vergadering **C185**
zittingsjaar 2021-2022

Woordelijk Verslag

Commissievergadering

Commissie voor Economie, Werk, Sociale Economie, Wetenschap en Innovatie

van 24 februari 2022

(Wegens de coronamaatregelen werd deze vergadering via videoconferentie georganiseerd.)

Vlaams Parlement

INHOUD

VRAAG OM UITLEG van Stijn De Roo aan Hilde Crevits, viceminister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw, over de steun aan bedrijven om te investeren in cybersecurity
– 1754 (2021-2022)
VRAAG OM UITLEG van Maurits Vande Reyde aan Hilde Crevits, viceminister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw, over de uitvoering van het Vlaams Beleidsplan Cybersecurity
– 1773 (2021-2022)
VRAAG OM UITLEG van Andries Gryffroy aan Hilde Crevits, viceminister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw, over cybersecurity in Vlaamse ondernemingen
– 1797 (2021-2022) 3

VRAAG OM UITLEG van Andries Gryffroy aan Hilde Crevits, viceminister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw, over het stimuleren van Vlaamse bedrijven om batterijen milieuvriendelijker te maken
– 1905 (2021-2022) 9

VRAAG OM UITLEG van Stijn De Roo aan Hilde Crevits, viceminister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw, over de steun aan bedrijven om te investeren in cybersecurity
– 1754 (2021-2022)

VRAAG OM UITLEG van Maurits Vande Reyde aan Hilde Crevits, viceminister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw, over de uitvoering van het Vlaams Beleidsplan Cybersecurity
– 1773 (2021-2022)

VRAAG OM UITLEG van Andries Gryffroy aan Hilde Crevits, viceminister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw, over cybersecurity in Vlaamse ondernemingen
– 1797 (2021-2022)

Voorzitter: de heer Robrecht Bothuyne

De voorzitter: De heer De Roo heeft het woord.

Stijn De Roo (CD&V): Minister, maar liefst 12 procent van de ondernemingen werd het afgelopen jaar geconfronteerd met cyberaanvallen. De aanvallen op de havens van Gent en Antwerpen eind januari sprongen misschien het meest in het oog, maar ook kleine ondernemingen ondervinden vaak zware gevolgen wanneer ze getroffen worden door een cyberaanval. Bij de getroffen kmo's stelt 40 procent dat de ICT-systemen onbruikbaar werden, 20 procent dat gegevens verloren gingen en 10 procent dat gegevens gestolen werden.

Om onze ondernemingen beter te beschermen, wordt de drempel voor overheidssteun bij een verbetertraject voor cybersecurity verlaagd, naast de bestaande steun die bedrijven konden aanvragen wanneer ze meer dan 25.000 euro investeerden in een verbetertraject rond cybersecurity. Nu wordt hiervan ook een lightversie ondersteund, waarbij een kleiner pakket aan begeleiding en advies wordt aangeboden dat zo'n 15.000 euro zou kosten. Daarnaast worden de steunplafonds opgetrokken die via de kmo-portefeuille kunnen worden opgevraagd. Dat is tot 45 procent voor kleine bedrijven – daarvoor 30 procent –, en tot 35 procent voor middelgrote bedrijven – daarvoor 20 procent.

Deze ondersteuning zal bedrijven ongetwijfeld aanzetten om bewuster te investeren in cybersecurity. Dat is natuurlijk een goede zaak. We moeten echter oppassen voor de effecten van dergelijke subsidies op de prijzen. Het Centraal Planbureau van Nederland merkte in 2018 bijvoorbeeld op dat de cybersecuritymarkt in Europa onvolkomen werkt: afnemers hebben doorgaans de keuze tussen een beperkt en duur nationaal aanbod of een goedkoper internationaal aanbod, waarin men echter te weinig vertrouwen heeft. De Europese markt biedt nog niet voldoende kansen om schaalvoordelen te realiseren voor Europese ondernemingen, waardoor betere concurrentie uitblijft. Ondertussen zijn er wel tal van initiatieven rond de Europese digitale markt genomen, onder meer een EU Cybersecurity Strategy, die werd aangenomen in december 2020.

Minister, kunt u meer toelichting geven over de aanleiding om de lightversie van de steun voor een cybersecurity-verbetertraject in het leven te roepen? Hoe weerspiegelt zich dat in de concrete modaliteiten?

Zult u monitoren of de subsidies een prijsopdrijvend effect zullen hebben?

