Samenvattend verslag Adviesraad IBD 28 Juni 2023

Nieuwe leden

In de Adviesraad IBD hebben de volgende nieuwe leden zitting genomen:

Esther Weststeijn
Burgermeester van de gemeente Rozendaal. Lid van de VNG-commissie Informatiesamenleving en Voorzitter van het Strategisch Overleg ENSIA. Daarnaast lid van het Dagelijks Bestuur van de K80 (de netwerkorganisatie van kleinere gemeenten in Nederland).

Jurian Hennip
Gemeentesecretaris van de gemeente Krimpenerwaard.

Dennis Kerssens
CIO bij de gemeente Utrecht. Tevens vertegenwoordiger van de CIO's van de G4.

Femke Graatsma
Strategisch relatiemanager bij het Nationaal Cyber Security Centrum (NCSC).

NIS2-richtlijn

TOELICHTING
NIS2 is de Europese verordening die op 17 oktober 2024 in werking zal treden. De voorganger (NIS1) is in Nederland verwerkt in de Wet beveiliging netwerk en informatiesystemen (Wbni). Deze wet wordt op dit moment door de NCTV herzien op grond van deze nieuwe Europese verordening. Deze wet heeft gevolgen voor de zorgplicht, meldplicht, toezicht en eventuele sancties. Ten aanzien van de zorgplicht regelt de nieuwe wet welke organisaties essentieel en belangrijk zijn. Zo worden bijvoorbeeld grote organisaties die processen uitvoeren op het gebied van verkeer, water en de sector zorg als essentieel aangemerkt. De praktische uitwerking hiervan in nadere regelgeving wordt op dit moment beoordeeld door de verschillende vakdepartementen. Daarnaast krijgt de minister van BZK de bevoegdheid om medeoverheden in zijn geheel (als entiteit) als essentieel aan te wijzen. De zorgplicht op basis van de nieuwe wet zal nader worden uitgewerkt in een nieuwe Baseline Informatiebeveiliging (BIO2). Voor de meldplicht blijft IBD het loket voor de gemeentelijke overheden.

Voor het toezicht geldt ENSIA als toezichtstelsel en vanuit IBD wordt op dit moment nagegaan wat NIS2 betekent voor de inrichting van dit stelsel en welke nieuwe netwerken hieraan moeten worden toegevoegd. Met BZK en IPO is inmiddels afgesproken dat het interbestuurlijk toezicht vanuit de provincies in elk geval geen betrekking zal hebben op informatiehuishouding- en beveiliging. Vanuit VNG zal daarnaast het standpunt worden ingenomen richting de beleidsverantwoordelijke departementen (BZK en Justitie) dat het huidige systeem van toezicht – op een aantal kleinere wijzigingen na – ook in de toekomst gehandhaafd kan blijven.

Het onderdeel van bestuurlijke sancties wordt momenteel nog nader uitgewerkt door BZK. De opzet hiervoor ligt in lijn met de opzet die reeds voor de AVV geldt; indienen van een verbeterplan met oplegging van een last onder dwangsom, die verbeurd wordt indien daar niet aan wordt voldaan.

ADVIESRAAD

Vanuit de Adviesraad wordt de zorg uitgesproken dat de implementatie van NIS2 een groot beslag zal leggen op de capaciteit, middelen en kennis van gemeenten. Dit vormde eveneens de aanleiding voor de motie van de gemeente Heemstede die tijdens het afgelopen VNG Congres is aangenomen ("Geen NIS2 in de keten, voordat we iets weten"). De Adviesraad benadrukt daarom het belang van een zorgvuldig en goed afgestemd implementatietraject waarbij behoudt van de centrale positie van de IBD in binnen het Landelijk Dekkend Stelsel belangrijk is. Dit signaal vanuit de Adviesraad zal nogmaals worden ingebracht in het bestuurlijk overleg tussen de VNG en het Rijk.

Landelijk Dekkend Stelsel en de toekomst van de IBD-CERT

TOELICHTING

CERT staat voor Computer Emergency Response Team. De incidentondersteuning door CERT is één van de drie taken van de IBD en wordt uitgevoerd door een team van 6 medewerkers. Het spectrum van de incidentondersteuning bestaat aan het ene uiterste uit preventie en aan het andere uiterste uit evaluatie. Daar tussenin bevindt zich detectie en hulp bij concrete incidenten. Bij de uitvoering van deze taak maakt IBD gebruik van diensten van het Nationaal Cyber Security Centrum (NCSC) en andere sectorale CERT's. Omdat NIS2 ook nieuwe eisen stelt aan CERT's heeft IBD deze eisen op hoofdlijnen getoetst aan de huidige inrichting. De uitkomsten van deze analyse zijn inmiddels ook gedeeld met BZK.

