Stelling D: De overheid zou een nationaal fonds moeten oprichten om MKB-bedrijven te ondersteunen bij het verbeteren van hun cyberveiligheid

Groep: Groen
Lokaal: LD107
Debatleider: Tim Hazeldonk
Voorstander: Bavli Armanyous
Tegenstander: Pascal de Bruijn
Jury voorzitter: Vo Nguyen
Jury lid: Lucas van Boxtel

Argument 1

Argument

De overheid moet dit doen omdat veel MKB-bedrijven onvoldoende budget en expertise hebben om basisbeveiliging op orde te brengen, terwijl zij wel dezelfde dreigingen krijgen als grote organisaties.

Uitleg

Cybersecurity is voor veel MKB'ers een kostenpost met onduidelijke opbrengst. Daardoor worden basismaatregelen zoals sterke inlogbeveiliging, patching, back-ups, training en monitoring uitgesteld. Dat maakt MKB-bedrijven een aantrekkelijk doelwit voor phishing en ransomware. Een fonds verlaagt de drempel en maakt het mogelijk om juist die basismaatregelen snel en structureel te implementeren.

Bewijs/Voorbeeld

Bij incidenten zien we dat basishygiëne vaak het verschil maakt. In Nederland zagen we dit bijvoorbeeld bij Van der Valk in september 2025: medewerkers klikten op phishing via een nagemaakte inlogpagina, waarna aanvallers reserverings- en klantgegevens gebruikten om gasten gericht op te lichten en betaalgegevens te stelen. Dit patroon geldt ook voor het MKB: één geslaagde phishingactie kan genoeg zijn om accounts over te nemen, data te misbruiken en schade te veroorzaken. Met fondssteun kan een MKB'er concrete basismaatregelen nemen zoals phishing-resistente multi-factor authenticatie en een meldcultuur, waardoor de kans op succes van dit soort aanvallen daalt.

Argument 2

Argument

Een nationaal fonds is logisch omdat cyberincidenten niet alleen private schade veroorzaken, maar ook maatschappelijke schade. De overheid investeert dus in het beschermen van de economie en het vertrouwen in digitale dienstverlening.

Uitleg

Als een MKB-bedrijf geraakt wordt, blijft het niet binnen dat ene bedrijf. Denk aan leveranciersketens, klanten, dienstverlening en vertrouwen. Bovendien kost herstel vaak veel meer dan preventie. Door preventie te subsidiëren beperk je continuïteitsproblemen, reputatieschade, juridische issues en indirecte schade zoals stress bij slachtoffers en verlies aan vertrouwen in digitale communicatie.

Bewijs/Voorbeeld

Het Change Healthcare-incident in februari 2024 (Verenigde Staten) laat zien hoe één partij in de keten enorme gevolgen kan hebben voor veel andere organisaties: door een ransomware-aanval vielen systemen uit en raakten processen zoals declaraties en zorgafhandeling grootschalig verstoord, met keteneffecten bij veel zorgverleners. Ook al is dat geen MKB, de les is ketenafhankelijkheid: als één schakel uitvalt, vallen processen bij anderen stil. Veel MKB'ers zitten als leverancier in ketens. Een fonds helpt om te voorkomen dat kleine schakels de "zwakke plek" worden die grote impact veroorzaakt.

Argument 3

Argument

Met een fonds kan de overheid sturen op effectiviteit: het geld kan gekoppeld worden aan bewezen maatregelen en meetbare eisen, zodat het niet blijft bij goede bedoelingen.

Uitleg

Een fonds is niet "gratis geld"; je kunt het slim inrichten. Bijvoorbeeld: subsidie alleen voor concrete verbeteringen zoals MFA, back-up en hersteltests, patch-SLA's, basis logging/monitoring, en korte rolgerichte trainingen. Ook kun je dit combineren met een nulmeting en een herhaalmeting. Zo wordt security voor het MKB niet ingewikkeld, maar haalbaar en controleerbaar.

Bewijs/Voorbeeld

Het CrowdStrike update-incident van 19 juli 2024 (wereldwijd) laat zien dat zelfs security tooling zelf risico's kan creëren als processen niet goed zijn ingericht: een fout in een update veroorzaakte wereldwijd Windows-crashes, waardoor veel organisaties tegelijk uitvielen en continuïteitsproblemen kregen. Dat onderstreept dat je naast tools ook procesmaatregelen nodig hebt, zoals change management en gefaseerde updates. Een fonds kan MKB-bedrijven helpen om tooling én processen goed in te richten, zodat maatregelen niet alleen "aan staan", maar ook veilig beheerd worden.

Korte afsluitzin (sterk in debat)

De overheid moet een nationaal fonds oprichten omdat het MKB anders structureel achterblijft, terwijl de dreiging hetzelfde is en de maatschappelijke impact groot kan zijn. Met gerichte, meetbare steun verbeter je de basisbeveiliging, verlaag je de kans en impact van incidenten, en bescherm je continuïteit en vertrouwen.

Verwachte tegenargumenten (kort) en jouw weerlegging

Tegenargument: “Dit is verantwoordelijkheid van bedrijven zelf.”

Weerlegging: Dat klopt, maar cyberrisico’s hebben externe effecten: ketens, klanten en vertrouwen raken mee. De overheid ondersteunt ook bij brandveiligheid, innovatie en duurzaamheid; cyberweerbaarheid is net zo’n basisvoorwaarde.

Tegenargument: “Dit wordt geldverspilling.”

Weerlegging: Alleen als je het slecht ontwerpt. Koppel subsidie aan concrete controls en meetbare verbeteringen, en je krijgt aantoonbaar effect.

Tegenargument: “MKB moet het gewoon via verzekeringen regelen.”

Weerlegging: Verzekeren voorkomt geen incident. Bovendien worden eisen van verzekeraars strenger; zonder basismaatregelen worden MKB’ers onverzekerbaar of extreem duur. Het fonds helpt juist om aan minimumniveau te voldoen.