Terugblik op bestuurlijk mini-symposium – 27 mei 2024
Cybersecurity dreigingen in relatie tot statelijke actoren

Op maandagavond 27 mei 2024 vond het bestuurlijk mini-symposium over cybersecurity dreigingen en statelijke actoren plaats bij het Centrum voor Veiligheid en Digitalisering (CVD) in Apeldoorn. Het symposium werd begeleid door dagvoorzitter Lodewijk Asscher, aanjager van het CVD.

Digitalisering levert naast economische kansen ook dreigingen op. Digitalisering zorgt immers voor een sterkere afhankelijkheid van digitale processen en netwerken. Overheden en (vitale) bedrijven lopen hierdoor een groter risico om slachtoffer te worden van een digitale dreiging. Een cyberaanval kan de continuïteit van een (digitaal en/of fysiek) proces verstoren met de mogelijke gevolgen van dien voor de getroffen organisatie(s) en de maatschappij. Daarnaast kan er door middel van cyberspionage waardevolle informatie over bijvoorbeeld innovatieve technologie worden buitgemaakt. Dreigingen kunnen een geopolitieke achtergrond hebben (bijvoorbeeld ongewenste beïnvloeding door statelijke actoren).

Opening door Ton Heerts

Het symposium werd geopend door Ton Heerts, burgemeester van Apeldoorn. Apeldoorn is de stad van veiligheid. Hier werken dagelijks vele duizenden veiligheidsprofessionals aan de bescherming van onze

maatschappij. Het CVD zet zich vanuit Apeldoorn samen met kennisinstellingen, bedrijven en overheden in om innovatieve technologische oplossingen te ontwikkelen voor complexe maatschappelijke digitale veiligheidsvraagstukken. Zo werkt het CVD nauw samen met de Universiteit Twente, Hogeschool Saxion, de Politieacademie, het Nederlands Instituut Publieke Veiligheid en ROC Aventus.

Het CVD verricht onderzoek naar digitalisering en veiligheid, verzorgt onderwijs voor onder andere young professionals, faciliteert ondernemerschap met het innovation & startup lab en deelt de opgedane kennis en ervaring uit onderzoek door middel van publieksactiviteiten waaronder bijeenkomsten.

Keynote door Bas Dunnebier

Bas Dunnebier, hoofd van de Eenheid Weerbaarheid bij de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) ging tijdens zijn presentatie in op de aard, omvang, verschijningsvormen en modus operandi van statelijke actoren. Statelijke actoren kunnen heimelijk toegang verkrijgen tot digitale systemen van overheden en (vitale) bedrijven. Hierbij kan het doel digitale spionage, beïnvloeding en/of sabotage zijn om strategische doelen te behalen. De AIVD richt zich op het informeren van overheden en (vitale) bedrijven over actuele dreigingen en het geven van handelingsperspectief om de cyberweerbaarheid te bevorderen.

Bas Dunnebier stelt dat de cybersecurity dreiging vanuit statelijke actoren de afgelopen jaren is toegenomen. Verschillende statelijke actoren proberen zich in te nestelen in de vitale sectoren. Een aantal jaar geleden heeft de AIVD de beslissing genomen om meer naar buiten te treden om te kunnen waarschuwen voor de (toegenomen) dreiging en mogelijke cybersecurity incidenten waarmee (semi) overheden en bedrijven te maken (kunnen) krijgen. Technologie van bedrijven uit landen met offensieve gedragingen wordt voortaan geweerd uit vitale processen (zoals scanners in de haven van Rotterdam).

Nieuwe technologieën zoals kunstmatige intelligentie, quantum en cloud zijn van belang voor cybersecurity, nu en in toekomst. De verwachting is dat er in 2030 een staat is die met een quantum computer crypto kan breken. Momenteel zijn we als Nederland nog (te) afhankelijk van andere staten uit andere continenten wat betreft technologie. Bas Dunnebier benadrukt dat (semi)overheden en bedrijven zich hiervan bewust moeten zijn en een gedegen risicoafweging moeten maken. Het is zeer voorspelbaar dat nieuwe technologieën door statelijke actoren misbruikt (gaan) worden. Om hier adequaat op te (kunnen) anticiperen zal Nederland op een slimme manier (nieuwe) technologie moeten omarmen. Daarnaast is publiek-private samenwerking vereist op het terrein van economische veiligheid, kennis veiligheid en vitale sectoren.

