Mondelinge vragen digitale veiligheid
25 maart is de website van provincie Noord-Holland (en drie andere provincies) door een DDoS-aanval uit de lucht geweest[1]. Het is al lang bekend dat digitale veiligheid geen vanzelfsprekendheid is door statelijke actoren, zoals dit voorval laat zien.
Uit beantwoording van technische vragen blijkt dat digitale veiligheid een rol met betrekking eigenlijk alle processen van de provincie speelt. Dus ook over operationele technologie, zoals op afstand bedienbare bruggen, tunnels en sluizen in Noord-Holland[2]. De maatschappij loopt in deze operationele technologie het grootste risico rondom digitale veiligheid.

Volt maakt zich grote zorgen over de digitale veiligheid, met name bij operationele technologie. Daarom de volgende vragen:

1. Voelt GS net als Volt ook de urgentie om digitale veiligheid, met name rondom operationele technologie, te waarborgen?
2. Wat vindt GS in het licht van de DDoS aanval ervan dat digitale veiligheid op dit naar marktpartijen geoutsourced is?

Onze fractie kan geen beleid rondom digitale veiligheid vinden. Terwijl dit thema met de komst van nieuwe EU richtlijn Network & Information Security 2 (NIS 2) dit urgenter is dan ooit.

3. Is GS van mening voldoende grip te hebben op digitale veiligheid? Worden er bijvoorbeeld audits en dergelijke uitgevoerd?
4. Is GS net als Volt van mening om beleid over digitale veiligheid te ontwikkelen?

Maik de Weerdt
Volt

[1] Brief GS aan PS over DDoS-aanval
[2] Centrale bediening bruggen en sluizen