Wat verwacht u van de Europese initiatieven rond cybersecurity? Zijn er zaken waarop we vanuit Vlaanderen nog verder kunnen inspelen?

De voorzitter: De heer Vande Reyde heeft het woord.

Maurits Vande Reyde (Open Vld): Ik wil me aansluiten bij deze vragen. Ze werden vorige week uitgesteld op vraag van collega Gryffroy. Ik heb hem toen volmondig gesteund, maar ik had wel de kleine voorwaarde gesteld dat hij een souvenir uit het mooie New York zou meebrengen. Ik heb gisteren vernomen dat hij niet aan die voorwaarde heeft voldaan. Dat stemt me toch enigszins ontevreden, maar ik neem aan dat hij daar misschien een goede reden voor heeft. Dit terzijde!

Wat de heer De Roo en de heer Gryffroy in deze vragen ook aanraken, is natuurlijk heel pertinent. We weten allemaal dat de digitalisering voor geweldige opportuniteiten zorgt, maar de gevaren voor onze bedrijven, overheidsadministraties en zorginstellingen zijn wel reëel en ze stijgen elke dag, niet in het minst ook vandaag. We hebben vandaag een dreiging van een imperialistische mogendheid, die zich ook op digitaal vlak zou kunnen verderzetten. Dat noopt ons toch om steeds meer na te denken over hoe we onze digitale infrastructuur kunnen beveiligen.

Zo was er recent nog een grootschalige cyberaanval op de Antwerpse haven. De potentiële economische schade daarvan is enorm.

Gelukkig hebben we ons daar al adequaat op voorbereid. Zo keurde de Vlaamse Regering in 2019 het Vlaams Beleidsplan Cybersecurity goed. Eind 2020 werden via een overheidsopdracht negen dienstverleners voor het aanbieden van cybersecurity-verbetertrajecten aangeduid. Via het Agentschap Innoveren en Ondernemen (VLAIO) kan de helft van de kostprijs daarvan gerecupereerd worden.

Wat is de algemene stand van zaken van het Vlaams Beleidsplan Cybersecurity? Welke maatregelen en initiatieven werden reeds uitgerold?

Er is een specifiek luik met betrekking tot de implementatie voor het bedrijfsleven. Hoeveel bedrijven werden inmiddels door deze maatregelen en verbetertrajecten bereikt?

Het goedgekeurde beleidsplan voorzag ook in een pijler waardoor er jaarlijks zou worden gerapporteerd aan het Hermes beslissingscomité. Dat zou dan een advies formuleren over de stand van zaken van de implementatie en een soort mini-audit over het beleidsplan bieden. Hoe verloopt dit vandaag? Hoeveel adviezen werden er reeds gegeven? Wat is de algemene inschatting van het Hermes beslissingscomité over de uitvoering en impact van het beleidsplan?

Er werd ook een stuurgroep opgericht voor de opvolging van de uitvoering van het beleidsplan. Hoe evalueert de stuurgroep onze initiatieven tot op heden? Kunnen wij daar zaken uit leren om onze bedrijven en onze kritische infrastructuur nog beter te beschermen, en dan zeker in de huidige context?

De voorzitter: De heer Gryffroy heeft het woord.

Andries Gryffroy (N-VA): Ik voel mij natuurlijk aangesproken door collega Vande Reyde. Ik was ten eerste niet als toerist in New York. Ten tweede: als iemand mij op deze manier iets nadrukkelijk vraagt, ga ik daar meestal niet op in. Dat is mijn slecht karakter dat dan bovenkomt.

De digitalisering helpt onze ondernemingen om processen en procedures te vereenvoudigen. Het is een uitdaging om de risico's goed in te schatten en voorbereidingen te treffen om toepassingen, software en applicaties te beschermen. Cyberaanvallen kunnen de ICT-systemen lamleggen en daarmee heel wat schade berokkenen. Maar

liefst een op de acht ondernemingen zou in 2021 te maken hebben gehad met een cyberaanval. Dat blijkt uit een nulmeting die de minister liet uitvoeren om het probleem in kaart te brengen. Een analyse toont aan dat een ruime meerderheid, namelijk 94,2 procent – en dat is heel veel –, van de Vlaamse ondernemingen wel maatregelen neemt, maar deze beperken zich vaak tot het hoogstnodige. De vraag is of dit in de toekomst voldoende zal zijn.

