Addendum notitie opvolging aanbevelingen *Kwetsbaar door Software*

Dit addendum bevat de reactie van de Vereniging Nederlandse Gemeenten (VNG) op de aanbevelingen uit het rapport *Kwetsbaar door software: Lessen naar aanleiding van beveiligingslekken door software van Citrix*. Op 13 december 2022 publiceerde de Onderzoeksraad voor Veiligheid de notitie opvolging aanbevelingen. De reactie van VNG kwam op 23 december binnen. In dit addendum zijn de meest relevante aspecten van de reactie van VNG opgenomen. De bevindingen en conclusies van de Onderzoeksraad over de opvolging van de aanbevelingen blijven ongewijzigd. De volledige notitie is gepubliceerd op de website.

Reactie Vereniging Nederlandse Gemeenten (VNG)

VNG stelt de conclusies en aanbevelingen van de Onderzoeksraad te herkennen en “de volle aandacht” te willen geven. Met name het stellen van veiligheidseisen rondom inkoop van software, alsook het delen van expertise en naadloze samenwerking op het gebied van digitale veiligheid, zijn volgens VNG relevant voor gemeenten.

VNG stelt er bij ministeries op aan te dringen dat de richtlijnen voor alle overheden eenduidig zijn en blijven. Om de kloof tussen digitale dreiging en weerbaarheid te dichten vindt de VNG het van belang om het onderscheid tussen vitaal en niet-vitaal te laten vervallen, bijvoorbeeld aangaande het delen van dreigingsinformatie. VNG: “Een digitaal veiligheidsstelsel, in samenhang met het fysieke veiligheidsstelsel is noodzakelijk om de continuïteit van de samenleving bij digitale verstoringen zowel lokaal, regionaal als ook nationaal te kunnen borgen.” Vanuit zijn positie benadrukt VNG de cruciale rol die ook gemeenten hierin spelen.

Volgens VNG hebben betrokken partijen sinds 2019 duidelijke lessen geleerd over het belang van een transparante en open uitwisseling van dreigingsinformatie. Als voorbeeld noemt VNG de respons op het Log4j-incident. Verbetering is volgens VNG echter mogelijk rondom informatiedeling vanuit het rijk en inlichtingendiensten met de Informatiebeveiligingsdienst (IBD) en gemeenten. VNG dringt daarom aan op een gelijke informatiepositie voor alle overheden. Ook stelt VNG dat de NLCS te weinig rekening houdt met de gemeentelijke uitvoeringscapaciteit om de doelen te bereiken. Daaromtrent ziet VNG drie “systeemuitdagingen” die moeten worden aangepakt om de digitale veiligheidsambitie te behalen, citaten schuingedrukt:

- *Een digitaal veiligheidsstelsel is nodig in samenhang met het fysieke veiligheidsstelsel, met uitwerking bevoegdheden en verantwoordelijkheden:*
- *Situationeel beeld is nu niet op te maken voor gemeentelijke organisatie én de stad, qua cyberdreigingsbeeld én cyberbeelden digitale criminaliteit.*
- *Er is structurele financiering op lokaal niveau noodzakelijk om uitvoering te geven aan deze plannen, met ingang van 2024 (Prinsjesdag 2023).*

Ook noemt VNG dat het momenteel een zogenoemd convenant opstelt met de minister van JenV en de staatssecretaris voor Digitalisering. Volgens VNG kunnen de partijen met dit convenant de samenwerking borgen tussen lokaal en nationaal bestuur. Zij tekenen het

convenant rond de jaarwisseling. Ten slotte noemt VNG dat het tijdens een recente ledenvergadering een motie heeft aangenomen voor meer structurele aandacht en financiering voor informatieveiligheid op lokaal niveau. Ondertekenaars van de motie vroegen de VNG ook zo spoedig mogelijk in gesprek te gaan met BZK over de processen rondom veiligheidsaudits.