Paneldiscussie

In navolging op de keynote vond een paneldiscussie plaats, gemodereerd door Lodewijk Asscher. Hieraan namen Koen Aartsma onderzoeker bij het Clingendael Institute, Evelien Bras directeur van FERM, Jeroen Joon burgemeester van Harderwijk en lid van de VNG-commissie Bestuur en Veiligheid, Ester Weststeijn burgemeester van Rozendaal en lid van de VNG-commissie Informatiesamenleving en Christian Prickaerts directeur van Fox-IT Crypto deel.

Veel wet- en regelgeving op het terrein van cybersecurity is in de basis goed. Er moet echter wel voor worden gewaakt dat (semi)overheden en bedrijven niet (te) veel bezig zijn met compliance in plaats van hun cybersecurity daadwerkelijk te bevorderen. De NIS2-richtlijn voorziet in wettelijke maatregelen om het algemene niveau van cyberbeveiliging in de EU te verhogen. Als essentiële entiteit in het kader van de NIS2-richtlijn krijgen gemeenten een zorgplicht, toezicht

en meldplicht. Ester Weststeijn stelt dat gemeenten (nog) onvoldoende zijn toegerust op het terrein van cybersecurity. Gemeenten zijn goed op weg, maar zijn nog niet waar ze willen zijn. Een gemeente kan zelf slachtoffer worden en tegelijkertijd de partij zijn om de situatie op te lossen, bijvoorbeeld als het gaat om de gemeentelijke dienstverlening richting burgers.

Ook de informatiepositie van een gemeente is volgens haar (nog) niet toereikend om adequaat te anticiperen op (dreigende) cybersecurity incidenten. Wanneer zich in Nederland het risico op een nationale crisis voordoet als gevolg van een cybersecurity dreiging, is het een meerwaarde als de AIVD sneller en vaker informatie kan delen met belanghebbenden (waaronder gemeenten of de informatiebeveiligingsdienst).

Jeroen Joon benadrukt dat wanneer er één bedrijf gehackt wordt dit doorgaans beperkt blijft tot economische schade. Wanneer er echter een of meerdere (semi)publieke instellingen met vitale processen worden getroffen door een cyberaanval kan de maatschappelijke impact aanzienlijk groter zijn.

De verspreiding van desinformatie op social media kan leiden tot spanningen in de samenleving en een verstoring van de openbare orde en veiligheid teweeg brengen. Koen Aartsma stelt dat statelijke inmenging van invloed is op de democratie en samenleving. De

manier van leven in Nederland is fundamenteel anders dan in verschillende andere landen. Diverse statelijke actoren hebben steeds meer capaciteit en nieuwe technologieën tot hun beschikking om invloed uit te oefenen.

Gemeenten beschikken over een bestuurlijk instrumentarium dat kan worden ingezet bij crises. Jeroen Joon stelt dat het niet vanzelfsprekend is dat het bestuurlijk instrumentarium dat is toegespitst op het fysieke stelsel ook toereikend is voor het digitale stelsel. Bijvoorbeeld bij online aangejaagde ordeverstoringen die kunnen leiden tot maatschappelijke onrust.

De nationale overheid organiseert cybersecurity en preventie daarop sectoraal. Maar de effecten van cybersecurity dreigingen zijn ook geografisch. In deze kanteling spelen regionale samenwerkingen een cruciale rol en deze zijn niet geïnstitutionaliseerd en/of worden niet structureel ondersteund vanuit publieke organisaties, aldus Evelien Bras. Zij benadrukt dat regionale samenwerking op het terrein van cyberweerbaarheid ook nodig is. Een voorbeeld hiervan vormt FERM dat zich inzet voor de cyberweerbaarheid van de Haven van Rotterdam.

Christian Prickaerts maakt zich zorgen over de hoeveelheid organisaties die de basis (nog) niet op orde lijken te hebben wanneer het op cybersecurity aankomt. Ondanks de normenkaders, kennis en oplossingen die al voor handen zijn. Hij werpt de stelling op om onderscheid te maken tussen organisaties die daadwerkelijk investeren in cybersecurity en organisaties die dit (nog) niet (voldoende) doen.

De resultaten van deze dialoog bevestigen dat het Centrum voor Veiligheid en Digitalisering zijn focus moet leggen bij vitale processen en infrastructuur in combinatie met cybersecurity, aldus Ben Kokkeler, directeur-bestuurder van het CVD. Een andere conclusie is dat de schaal van het vraagstuk samenwerking in publiek-private consortia vergt, waarbij bedrijven op het terrein van cybersecurity kennispartner zijn. Daarnaast moet cybersecurity voldoende aan bod komen in relevante beroepsopleidingen, waaronder de HBO opleiding Integrale Veiligheidskunde.

Apeldoorn, juni 2024

Frank van Summeren
Centrum voor Veiligheid en Digitalisering