Tal van cyberaanvallen kunnen worden vermeden door oplettender te zijn. Daarvoor is er nog heel wat werk aan de winkel. Het is evident dat men 's avond de deuren en hekken op de parking sluit. Waarom sluit men dan ook de digitale poorten niet grondig af? Opvallend is dat het vooral de kleine ondernemingen zijn die het kwetsbaarst zijn. Doorgaans heeft men niet dezelfde mogelijkheden om zich te beschermen tegen cyberaanvallen.

U voorziet jaarlijks een budget voor cybersecurity. Dat moet bijdragen om het bewustzijn en de basiskennis rond cybersecurity bij onze ondernemers en kmo's te versterken. Om de kmo's beter te ondersteunen, maakt u de cybersecurity-verbetertrajecten van VLAIO beter toegankelijk en de kmo-portefeuille aantrekkelijker.

Op welke manier zult u de cybersecurity-verbetertrajecten toegankelijker en de kmo-portefeuille aantrekkelijker maken voor kmo's? Hoe zullen de kmo's worden gemotiveerd om effectief gebruik te maken van deze instrumenten?

Hoe kunnen de kmo's die minder met ICT-toepassingen werken beter worden gesensibiliseerd? Ik ben er immers van overtuigd dat heel wat laagdrempelige en eenvoudige initiatieven het verschil kunnen maken.

Welke bijkomende knelpunten en lessen leert u uit de barometer of de zogenaamde nulmeting om cybersecurity aan te pakken? Zijn er ook bijkomende inzichten om deze aan te pakken?

De voorzitter: Minister Crevits heeft het woord.

Minister Hilde Crevits: Dank voor de vele vragen. Ik begrijp de heer Vande Reyde, maar ik denk dat de heer Gryffroy misschien nog iets in zijn achterzak heeft zitten. Wie weet?

Ik zal proberen om systematisch op jullie vragen te antwoorden. Het thema cyberveiligheid is al sinds enkele jaren een prioriteit voor Vlaanderen. Concreet werd de beleidsagenda eind 2019 opgestart.

We sluiten hiermee aan bij de ambitie van de Europese cybersecuritystrategie om de cyberweerbaarheid van publieke en private sectoren in een digitaal en geconnecteerd Europa te versterken. De Vlaamse beleidsagenda bestaat uit een onderzoeksluik, een implementatieluik en ten slotte een flankerend luik met specifieke aandacht voor opleidingen. Het onderzoeksluik onder leiding van de KU Leuven is volop in uitvoering en heeft al tweemaal een positieve evaluatie van de onafhankelijke internationale adviesraad mogen ontvangen. Binnen het flankerend luik werden de voorbije jaren eveneens verschillende initiatieven ondersteund om het opleidingsaanbod inzake cyberveiligheid te versterken.

De vraagstelling vandaag gaat vooral over het implementatieluik. De centrale doelstelling ervan is dat de Vlaamse bedrijven hun maturiteit inzake cybersecurity verhogen en gebruikmaken van innovatieve technologieën. Ter ondersteuning hiervan voorzie ik via het beleidsplan jaarlijks 9 miljoen euro voor het implementatieluik onder leiding van VLAIO. We richten hierbij de acties niet enkel op de innovatieleiders of de digitale voorlopers maar we willen een zo breed mogelijke groep van Vlaamse bedrijven bereiken met acties in het beleidsplan. Dit is dan ook de reden waarom er sterk wordt ingezet op sensibiliseren en het bijbrengen van basiskennis

rond cyberveiligheid. Hiervoor doen we een beroep op de structurele partners binnen het VLAIO-netwerk en op de onderzoeksorganisaties. Deze actoren hebben samen sinds 2019 meer dan vijfduizend ondernemingen bereikt.

Het gaat hierbij om een brede mix van acties. Er is bijvoorbeeld de zeer laagdrempelige sensibilisering 'Wees hackers te slim af' of 'Het belang van cybersecurity voor kmo's' door respectievelijk de Unie voor Zelfstandige Ondernemers (UNIZO) en het Vlaams netwerk van ondernemingen (Voka). Er is eerstelijnsadvies/toeleiding, er zijn masterclasses 'Cyberveilig in 30 stappen', er zijn hackingdemo's enzovoort. Naast de structurele partners uit het contract ondernemerschap worden ook de hogescholen betrokken. Hierbij aansluitend zijn er ook activiteiten van kennisverspreiding via collectieve projecten inzake nieuwe technologische ontwikkelingen op vlak van cybersecurity.

