4
Vragenuur: Vragen Van der Molen

Vragen van het lid Van der Molen aan de minister van Infrastructuur en Waterstaat over **het bericht "Sluizen gammel beveiligd"**.

De **voorzitter**:
Dan ga ik nu naar de heer Van der Molen, namens het CDA, die een vraag stelt aan de minister van Infrastructuur en Waterstaat over de beveiliging van sluizen.

☐

De heer **Van der Molen** (CDA):
Voorzitter, dank u wel. Je moet er niet aan denken dat in juist een land als Nederland, waar de hele wereld kijkt naar hoe we het water buiten de dijken houden, er op grote schaal iets mis zou zijn met de beveiliging van onze sluizen. Je zult maar in bijvoorbeeld de Zuidplaspolder, naast de A20, meer dan 6 meter onder NAP, voor je droge voeten afhankelijk zijn van de nationale waterhuishouding.

Toch is er veel aan de hand met de beveiliging van onder andere onze sluizen. Het blad Binnenlands Bestuur kopte dit weekend "Sluizen gammel beveiligd", en zegt ook dat het erop lijkt dat de waterschappen de kop in het zand steken. Software voor onze sluizen gaat 25 tot 30 jaar mee, maar wordt hooguit tot vijf jaar na inkoop ondersteund met beveiligingsupdates. Een betrouwbare bron binnen de waterschappen meldt het blad dat de beveiliging van de software waarmee sluisdeuren worden bediend, op dit moment rammelt. Sta er eens bij stil; een hacker kan nu op afstand sluisdeuren openzetten, zonder dat we dat meteen doorhebben. Vooral wanneer een hacker dat bij veel systemen zou doen, tegelijkertijd, kan er grote schade veroorzaakt worden.

Er wordt in het artikel een opsomming van problemen gegeven. Er zou vaak geen cruciaal onderhoud voor oudere software beschikbaar zijn. Waterschappen zouden te kleine budgetten hebben om tests uit te voeren. In aanbestedingen zou er te weinig aandacht voor informatieveiligheid zijn. Waterschappen kunnen het amper opnemen tegen de machtige softwareleveranciers. Er zou ook geen goede wetgeving zijn om de beveiliging af te dwingen. Bij de begroting Infrastructuur en Waterstaat zei de minister nog dat cybersecurity van groot belang is, maar ze maakte er verder weinig woorden aan vuil.

Het CDA vindt het niet acceptabel dat onze sluizen op dit moment dit risico lopen. Vandaar een aantal vragen aan de minister. Erkent de minister dat we in Nederland een onaanvaardbaar risico lopen als het gaat om de bewaking van onze sluizen? Wat gaat de minister naar aanleiding van het artikel concreet ondernemen om onze infrastructuur ook digitaal te beveiligen? Is de minister bereid om met gezwinde spoed naar de eigen infra van Rijkswaterstaat te kijken en met waterschappen en gemeenten, die ook op grote schaal sluizen beheren, in overleg te gaan over wat er mogelijk is om het hacken van sluizen en bruggen te voorkomen? Wil ze de Kamer over de uitkomst hiervan op de hoogte stellen?

De **voorzitter**:
Het woord is aan de minister.

☐

Minister **Van Nieuwenhuizen-Wijbenga**:
Dank u wel, voorzitter. Ik ben blij dat de heer Van der Molen deze vragen stelt. Ik heb bij de begroting van ons ministerie aangegeven dat ik zelf ook een heel belangrijke prioriteit wil maken van cybersecurity. Als u zegt dat het onaanvaardbaar is dat onze kritische infrastructuur dit soort risico's loopt, ben ik dat direct met u eens. Gelukkig heeft de kritische infrastructuur een heel goede beveiliging. Die is heel goed op orde. U verwijst naar het artikel, dat specifiek over de waterschappen gaat. De waterschappen gaan niet over de kritische infrastructuur. Daarvoor is Rijkswaterstaat verantwoordelijk, en wij op het ministerie dus ook.

Meteen bij mijn aantreden heb ik in brede zin gevraagd naar de cybersecurity, zowel over wat we aan de voorkant doen aan preventie en monitoren en wat we doen voor het geval het toch mocht gebeuren. Ik ben erachter gekomen dat daar in de afgelopen jaren al flink aan is gewerkt. Er is de afgelopen jaren al ongeveer 100 miljoen specifiek uitgegeven voor de fysieke en digitale beveiliging van kritische infrastructuur, maar we zijn er nog niet mee klaar. Er komt ook nog een Algemene verordening gegevensbescherming aan, die meer ziet op privacyrisico's.

Om al die digitale dreigingen aan te pakken, zijn nog heel veel aandacht en inzet nodig. Dat is gelukkig een speerpunt van het kabinet. Het staat ook in het regeerakkoord. Er wordt extra geld voor uitgetrokken. Ik zie de voorzitter al kijken dat het antwoord niet te lang moet duren, maar het waren meerdere vragen in één. Uw suggestie om er met het veld over in gesprek te gaan, had ik zelf ook op mijn lijstje staan. Morgen hebben we een bestuurlijk overleg water, waarbij we alle partners uit het waterveld, van provincies, gemeenten, waterschappen en de Unie van Waterschappen aan tafel hebben. Ik wil dit heel graag met hen bespreken om te bekijken wat zij eraan kunnen doen.

