

Zaaknummer: 347860

Vragen van statenlid de heer Berend Boone (BBB) ingevolge artikel 44 reglement van orde

AANHANGSEL

tot de notulen van de Provinciale Staten van Zeeland 2023 nummer 001.

Vragen ingevolge artikel 44 van het reglement van orde inzake Ddos-aanval die havenbedrijf North Sea Port platlegde:

(ingekomen: 21 juni 2023)

Vragen aan Gedeputeerde Staten		Antwoorden van Gedeputeerde Staten	
1.	Is GS bekend met de ddos aanval op de website van North Sea Port?	1.	Ja
2.	Hoe kijkt GS naar de ddos-aanval op de website van North Sea Port?	2.	Wij vinden DDoS-aanvallen, zoals de aanval op de website van North Sea Port, een zorgelijke ontwikkeling. Met deze aanvallen kan in het slechtste geval grote schade worden aangericht. Veel organisaties, zowel groot als klein, hebben hier mee te maken. Zo werden zeer recent ook DDoS-aanvallen op de websites van andere Nederlandse havens uitgevoerd.
3.	Hoe kwetsbaar is North Sea Port voor cyberaanvallen?	3.	North Sea Port onderkent de noodzaak van een goede cyberweerbaarheid om de continuïteit van haar organisatie te borgen. Daartoe hanteert North Sea Port een internationaal erkende methodiek om risico's te inventariseren en daarvoor passende en aanvaardbare maatregelen te nemen. North Sea Port meet en rapporteert dit aan haar bestuur en het Toezicht-houdend orgaan. Binnen North Sea Port is een team van IT- en Cybersecurity specialisten werkzaam dat zich ook met deze problematiek bezighoudt.
4.	Is de veiligheid in de Zeeuwse havens in het geding geweest gedurende de ddos-aanval?	4.	Nee, de veiligheid is op geen enkel moment in het geding geweest. Gedurende de DDoS-aanval zijn alle diensten die zich bezighouden met operatie en veiligheid in de havens, conform de noodplannen, op de hoogte gehouden.
5.	Wat zijn de risico's voor de Zeeuwse havens bij dergelijke aanvallen?	5.	Op de vraag wat de risico's kunnen zijn, kan om reden van veiligheid niet worden ingegaan. North Sea Port neemt maatregelen om de cyberrisico's die een bedreiging vormen voor haar eigen organisatie, de operatie in de haven en veiligheid daarbinnen weg te nemen of te mitigeren. Daarbij neemt zij ook haar verantwoordelijkheid om ervoor te zorgen

Vragen aan Gedeputeerde Staten		Antwoorden van Gedeputeerde Staten	
			dat haar eigen systemen niet ingezet kunnen worden voor een cyberaanval op derden.
6.	Hoe kunnen dergelijke aanvallen op belangrijke infrastructurele organisaties in Zeeland in de toekomst voorkomen worden?	6.	Een DDoS-aanval kan niet voorkomen worden, maar wel worden afgeslagen.

MIDDELBURG, 11 juli 2023

Namens fractie: BBB

Gedeputeerde Staten

Statenlid de heer Berend Boone

Drs. J.M.M. Polman

Drs. M.C.J. Franken