Het is opvallend dat nog veel Vlaamse bedrijven overtuigd moeten worden van de noodzaak om te investeren in hun cyberveiligheid. Om dit te ondersteunen heeft VLAIO in november 2021 sterk ingezet op een bijkomende communicatiecampagne met ondernemers die getuigen waarom zij investeren in cyberveiligheid. De focus ligt op cyberveiligheid als verkoopstroef voor ondernemingen. Deze getuigenissen zijn aanvullend op de vele verhalen en voorbeelden die de voorbije jaren door VLAIO werden verspreid in het kader van de website Digitale toekomst. Via deze website en de VLAIO-website werden sinds de start van de beleidsagenda al 65.000 gebruikers bereikt rond het thema cyberveiligheid. Een specifieke reeks voor bedrijven op Kanaal Z is in voorbereiding.

Ik kom tot de lightversie. We lanceerden in 2020 via een overheidsopdracht de cybersecurity-verbetertrajecten waarbij een selectie van private dienstverleners ondernemingen op een diepgaande wijze moeten ondersteunen in hun cybersecurityaanpak. Dit aanbod en de prijzen werden voor een periode van vier jaar vastgelegd na onderhandelingen met de dienstverleners. Van deze dienstverleners en de intermediaire actoren kregen we evenwel het signaal dat er bij de kmo's nog grote terughoudendheid is om te investeren in cyberveiligheid.

In het najaar van 2021 is beslist om de financiële drempel van de steunmaatregelen te verlagen met als doel om ook ondernemingen te overtuigen die nog van start moeten gaan met investeringen in cyberveiligheid. Meer concreet werd het steunpercentage voor cyberveiligheid binnen de kmo-portefeuille opgetrokken met 15 procentpunt en anderzijds is ook het instapbedrag van de cybersecurity-verbetertrajecten verlaagd tot projecten van 15.000 euro, waarvan 45 procent wordt gesubsidieerd. Op die manier zijn beide instrumenten qua projectomvang complementair en is de financiële tussenkomst gelijkwaardig. De ondersteuningsmogelijkheden worden breed kenbaar gemaakt via zowel de reguliere communicatiekanalen van VLAIO als de communicatiecampagne waar ik naar verwees. Er zijn ook 92 cybersecurityprojecten gesteund via de kmo-portefeuille en er zijn 66 trajecten opgestart. Er zijn ook 8 lighttrajecten.

In oktober 2020 is cybersecurity uitgebreid behandeld binnen het beslissingscomité. De focus ligt vanuit de bevoegdheid op de toekenning van innovatiesteun binnen de beleidsagenda via ICON-projecten (Interdisciplinair Coöperatief Onderzoek). Het beslissingscomité onderstreepte het belang van een goede samenwerking tussen de actoren op het veld en de noodzaak om cybersecurity hoog op de agenda te houden en vroeg de aanbodzijde goed te betrekken. Ook dit jaar werden er nieuwe ICON-projecten geëvalueerd door het beslissingscomité, maar er vond geen ruimere reflectie plaats.

Ik kom tot de stuurgroep en de knelpunten. De algemene opvolging van de beleidsagenda gebeurt inderdaad door een stuurgroep die samengesteld is door onze Vlaamse Regering. Het voorzitterschap zit bij Stijn Bijnens. Die kennen jullie van

de onderneming Cegeka. Deze stuurgroep komt vier maal per jaar bijeen. In de stuurgroep zijn naast de kennisinstellingen ook de bedrijven en de ondernemersorganisaties vertegenwoordigd, en ook dezelfde organisaties die mee instaan voor de sensibilisering en het eerstelijnsadvies.

De stuurgroep stelt met betrekking tot het implementatieluik vast dat alle actoren die betrokken zijn bij de Vlaamse beleidsagenda gezorgd hebben voor een nieuwe dynamiek rond het thema cyberveiligheid. Men vindt dat er stappen vooruit werden gezet. De ervaring leert echter dat het tijd vraagt om ondernemingen en zeker kmo's tot concrete acties aan te zetten. Daarom is het voor de stuurgroep ook belangrijk om de activiteiten inzake sensibilisering en activering in de toekomst verder te zetten en waar nodig nog verder te intensifiëren. De volgende vergadering heeft plaats op 1 maart en dan staat de bespreking van de cybersecuritybarometer op de agenda.

Uit de barometer valt te leren dat naast een gebrek aan bewustzijn over cyberveiligheid, een gebrek aan kennis en expertise het meest opmerkelijk is. Naast het breed sensibiliseren, geven we daarom ook de nodige aandacht aan het bijbrengen van basiskennis bij ondernemers en hun werknemers en het ondersteunen van het inkopen van extern advies rond het zeer complexe onderwerp dat cyberveiligheid is.