Eén van de doorontwikkelrichtingen van IBD is het versterken van de CERT bestaande uit het leveren van politiek/bestuurlijke ondersteuning enerzijds en technische verdieping anderzijds. Vanuit BZK zijn er twee scenario's geschetst in het kader van het nieuwe CERT-stelsel: ofwel IBD-CERT voert alle wettelijke taken centraal uit met ondersteuning vanuit NCSC (scenario 1) danwel NCSC voert deze centrale rol uit waarbij IBD dan ondersteunend optreedt. Omdat het NCSC zelf ook volop in ontwikkeling is brengt het eerste scenario voor IBD de nodige risico's met zich mee. Het andere scenario heeft als belangrijkste nadeel dat gemeenten daarin alleen kunnen rekenen op de minimale eisen vanuit NIS2 waarmee de ondersteuning op locatie in feite wegvalt.

IBD stelt zich op het standpunt dat het terugbrengen van de incidentdienstverlening tot het niveau van de minimale eisen vanuit de wet (scenario 2) afbreuk doet aan hetgeen gemeenten met de IBD hebben opgebouwd aan sectorale kennis. Ook staat de goede samenwerking binnen het Landelijk Dekkend Stelsel zoals dat de afgelopen jaren is opgebouwd op het spel. Naar de mening van VNG zou juist meer moeten worden ingezet op samenwerking en kennisdeling binnen het netwerk.

ADVIESRAAD

De Adviesraad spreekt eveneens haar voorkeur uit voor scenario 1. In dat verband dient te worden ingezet op zo efficiënt mogelijk te organiseren van het werk binnen de bestaande structuur en op het versterken van de samenwerking en kennisdeling tussen gemeenten, bijvoorbeeld door middel van pooling of het fungeren als elkaars "achtervang". Op de meer schaarse kennisgebieden (zoals forensics) zou een intensievere samenwerking met de markt kunnen voorzien in de kennisbehoefte.

Effecten vonnis Hof van Twente in relatie tot opdrachtgeverschap gemeenten en de zorgplicht van leveranciers

TOELICHTING

De gemeente Hof van Twente heeft een leverancier in rechte aangesproken voor de geleden schade. De rechter heeft in zijn vonnis alle vorderingen afgewezen. Als onderbouwing hiervan stelt de rechter dat de gemeente zelf verantwoordelijk is voor de (digitale) informatiebeveiliging en als niet nadrukkelijk met de leverancier is overeengekomen dat hij verantwoordelijk is voor het uitvoeren van securitytests, hij dit dan ook niet hoeft te doen. Deze uitspraak heeft twee belangrijke effecten voor gemeenten. Allereest betekent dit dat alle bestaande contracten met leveranciers zouden moeten worden gescand op dit aspect. Een tweede effect is dat leveranciers op basis van dit vonnis zelf deze diensten - als aanvulling op bestaande contracten - tegen meerkosten zouden kunnen gaan aanbieden. Daarnaast zal ook bij de inkoop en aanbesteding van nieuwe contracten rekening met dit vonnis moeten worden gehouden. Deze uitspraak ziet overigens niet alleen op de zorgplicht van gemeenten, maar van alle overheden en ook van bedrijven.

VNG beziet samen met de gemeente Hof van Twente op welke wijze gepast gevolg kan en moet worden gegeven aan deze uitspraak.

ADVIESRAAD

De Adviesraad neemt met belangstelling kennis van deze uitspraak en geeft aan dat veel gemeenten nog onvoldoende doordrongen zijn van de gevolgen van deze uitspraak. Veel kleinere gemeenten zullen bovendien niet over de vereiste kennis en capaciteit beschikken om alle lopende contracten te scannen. Daarom adviseert de Adviesraad om hier vanuit IDB meer aandacht aan te schenken en hierover op een hoger (bestuurlijk) niveau met gemeenten te communiceren, bijvoorbeeld door middel van een ledenbrief.

***