Alle aanwezige fracties stemden voor

Onderwerp Zienswijzemogelijkheid Regionaal Risicoprofiel VGGM

De raad van de gemeente Renkum in vergadering bijeen op 30 september 2026 behandelend het raadsvoorstel Zienswijzemogelijkheid Regionaal Risicoprofiel VGGM

concludeert, dat
- gemeenteraden de mogelijkheid krijgt een zienswijze in te dienen op het Regionaal Risicoprofiel VGGM om daarmee te voldoen aan de verplichtingen uit de Wet veiligheidsregio's;
- dit dan moet gebeuren voor 2 oktober 2026;
- de gemeente Renkum niet het voornemen heeft een Zienswijze in te dienen;

is van mening, dat
1. hoewel redundantie en noodvoorzieningen zoals NCV bestaan, snelle detectie en herstel cruciaal blijft om de gevolgen te beperken, zou het risicoprofiel gegeven recente ontwikkelingen nadrukkelijker aandacht moeten krijgen;
2. de in het VGGM risicoprofiel benoemde redundantie a die de impact zou kunnen beperken tot niveau 3 geldt voor de netstroombeheerders en sommige onderdelen van defensie, maar niet voor de gemeente of maatschappij, waardoor de impact veel groter zou kunnen zijn dan verondersteld bij het wegvallen van vitale infrastructuur bijvoorbeeld langer dan 48 uur;
3. hacking in het rapport als ontwikkeling kort wordt benoemd, terwijl volgens experts deze dreiging als een significante dreiging wordt genoemd, (https://openai.com/nl-NL/collective-cyberdefense) en dit hacken kan komen door criminelen, buitenlandse inlichtingendiensten of gewoon door A.I. die zelf iets in gang zet (zie bijv. https://en.wikipedia.org/wiki/OpenAI%E2%80%93HuggingFace_incident);

Amendeert het voorstel door beslispunt 2 te veranderen in: een zienswijze wordt voor 2 oktober 2026 ingediend met de mening van de raad waarin meer aandacht gevraagd wordt voor een hogere weging van de schade impact factor van het risico door uitval van vitale infrastructuur, daarbij tevens via een analyse blijvende aandacht te geven welke groepen inwoners per risico het meest kwetsbaar zijn, hoe zelfredzaam zij zijn, en stil te staan bij de maatschappelijke weerbaarheid zowel bij uitval van elektronische communicatie als grootschalige mis- en desinformatie ten tijde van crises.

De raad gaat over tot de orde van de dag.
PRD/John Bartels PRO/ Naut Engelsma

Noot 1 : uit het voorliggende raadsvoorstel

Beslispunten
1. kennis te nemen van het Regionaal Risicoprofiel VGGM.
2. geen zienswijze in te dienen op het Regionaal Risicoprofiel VGGM.

Samenvatting
Gemeenteraden krijgen de mogelijkheid een zienswijze in te dienen op het Regionaal Risicoprofiel VGGM om daarmee te voldoen aan de verplichtingen uit de Wet veiligheidsregio's. Het voorstel is hier geen gebruik van te maken en geen zienswijze in te dienen. **Op 2 oktober 2026 loopt de termijn voor zienswijzen af.**

***Noot 2:** maatschappelijke impact bij stroomuitval langer dan 48/72 uur*
Hoewel redundantie en noodvoorzieningen zoals NCV bestaan, blijft snelle detectie en herstel cruciaal om de gevolgen te beperken.

1. Deze redundantie geldt alleen voor de netstroombeheerders en sommige onderdelen van defensie, maar niet voor de gemeente of maatschappij:
2. De gemeente heeft 1 mobiel noodstroomaggregaat en 1 vast noodstroomaggregaat en een paar honderd pompen voor het wegpompen van bijvoorbeeld afvalwater. Dat betekent dat na 3 tot 4 dagen stroomuitval bij veel inwoners de poep door de leidingen hun huizen instroomt.
3. De tankstations hebben geen noodstroomaggregaten waardoor er wel diesel in de grond zit, maar die niet bereikt kan worden.
4. De politie heeft geen noodstroomaggregaten waardoor bijvoorbeeld elektronische wapenkluizen, etc niet meer zullen werken.
5. De supermarkten en apotheken hebben geen noodstroomaggregaten en hebben allemaal het protocol om bij stroomuitval dicht te gaan.
6. Het GSM netwerk heeft maximale accucapaciteit voor 4 uur noodstroom, dus dit netwerk valt daarna uit.
7. Het C2000 netwerk heeft maximale accucapaciteit voor 8 uur noodstroom, dus dit netwerk valt daarna uit en hulpdiensten kunnen dan niet meer bereikt worden.
8. Veeteeltbedrijven, intramurale zorginstellingen (zoals niet-academische ziekenhuizen of verzorgingstehuizen), gemeentes etc. hebben een verplicht noodstroomaggregaat, echter vaak maar voor maximaal 48 uur aan diesel. Zij doen allemaal de aanname dat ze aan diesel kunnen komen. Dat lijkt niet realistisch te zijn.
9. Als alle beveiligingscamera's het niet meer doen en 112 niet gebeld kan worden, dan leert de ervaring in andere landen dat binnen 24 uur de eerste plunderingen starten. Die plundering leiden ook tot minder herstelvermogen (kapotte supermarkten kunnen niet open) en kunnen een vicieuze cirkel effect geven wat een hersteloperatie ernstig kan hinderen. Denk ook bijvoorbeeld aan het stelen van onbeveiligde noodstroomaggregaten, het aanvallen van zorgmedewerkers, het plunderen van verdovende middelen in een ziekenhuisapotheek, etc.
10. Een stroomstoring van slechts 24 uur zonder noodstroom verstoort ons distributiesysteem enorm. Er treedt dan een totale chaos op in distributiecentra, logistieke bedrijven etc., omdat die werken volgens just in time. Dat duurt heel lang om van te herstellen.
11. Als de NAVO in oorlog zou komen dan zijn de snelwegen en treinwegen nodig voor defensie. Dat werkt ook disruptie in allerlei ketens in de weg (om files te voorkomen, mag dan waarschijnlijk niemand de weg op). Ziekenhuispersoneel, distributiecentrum personeel, et cetera kunnen of gaan dan niet de weg op om naar hun werk.
12. Sommige cyberveiligheidsexperts zeggen:

Als hackers onze zonnepanelen massaal uit- en aanzetten, dan valt ons energienetwerk om. Dat moet dan vervolgens wijk voor wijk weer worden aangezet, wat vele dagen kost. Daarna kunnen ze gewoon het trucje herhalen en begint de cyclus weer van voren af aan. Zie ook (maar een voorbeeld, maar er zijn talloze rapporten: https://eenvandaag.avrotros.nl/artikelen/deze-ethische-hackers-kunnen-met-gemak-miljoenen-zonnepanelen-uitschakelen-dan-heb-je-een-landelijke-black-out-151574.

Het grote probleem is natuurlijk naast een risico analyse dat we nog niet weten hoe om te gaan met de maatschappelijke weerbaarheid. Veel ambtenaren en politici denken dat we 3 jaar de tijd hebben. Volgens verschillende cyberveiligheids- en defensieexperts, spreken we over 6 tot 24 maanden. Een enorme disconnect. Dat gat in horizon beleving zou in de risico analyse meer benoemd kunnen worden.