Een andere opvallende vaststelling is dat bij vele ondernemingen de maatregelen inzake cyberveiligheid zich beperken tot enkele technologische standaardingrepen zoals het eenmalig installeren van een firewall of antivirussoftware. In de praktijk volstaat dit echter niet en kan dit zelfs leiden tot een vals gevoel van veiligheid. Een goede cybersecuritymaturiteit omvat naast een technologische component ook altijd een governancecomponent.

Ditzelfde geldt ook voor een cyberverzekering, waar volgens de barometer 22,5 procent van de ondernemingen over beschikt. Als je bedrijf beschikt over een dergelijke verzekering, betekent dat niet dat je voortaan alle deuren en ramen zomaar kunt laten openstaan voor hackers en geen verdere actie moet ondernemen.

Om een lang verhaal kort te maken: het verhogen van die maturiteit bij onze kmo's is een werk van lange adem dat de nodige mentaliteitsveranderingen zal vragen. We hebben binnen het beleidsplan een sterke coalitie van topdeskundigen en organisaties die dicht bij de bedrijven staan. Doorbraken realiseren voor meer cyberveiligheid is een moeilijke maar gezamenlijke opdracht voor overheid, kennisinstellingen en ondernemersorganisaties zoals UNIZO en Voka. Ik voel binnen de stuurgroep een groot engagement om hier daadkrachtig mee door te gaan.

De voorzitter: De heer De Roo heeft het woord.

Stijn De Roo (CD&V): Minister, dank u wel voor uw antwoord. Ik ondersteun het laatste wat u zei. Die maturiteit bij onze bedrijven moet omhoog. Er zijn al veel acties rond ondernomen maar het zal nog tijd kosten vooraleer iedereen zal beseffen wat dat betekent binnen zijn onderneming en dat het niet opgelost is met een programma te installeren. Ik hoop dat die kennis nog verder blijft doordringen.

De basiskennis rond veiligheid bijbrengen is zeer belangrijk binnen ondernemingen. Als het gaat over het alarm aanschakelen of de deur openen, dan krijgt iedereen daar bij wijze van spreken op zijn eerste werkdag een opleiding voor of zijn ondernemers goed uitgerust en opgeleid door externe firma's die dat komen installeren. Maar wanneer het gaat over de digitale veiligheid in het bedrijf, dan zien we dat dat veel minder en nog veel te weinig gebeurt.

Ik wil nog eens inpikken op wat ik in mijn vraag suggereerde. Ik vind het zeer goed dat de steunplafonds worden opgetrokken. Zo werk je een aantal drempels weg voor de ondernemingen om in te tekenen op een aanbod rond cybersecurity en om

daarmee bezig te zijn. Ik zou u willen vragen om zeker in het oog te houden dat het aanbod niet gewoon diezelfde prijsstijging volgt waardoor de kosten die een ondernemer daarin moet steken uiteindelijk even hoog blijven, en dat de subsidie die van de overheid wordt voorzien, de ondersteuning, blijft plakken bij de bedrijven die al bezig zijn met het aanbieden van dergelijke technologieën. Ik hoop vooral dat het ervoor kan zorgen dat ook een aantal nieuwe bedrijven opstarten en dat we binnen Europa nog wat meer concurrentie hebben en wat meer ondernemingen die bezig zijn met cybersecurity.

Voorzitter, ik heb geen bijkomende vragen maar ik ondersteun het traject dat de minister daaromtrent opzet.

De voorzitter: De heer Vande Reyde heeft het woord.

Maurits Vande Reyde (Open Vld): Ik beaam wat collega De Roo net heeft gezegd. Minister, wat ik vooral goed vind in uw antwoord is dat u voor een heel brede aanpak gaat waarvan u de verschillende facetten hebt toegelicht, en dat u vooral kijkt naar zowel grotere als kleinere ondernemingen.

Als we kijken naar de statistieken zien we dat ongeveer de helft van de Vlaamse ondernemingen die minstens tien werknemers hebben, ten minste al een plan of enkele maatregelen hebben rond cybersecurity. Bij kleinere ondernemingen, tot tien werknemers, is dat slechts 15 procent. Er is dus inderdaad een gap tussen grotere en iets minder grote ondernemingen. Het is goed dat ons beleidsplan er echt op inzet om breed te gaan en zoveel mogelijk ondernemingen te bereiken.