De heer **Van der Molen** (CDA):
Ik val de minister bij als zij zegt dat waterschappen een eigen verantwoordelijkheid hebben, maar als minister wilt u natuurlijk ook weten dat hun onderdeel van de beveiliging van onze sluizen op orde is. Ik ben blij om te horen dat de minister met waterschappen en andere overheden om tafel wil, maar het is ook belangrijk dat de Kamer straks precies weet wat de kwetsbaarheid is van deze sluizen.

Ik wil de minister vragen nog iets specifieker te zijn over de toezegging om de Kamer te informeren na het overleg. Zou de minister kunnen toezeggen wat een eventueel plan van aanpak gaat worden? Het artikel geeft heel nadrukkelijk risico's aan. Zou de minister de Kamer ook kunnen laten weten wat de specifieke kwetsbaarheden zijn? Over welke punten hebben we het dan en waarmee moeten we rekening houden? Is de minister bereid om niet alleen te overleggen met waterschappen en gemeenten, maar ze ook te helpen op de vlakken waarop ze zelf misschien niet kunnen bereiken, bijvoorbeeld bij softwareleveranciers, dat ze de beveiliging wel op orde krijgen?

Minister **Van Nieuwenhuizen-Wijbenga**:
Dat zijn wederom een heel aantal vragen. Ik denk helemaal in dezelfde lijn. Ik wil met alle waterbestuurders een nieuw Bestuursakkoord Water gaan afsluiten. Wat mij betreft wordt cybersecurity daarin een heel nieuw aandachtspunt, waarover we met elkaar afspraken maken. Net zoals u over de rest van het Bestuursakkoord Water wordt geïnformeerd, zal wat mij betreft ook het onderdeel cybersecurity daarin een belangrijke rol spelen. We werken al heel goed samen met de Unie van Waterschappen. We hebben ook een security operation center, waarbij vanuit de Unie van Waterschappen steeds mensen naar voren worden geschoven die een aantal maanden mee komen draaien, ook in de 24/7-diensten waarbij ze ook actief mee naar oplossingen moeten zoeken als er zich iets voordoet. Daar is de Unie van Waterschappen al bij aangehaakt, maar ik wil u daarover ook graag informeren. Waar het gaat om het aanbestedingsbeleid, het inkoopbeleid lopen we redelijk voorop met het principe van security by design. Bij het begin van het ontwerpen van het systeem wordt dus al nagedacht over hoe je de cybersecurity aanpakt. Daar zijn we al voortvarend mee aan de slag, maar ik wil u graag informeren hoe we dat verder breed kunnen uitdragen, ook bij de waterschappen.

De heer **Van der Molen** (CDA):
Dank aan de minister voor de toezeggingen. Het is goed om te horen dat zij ook bij dat nieuwe akkoord waarvoor ze ook met de waterschappen om de tafel gaat, cybersecurity een hoofdonderdeel laat zijn. Als CDA-fractie zullen wij daar heel kritisch naar kijken, want het artikel in Binnenlands Bestuur heeft namelijk nog eens benadrukt hoe belangrijk het is om ook onze cyberveiligheid op orde te hebben. Nogmaals, het is goed om te horen dat de minister dat op dit vlak ook tussen de oren heeft.

Dank u wel.

De **voorzitter**:
Dank u wel. Dan kijk ik of er aanvullende vragen zijn. Dat is het geval. De heer Bisschop namens de SGP.

De heer **Bisschop** (SGP):
Voorzitter, dank. Het gaat hier over een cruciaal onderdeel van de waterinfrastructuur. Als dan blijkt dat het zo kwetsbaar is, dan is het goed dat er op gereageerd wordt en er maatregelen worden genomen ter voorkoming. Om de juiste maatregelen te nemen, kan ik mij wel voorstellen dat de minister zich ook afvraagt waar het dan fout is gegaan in het verleden en hoe die situatie heeft kunnen ontstaan. Heeft de minister daar zicht op en wordt daar voldoende op geacteerd om te voorkomen dat iets soortgelijks in de toekomst zich opnieuw voordoet?

Minister **Van Nieuwenhuizen-Wijbenga**:
Ik wil wel het beeld wegnemen dat er nu van alles mis zou zijn. Zeker waar het de kritische infrastructuur aangaat, wil ik ook het beeld wegnemen dat daar nog met verouderde software wordt gewerkt waar je dan niets meer mee zou kunnen qua update. Er is heel erg goed gekeken naar de fysieke beveiliging — hoe zou je bij die systemen kunnen komen? — maar ook naar de digitale beveiliging. Er is voor gezorgd dat het standalonesystemen zijn, die dus niet verbonden zijn met internet en die dus ook op die manier niet te hacken zijn. Bovendien is er een achtervang dat als het systeem uitvalt, handmatige of mechanische bediening mogelijk is. Dus u hoeft zich er geen zorgen over te maken dat er met de echt vitale onderdelen iets mis zou zijn.

Wat betreft uw vraag hoe we dit voor de toekomst kunnen verbeteren, sta ik open voor iedere suggestie, maar we zijn er dus al hard mee aan het werk. We zullen dat de komende tijd alleen maar verbreden. Ik ben blij met iedereen die met ons hieraan prioriteit wil geven. Het is wat dat betreft ook heel goed om te zien dat het prominent in het regeerakkoord staat, want het geldt niet alleen voor onze kritische infrastructuur maar natuurlijk voor de gehele overheid en ons gehele bedrijfsleven. Kijk ook naar de algemene verordening Gegevensbescherming die in mei 2018 van kracht wordt, waaraan we samenlevingbreed nog een hele uitdaging hebben met elkaar.

De **voorzitter**:
Dank u wel.