringen ondermaats ingeschat wordt. De onderschatting leidt tot onvoldoende beschermingsmaatregelen. Onderdeel van cyberrisicomanagement is het inrichten van en oefenen met crisisorganisatie. Met

[2] Voorbeeld van een model is breder toegankelijkere versie van de Algemene Beveiligingseisen Defensieopdrachten 2019 (ABDO).

name in geval van keten- of systeemaanvallen is snelle en effectieve coördinatie over individuele organisaties essentieel om aanvallen af te wenden of (economische en/of maatschappelijke) schade te beperken.

Systeem- en ketenveiligheid
Topsectoren hebben ook de behoefte geuit voor bedrijfsoverstijgend mitigeren van risico's. Digitale weerbaarheid van ketens of van een systeem van componenten (of organisaties) is door de soms eenvoudige verspreiding van cyberdreigingen noodzakelijk. Kunnen cascade-effecten of grote geaccumuleerde schade worden voorkomen!? Het gaat dan bijvoorbeeld om het hacken van leveranciers van een bedrijf dat hoogtechnologische beveiligingsapparatuur ontwikkelt en dan daar tot digitale spionage of sabotage leidt. Of om het tegelijkertijd verstoren van meerdere sluizen in de grote waterwegen van Nederland.

Systeem- of ketenveiligheid omvat supply chain security als specifieke verschijningsvorm. Dat organisaties onderdeel zijn van lange en complexe, tijdkritieke supply chains is voor velen een gegeven. Er is aanvullende kennis nodig om de cyberrisico's in complexe supply chains inzichtelijker te maken en te mitigeren. De effecten van incidenten of verstoring in de keten zorgen voor effecten waar bedrijven niet op voorbereid zijn. Een ander soort risico betreft hier niet de bedrijfsvoering, maar digitale componenten die verderop in de keten worden geassembleerd in een groter product. Een specifieke categorie hierbinnen is software. Grote applicaties bevatten vele componenten en componenten van componenten, die bij elke update weer veranderen in samenstelling.[3] Op basis van een modern cyberrisicomanagement moeten de juiste beheersmaatregelen gekozen en geïmplementeerd worden. De behoefte hieraan is op dit moment al groot en de verwachting is dat dit de komende jaren enkel in belang toeneemt.

Cybersecurity awareness, kennis en vaardigheden
Misschien wel het belangrijkste gemeenschappelijke knelpunt en zeker randvoorwaarde voor succes van cybersecurity is het kunnen beschikken over voldoende kennis en vaardigheden en tijdig en voldoende prioriteren van het onderwerp. Bedrijven hebben het onderwerp cybersecurity echter niet of onvoldoende op de agenda staan,[4] omdat b.v. bestuurders onvoldoende op de hoogte van de dreigingen en/of het onderwerp onvoldoende (concreet) agenderen. Bedrijven hebben daarnaast beperkt zicht op de wet- en regelgeving. Een van de gevolgen daarvan is dat lagere managementniveaus geen capaciteit hebben om de organisatie te beschermen of te voldoen aan wet- en regelgeving (compliance). Bestuurders moeten in staat gesteld worden om de risico's te besturen en de verantwoording te nemen.

Daarnaast is het personeelsvraagstuk breed onderkend. Ook al krijgt het onderwerp voldoende prioriteit, het tekort aan gekwalificeerd cyberpersoneel en voldoende kennis bij niet-cyberpersoneel is alsnog een belemmering. Bedrijven en overheden kunnen de cybersecurity-vacatures niet vullen door een gebrek aan geschoold personeel en de hoge doorloopsnelheid van werknemers. Capaciteit wordt extern ingehuurd over langere perioden met als gevolg een zwakke eigen kennispositie en beperkte interne cultuur van

[3] Log4J is hier een goed voorbeeld van. Deze Java component zit in talloze applicaties overal ter wereld, zonder dat beheerders zich daar altijd bewust van zijn.
[4] Zie b.v. eindrapportage Cybervolwassenheidsonderzoek (2021), DCMR Milieudienst Rijnmond, online: https://www.dcmr.nl/sites/default/files/2021-10/Eindrapportage%20Cybervolwassenheidsonderzoek%20DCMR%20v1.1.pdf

cybersecurity-personeel. Er zijn wel meerdere initiatieven gestart.[5] Zo is de Human Capital Agenda ICT samen met haar partners bezig met de uitvoering van een plan om meer ICT-professionals op te leiden doormiddel van omscholing.

Medewerkers zijn onvoldoende op de hoogte van wat veilig (digitaal) gedrag is, of weten dat wel maar voeren dat gedrag niet uit. In samenwerking met bestuurders moet getoond worden wat de kosten en impact van verstoringen zijn. Daarnaast moet het 'digitale veiligheidsdenken' aangeleerd worden en veilig gedrag moet de norm worden; het is een randvoorwaarde voor toekomstbestendige innoverende en digitaliserende organisaties. Hier kan een rol voor HCA liggen in de vorm van bewustwording en vaardigheden bij brengen bij het personeel. Ook de creatieve industrie kan bijdragen aan innovatieve vormen van kennisoverdracht, bewustwording en de vertaling naar handelingsperspectief.

[5] Andere initiatieven komen o.a. van EZK, Security Delta (HSD) en Centrum voor Veiligheid en Digitalisering.