Ik heb nog een heel kleine bijkomende vraag. Ik heb dat al eens geopperd in een eerdere gedachtewisseling. Kan er eventueel worden gekeken naar steun voor ondernemingen die, buiten de negen dienstverleners om, iets willen doen aan cybersecurity? Waarom? Niet omdat die negen per se een niet-adequate dienstverlening zouden doen of dat daar iets aan zou mankeren, maar vooral omdat het een domein is dat heel snel evolueert, omdat het vaak een niche is, gericht op een bepaalde sector. Zo zal er bijvoorbeeld specifieke knowhow nodig zijn voor de beveiliging van de medische sector. U hebt toen gezegd dat u ervoor openstond om de aanpak op dat vlak te evalueren en te bekijken hoe er naast de negen dienstverleners eventueel steun zou kunnen worden gegeven als ondernemingen daarvan willen gebruikmaken. Kijkt u daar nog naar? Staat u ervoor open om daar eventueel breder te gaan? Hartelijk dank.

De voorzitter: De heer Gryffroy heeft het woord.

Andries Gryffroy (N-VA): We moeten vaststellen dat er altijd een spanningsveld zal zijn tussen enerzijds onze nieuwe technologische ontwikkelingen en anderzijds het beveiligen van deze technologische ontwikkelingen. De vraag zal altijd blijven hoe we onze veiligheid kunnen garanderen, maar tegelijk ook kunnen verzekeren dat we de dynamiek voor verdere ontwikkelingen en innovatie niet ondermijnen, bijvoorbeeld op het terrein van de artificiële intelligentie.

Wat we wel moeten vaststellen, is dat heel vaak een gewone simpele menselijke fout de oorzaak is van een aantal veiligheidsproblemen en een cyberaanval. Dat gaat soms heel simpel over een mailtje dat men verkeerd heeft aangeklikt of een te gemakkelijk paswoord. Heel recent nog werden er via sms berichtjes gestuurd dat je itsme moest updaten en als je dat deed, kwam je in de problemen. Het wordt zodanig georganiseerd dat het iedereen kan overkomen. Dat kan dan zware gevolgen hebben voor de onderneming. Het is dan ook van het grootste belang om te proberen al je medewerkers te sensibiliseren en alert te maken voor deze problematiek.

Ik heb een bijkomende vraag. In welke mate zouden we kunnen samenwerken met allerlei sectorfederaties, beroepsorganisaties, de Voka's, de UNIZO's enzovoort,

om de heel simpele voorbeelden die we zelf dagelijks tegenkomen, te delen? Als ik een verdachte mail krijg, stuur ik die door naar mijn IT-medewerkers. En zij zeggen dan dat ik daarvan moet afblijven. Misschien heeft niet iedereen die reflex. Maar misschien kan het gebeuren met een algemene communicatiecampagne in hun nieuwsbrieven, hun tijdschriften enzovoort: "Opgelet! Als je zoiets krijgt, blijf eraf!" Kunnen we zoiets opzetten, zeer laagdrempelig, om de zeer laagdrempelige menselijke fouten zoveel mogelijk te kunnen inperken?

De voorzitter: Minister Crevits heeft het woord.

Minister Hilde Crevits: Collega's, ik dank jullie voor alle nuttige aanvullingen.

Collega De Roo, in onze acties gaan we sowieso uit van integrale benaderingen. Dat betekent: technologie, management en mensen. De prijs voor het pakket diensten is vastgelegd in een overheidsopdracht. Dat is een goede manier om de prijsstijgingen mogelijk te beheersen.

Collega Vande Reyde, onze trajecten en kmo-portefeuille zijn net gericht op kmo's. Er is geen steun voor grote ondernemingen. Dat wil ik toch onderstrepen. Naast de trajecten via de negen dienstverleners hebben we het kanaal van de kmo-portefeuille. Dienstverleners kunnen binnen een contract gespecialiseerde ondernemers inzetten. Dat wordt ook aangemoedigd. Er is daarvoor meer dan voldoende budget in de overheidsopdracht.

We verhoogden ook de steun voor cybersecurity in de kmo-portefeuille, collega Vande Reyde. Dat is niet onbelangrijk. Het steunpercentage is opgetrokken tot 45 procent voor kleine ondernemingen, en 35 procent voor middelgrote. Ook hier zie je dat we prioriteit geven aan de kleine ondernemingen.

