V-100 (27 mei 2024) – Vragen over thema (7) Cyberweerbaarheid mkb en data-encryptie

Aan de minister van Economische Zaken en Klimaat

1. Het Digital Trust Center (DTC) zet in op het delen van kwetsbaarheidsinformatie met door DTC gesubsidieerde stichtingen en samenwerkingsverbanden die deze informatie commercieel beschikbaar stellen. Dat heeft tot gevolg dat publiek beschikbare beveiligingsinformatie alleen te verkrijgen is door bedrijven die daarvoor betalen. Volgens informatie van het DTC betreft het hier minder dan 1% van het aantal bedrijven in Nederland.
   Bent u zich bewust van deze situatie, in hoeverre acht u dit wenselijk en zo nee, ziet u mogelijkheden dit te veranderen?

2. In hoeverre denkt u dat de cyberweerbaarheid te verhogen is door bedrijven te verplichten zich te verzekeren tegen digitale dreigingen (naar analoge van traditionele risico's als brand, inbraak of aansprakelijkheid) en in hoeverre overweegt u een dergelijke verplichting?

3. Nederland is buiten de top-10 vestigingsklimaat beland voor start-ups en scale ups. In hoeverre overweegt u belastingvoordelen of een voorkeursbeleid bij het inhuren van Nederlandse start-up/scale-ups op gebied van digitale weerbaarheid op deze positie te verbeteren?

4. Generatieve AI wordt al ingezet voor cyber-aanvallen. De huidige maatregelen lijken vooral gericht op het opleiden van MKB'ers tot cybersecurity-specialist.
   Wat wordt er concreet nu gedaan rondom generatieve AI en hoeveel geld is hiervoor gereserveerd? In hoeverre hebben deze investeringen resultaat en hoe worden deze gemeten?

5. Projecten zoals GPT-NL en OpenKAT worden door de overheid gefinancierd.
   Is er bij deze projecten rekening gehouden met (verwachtingen ten aanzien van) de kwaliteit van het GPT-NL model gezien het lage budget wat hiervoor is gereserveerd?
   In hoeverre gaat GPTNL concurreren met LLM's als ChatGPT4o en LLama70b?
   Zijn deze initiatieven vanuit de overheid rechtmatig of is hier sprake van concurrentie met de markt (zie Wet markt & overheid)?
   Worden er Nederlandse startups en scale-ups betrokken bij de ontwikkeling van deze projecten?
   Hoe zorgt de overheid voor een beheer-ecosysteem, waarin de verantwoordelijkheid binnen de keten wordt geadresseerd zodra het project de eerste resultaten heeft opgeleverd?

6. In sectoren zoals brandveiligheid, automotive en beveiligingsbedrijven is het vanzelfsprekend dat je met goedgekeurde/gecertificeerde bedrijven samenwerkt en je als gebruiker geen specialist hoeft te worden om het product te gebruiken. De huidige maatregelen rondom cybersecurity en AI lijken er op gericht om het MKB op te leiden als specialist i.p.v. concrete oplossingen voor de problematiek te komen.
   Hoe maken we het MKB vanzelfsprekend veilig?

Hoe kan een MKB'er zekerheid krijgen op het feit dat zij voldoet aan de gestelde veiligheidseisen? Als parallel met de auto-industrie valt er veel te leren: i) je bent verplicht verzekerd; ii) je hebt een zorgplicht om met een veilige auto de weg op te gaan; iii) je rijdt in een gecertificeerd type voertuig dat door een gecertificeerde partij is gekeurd en door een gecertificeerde partij is geproduceerd; en iv) mensen zijn (zo goed als) gestopt met rijden onder invloed toen verzekeraars verklaarden dat je in dat geval onverzekerd rondrijdt.

7. Welke concrete doelen heeft u het DTC gesteld ten aanzien van cyberweerbaarheid van het MKB? Welke maatregelen heeft u getroffen om te zorgen dat het MKB wordt betrokken, de dienstverlening van DTC de MKB ook daadwerkelijk bereikt en hoe en worden doeltreffendheid van de activiteiten gemeten?

<u>Aan de minister van Justitie en Veiligheid</u>

1. Cybersecurityprofessionals kunnen in reactie op een cybersecurityincident soms data terughalen of schade voorkomen door snel acties te ondernemen die juridisch onrechtmatig of strafbaar zijn (naar analogie van noodweer of een burgerarrest in de fysieke wereld). In hoeverre overweegt u deze professionals - onder bepaalde voorwaarden - ruimte te geven deze acties toch te nemen?