provincie Zuid-Holland

Antwoord van Gedeputeerde Staten op vragen van

E. D. van Engel (VVD)
(d.d. 28 maart 2024)

Nummer
4072

Onderwerp
Internetbeveiliging provinciale websites

Aan de leden van Provinciale Staten

Toelichting vragensteller

Op 25 en 26 maart jl. berichtten Binnenlands Bestuur en diverse andere media in online artikelen over ddos-aanvallen op provinciewebsites van Noord-Holland, Groningen en Noord-Brabant.

De VVD maakt zich zorgen over de digitale beveiliging van de websites van provincie Zuid-Holland. Wij hechten belang aan een goede online zichtbaarheid, toegankelijkheid en bereikbaarheid van onze overheid; het neerhalen van overheidswebsites door cyberaanvallen heeft hier een negatief effect op.

1. *Deelt Gedeputeerde Staten deze opvatting en welke (preventieve) maatregelen worden genomen om onze digitale infrastructuur tegen dergelijke bedreigingen te wapenen?*

Antwoord
Ja. De website zuid-holland.nl is benoemd als een belangrijk informatiesysteem voor de provincie Zuid-Holland omwille van de zichtbaarheid, toegankelijkheid en bereikbaarheid. Om de website tegen uitval door DDoS-aanvallen te beschermen, maakt de provincie gebruik van anti-DDoS-maatregelen (Distributed Denial of Service). Deze maatregelen zijn op 25 en 26 maart 2024 effectief geweest tegen de DDoS-aanval die ook de website van provincie Zuid-Holland tot doel had. De website is op 25 en 26 maart steeds bereikbaar geweest.

2. *Hoe zorgt onze provincie voor een vooruitstrevende aanpak in digitale veiligheid, anticiperend op potentiële cyberdreigingen? Wordt bijvoorbeeld gebruik gemaakt van initiatieven als Nawas en/of ethical hacking?*

Antwoord
De provincie kent een breed palet aan maatregelen en initiatieven op het gebied van techniek, organisatie en medewerkers om cyberveiligheid te waarborgen. De provincie maakt gebruik van een anti-DDoS wasstraat en voert planmatig ethical hacking testen uit.

3. *Wat zijn de lange termijn plannen van de provincie om de cyberweerbaarheid te vergroten tegen zowel huidige als toekomstige digitale bedreigingen?*

Antwoord
De provincie heeft de aanpak van informatieveiligheid de afgelopen jaren geïntensiveerd. De provincie werkt aan de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)[1] en het normenkader ISO27001 voor informatieveiligheid[2], waaraan de provincie zich interprovinciaal heeft gecommitteerd. Daarnaast implementeert de provincie de Europese richtlijn *Network and Information Security Directive* (NIS2-richtlijn)[3] die momenteel door het Rijk in Nederlandse wetgeving wordt omgezet.

4. *Op welke wijze initieert en stimuleert Zuid-Holland de samenwerking met andere provincies en nationale overheden om kennisuitwisseling en gezamenlijke verdedigingsstrategieën tegen cyberaanvallen te bevorderen?*

Antwoord
De provincie neemt actief deel aan interprovinciale gremia en initiatieven op het gebied van informatieveiligheid, zoals bijvoorbeeld het interprovinciale project dat tot aansluiting bij het Nationaal Cyber Security Centre (NCSC) zal leiden. Het NCSC zal, in het kader van NIS2, voor de provincies de rol van computercrisisteam (Computer Security Incident Response Team - CSIRT)[4] nemen.

Den Haag, 23 april 2024

Gedeputeerde Staten van Zuid-Holland,
secretaris, voorzitter,

drs. M.J.A. van Bijnen MBA drs. J. Smit

[1] Voor meer informatie: https://www.bio-overheid.nl
[2] Voor meer informatie: https://nl.wikipedia.org/wiki/ISO/IEC_27001
[3] Voor meer informatie: https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/samenvatting-nis2-richtlijn
[4] Voor meer informatie: https://www.ncsc.nl/over-ncsc/wettelijke-taak