Collega Gryffroy: cybersecurity is een combinatie van technologie, management, betrokkenheid, motivatie en kennis bij alle medewerkers. Dat is ook het uitgangspunt in ons beleid. Via de ESF-oproepen (Europees Sociaal Fonds) doen we ook heel specifiek opleidingen, en in de communicatie richten we ons vooral naar bedrijfsleiders. Zij moeten het kader scheppen, het beleid voeren en investeren.

De voorzitter: Hebben de vraagstellers nog slotbedenkingen? *(Neen)*

De vragen om uitleg zijn afgehandeld.

VRAAG OM UITLEG van Andries Gryffroy aan Hilde Crevits, viceminister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw, over het stimuleren van Vlaamse bedrijven om batterijen milieuvriendelijker te maken – 1905 (2021-2022)

Voorzitter: de heer Robrecht Bothuyne

De voorzitter: De heer Gryffroy heeft het woord.

Andries Gryffroy (N-VA): Als eerste initiatief in het nieuwe actieplan voor circulaire economie in 2020, stelde de Europese Commissie voor om de Europese wetgeving inzake batterijen te moderniseren. Batterijen die in de Europese Unie (EU) in handel worden gebracht, moeten gedurende de hele levenscyclus duurzaam, uiterst efficiënt en veilig zijn. Dat is cruciaal om klimaatneutraliteit te bereiken tegen 2050 en noodzakelijk voor de verwezenlijking van de doelstellingen van de Europese Geen Deal. Daarin zit de ambitie om verontreiniging tot nul terug te dringen. Hiervoor is het van cruciaal belang dat batterijen gedurende de hele levenscyclus duurzamer worden.

Nu wil het Europees Parlement batterijen duurzamer maken door hun milieu- en sociale impact af te bouwen. De bevoegde parlementscommissie wil dat batterijen in de toekomst een label dragen dat hun CO_2-voetafdruk weergeeft, een bovengrens krijgen voor die voetafdruk tijdens hun hele levensduur en een ondergrens voor de hoeveelheid kobalt, lood, lithium en nikkel die kan worden hergebruikt. De parlementsleden willen ook de verplichting invoeren dat vanaf 2024 de batterijen voor draagbare toestellen zoals smartphones makkelijk verwijderd en vervangen moeten kunnen worden. Als het van hen afhangt moet 80 procent van de draagbare batterijen tegen 2030 ingezameld worden. Hiermee gaan ze zelfs verder dan de Europese Commissie.

Een label invoeren met CO_2-voetafdruk, boven- en ondergrens, en maken dat batterijen makkelijk verwijderd kunnen worden uit draagbare toestellen, gebeurt uiteraard niet zomaar. Daarom heb ik de volgende vragen voor u, minister.

Wat vindt u van het voorstel van het Europees Parlement? Welke rol kan Vlaanderen opnemen om batterijen duurzamer te maken? Op welke manier kan een label daartoe bijdragen?

Hoe kunnen we ondernemingen nog meer aansporen om het gebruik van batterijen duurzamer te maken? Welke instrumenten gaat u daarvoor inzetten?

De voorzitter: Minister Crevits heeft het woord.

Minister Hilde Crevits: Dank u wel, collega Gryffroy. Het voorstel van het Europees Parlement om nog sterker in te zetten op duurzame batterijen is zeker interessant. Ik moet u er niet van overtuigen dat de transitie naar een circulaire economie belangrijk is, en dat past ook in de Europese Green Deal.

We gaan een stijgende vraag krijgen naar batterijen, en dus ook naar de grondstoffen ervan, zoals zeldzame metalen. Naast het feit dat we de hoge milieu-impact van de aanvoer van dergelijke metalen moeten vermijden, is het ook van cruciaal economisch belang dat we de toevoer van die grondstoffen verzekeren. Dat kunnen we doen met de circulaire economie.

De Europese Commissie heeft in mei 2018 het strategisch actieplan voor batterijen vastgelegd. Dat heeft als doel een waardeketen voor batterijen op te bouwen, vanaf de winning, de levering en verwerking van grondstoffen en materialen, tot de productie van batterijcellen, het hergebruik en de recyclage. Hiervoor moeten we het industrieel leiderschap versterken door innovatie te ondersteunen, door in te zetten op opleiding, en door duidelijke regelgevende kaders te verzekeren.

Specifiek betreffende uw vraag over het voorstel van het label is het zo dat productnormering een federale materie is en dus federaal opgevolgd wordt. Maar onze administratie is samen met Vlaanderen Circulair in gesprek met de federale partners om dat mee te volgen, want als dit een manier is om de recyclage van batterijen te versnellen, kunnen we dat ook met Vlaanderen ondersteunen.

Zoals u weet, zet ik ook volop in op innovatie voor de transitie naar een circulaire economie. We hebben Vlaanderen Circulair versterkt en er zijn heel wat relancemiddelen naar innovatie in de circulaire economie gegaan, waaronder 15 miljoen euro naar circulaire maakindustrie met focus op textiel en elektronica.

Eind 2019 nam Vlaanderen ook al deel aan het Europese Important Project of Common European Interest (IPCEI) Batterijen, met deelname via Umicore. Umicore richt zich binnen dit kader op de ontwikkeling van materialen, zowel anodematerialen als kathodematerialen, maar ook op recyclage van materialen uit oude batterijen. Dat laatste punt draagt rechtstreeks bij tot de duurzaamheid. Het luik recyclage omvat

ongeveer 80 procent van het projectbudget en bevat ook investeringen in een eerste industriële ontwikkeling.

Binnen mijn bevoegdheid zet ik ook in op onderzoek en ontwikkeling, bijvoorbeeld via ecologische investeringssteun voor recyclageprojecten. Eind vorig jaar bijvoorbeeld hadden we het STRES-dossier (strategische ecologiesteun) van Metallo in Beerse voor de recyclage tot zuivere materialen. De speerpuntcluster Strategisch Initiatief Materialen (SIM), die de groei van innovatieve spelers uit de Vlaamse materiaalsector ondersteunt, is vorig jaar ook een belangrijk strategisch basisonderzoek gestart met als doel de levensduur van de volgende generatie batterijen te optimaliseren.

We zullen ook de komende jaren onze innovatiemiddelen blijven inzetten op dit soort recylage- en circulaire projecten. Met de grotere nadruk die ik aan het leggen ben op de klimaatimpact van innovatiesteun, wil ik bedrijven extra doen nadenken over hoe ze in een ruimer opgezet innovatieproject aandacht kunnen geven aan zaken als hergebruik en circulariteit. Ook voor projecten om het gebruik en de levensduur van batterijen te verbeteren via onder andere batterijmanagementsystemen, kan ons onderzoek- en innovatie-instrumentarium gebruikt worden. Ook ons Vlaams Strategisch Onderzoekscentrum (SOC) Flanders Make is op dit vlak actief via een aantal Europese projecten. En uiteraard weet u dat ook de samenwerking met de Openbare Vlaamse Afvalstoffenmaatschappij (OVAM) in dit verband zeer belangrijk is.

De voorzitter: De heer Gryffroy heeft het woord.

Andries Gryffroy (N-VA): Juist, het is een federale bevoegdheid, maar het zit zo dicht verweven met Vlaanderen Circulair dat we dat natuurlijk niet los van elkaar kunnen zien.

Wat de circulaire economie, het circulair denken betreft: ik denk dat we het er allemaal over eens zijn dat de ondernemingen die het minst geleden hebben tijdens de coronacrisis, ook de ondernemingen waren die op circulariteit zijn gaan werken, en zich minder afhankelijk maken van grondstoffen vanuit het buitenland.

Ik vind het een zeer goed initiatief van het Europees Parlement. Maar voor een keer ben ik wel voor een verstrenging, omdat we een shift krijgen van de fossiele grondstoffen die we nodig hebben naar andere mineralen, zoals kobalt, lood, lithium en nikkel. En als we niet opletten, rijden we ons op dat vlak straks ook in de problemen. Over dat tekort aan grondstoffen hebben we het al gehad, toen het over chips ging. Dat is wel een belangrijke factor, denk ik.

Als men dat zou willen invoeren vanaf 2024, dan gaat dat naar de lidstaten. De lidstaten moeten dat dan ook vertalen. Dat is een federale bevoegdheid, want het gaat over productnormering. Maar daar zal ook het circulair denken in betrokken worden. 2024 is binnen twee jaar. Zullen we daar op tijd klaar mee zijn?

De voorzitter: Minister Crevits heeft het woord.

Minister Hilde Crevits: Het klopt uiteraard dat de circulaire transitie een Vlaamse prioriteit is, maar we hebben natuurlijk wel een afstemming nodig met het federale niveau rond productnormering. Het is een duidelijke ambitie om via overleg met de federale collega's ook op tijd klaar te raken.

De voorzitter: De ambities zijn duidelijk.

De heer Gryffroy heeft het woord.

Andries Gryffroy (N-VA): Ja, de ambities zijn duidelijk. En ze zijn genoteerd. Bedankt.

De voorzitter: De vraag om uitleg is afgehandeld.