Commissie voor Economie, Consumentenbescherming en Digitalisering

van

WOENSDAG 23 OKTOBER 2024

Namiddag

_____

Commission de l'Économie, de la Protection des consommateurs et de la Digitalisation

du

MERCREDI 23 OCTOBRE 2024

Après-midi

_____

Le développement des questions commence à 15 h 03. La réunion est présidée par M. Roberto D'Amico.
De behandeling van de vragen vangt aan om 15.03 uur. De vergadering wordt voorgezeten door de heer Roberto D'Amico.

01 Vraag van Dieter Keuten aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "CrowdStrike" (56000155C)
01 Question de Dieter Keuten à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "CrowdStrike" (56000155C)

01.01 **Dieter Keuten** (VB): Mijnheer de staatssecretaris, mijn eerste vraag gaat over de CrowdStrike-aanval. Op 19 juli 2024 veroorzaakte CrowdStrike wereldwijd een massale uitval van Microsoftsoftwaresystemen. Volgens hen was die te wijten aan een gebrekkige software-update. Bijgevolg moesten computers manueel worden hersteld. Dat leidde tot urenlange storingen. Hierbij werd de werking van banken, ziekenhuizen en noodlijnen ontwricht. Verschillende bedrijven kampten dagenlang met de gevolgen van deze panne. Nadien waarschuwde het bedrijf CrowdStrike zijn klanten voor mogelijke phishingaanvallen, waarbij werd gevraagd om malafide bestanden te installeren.

Welke federale diensten werden getroffen door deze panne?

Wat waren de gevolgen hiervan voor onze burgers? Was er nadien sprake van phishingaanvallen ten gevolge van deze uitval?

Op welke wijze zal de beveiliging tegen dergelijke storingen worden opgedreven?

01.02 Staatssecretaris **Mathieu Michel**: Het incident van 19 juli 2024, veroorzaakt door een foutieve update van de CrowdStrikebeveiligingssoftware, zorgde voor een wereldwijde verstoring die verschillende belangrijke sectoren getroffen heeft. In België heeft de FOD Beleid en Ondersteuning (BOSA) mij laten weten dat ze geen kennis heeft van significante gevolgen voor zijn partners, of het nu gaat om overheidsinstellingen of private spelers. Zo werden de diensten van itsme niet getroffen.

Alleen de telefoondiensten van een externe leverancier waren gedurende drie dagen niet beschikbaar, tot 22 juli. De burgers konden echter nog wel op andere manieren contact opnemen met de overheid, met name via e-mail. Het Centrum voor Cybersecurity België (CCB) heeft het incident op de voet opgevolgd. Hoewel er geen meldingen van federale administraties werden ontvangen, werden er wel meldingen van storingen verzameld van verschillende essentiële sectoren, zoals de transportsector, het bankwezen en de gezondheidszorg, maar ook van organisaties zoals de NMBS, bpost, Telenet en de luchthavens van Charleroi en Zaventem.

Op de dag van het incident heeft het CCB om 9 uur ’s morgens een kritische flashmelding verstuurd waarin het CrowdStrike-incident werd uitgelegd en een manier werd voorgesteld om het te omzeilen.

Het incident werd evenwel snel uitgebuit door cybercriminelen om een phishingcampagne te lanceren en malware te verspreiden. Die aanvallen waren erop gericht gebruik te maken van de door de storing ontstane verwarring om zo gevoelige informatie te stelen via frauduleuze e-mails, waarin werd beweerd dat er oplossingen werden geboden voor updateproblemen. Tot op heden hebben onze administraties

evenwel geen indirecte phishingpogingen gemeld.

Op het gebied van preventie neemt de FOD Beleid en Ondersteuning (FOD BOSA) proactieve maatregelen om de impact van dit soort incidenten te beperken. Dat omvat onder andere een strikt versiebeheer, waarbij elke update wordt geanalyseerd en getest voordat die wordt ingezet, en bedrijfscontinuïteitsplannen om een snel herstel te garanderen in geval van een grote storing.

Bovendien zullen federale overheidsdepartementen die niet over een specifiek beveiligingsteam of de nodige diensten beschikken, die kunnen verwerven dankzij het komende SECaaS 2-contract.

Het CCB houdt toezicht op cyberdreigingen door informatie over dreigingen, kwetsbaarheden en aanvallen op de informatie- en communicatiesystemen van de vitale sectoren van België te verzamelen, te analyseren en te verspreiden. Na het CrowdStrike-incident heeft het CCB informatie verzameld en geanalyseerd over getroffen organisaties in België, zowel indirect door het monitoren van OSINT-rapporten (Open Source Intelligence) en berichtgeving in de media als direct door rapporten van organisaties aan het CCB.

Het CCB heeft ook het Cyberfundamentals Framework ontwikkeld om organisaties te helpen hun cyberweerbaarheid te versterken en zich voor te bereiden op toekomstige cyberdreigingen.

Op Europees niveau zullen initiatieven zoals de Cyber Resilience Act (CRA) en de NIS2-richtlijn, die op 18 oktober 2024 in België van kracht is geworden, de cyberveiligheid versterken. Dat regelgevingskader zal minimumbeveiligingseisen opleggen voor digitale producten en diensten, inclusief die welke de publieke en private sector gebruiken.

De NIS2-richtlijn in het bijzonder vereist van alle entiteiten die onder de richtlijn vallen, een strikt beheer van cyberrisico's en een snelle rapportage van incidenten evenals een betere beheersing van de risico's in de toeleveringsketen.

De Belgische initiatieven in combinatie met de aankomende Europese regelgeving moeten helpen om dergelijke incidenten in de toekomst beter te voorkomen en de gevolgen ervan te beperken.

Le **président**: Merci, monsieur le secrétaire d'État.

Avant de donner la parole à M. Keuten, je souhaiterais rappeler quelques règles à propos du temps de parole: deux minutes pour la question, deux minutes pour la réponse et une minute pour la réplique. On peut bien sûr être un peu flexible, merci.

01.03 **Dieter Keuten** (VB): Mijnheer de staatssecretaris, ik ben blij dat uw diensten bezig zijn met preventie en met de analyse van dergelijke software-updates die mogelijk risico's inhouden. Ik wil u nog even wijzen op een lokaal incident dat dinsdag plaatsvond. Er waren betaalproblemen bij de betaalterminals om elektronisch te betalen bij tankstations die gebruikmaken van Wordlinesoftware. Er was een tijdelijke storing veroorzaakt door een software-update. Dit blijkt dus een probleem te zijn dat kan terugkomen.

Het incident is gesloten.
L'incident est clos.

02 Vraag van Dieter Keuten aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "De digitalisering van de overheidsdiensten" (56000156C)
02 Question de Dieter Keuten à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "La numérisation des services publics" (56000156C)

02.01 **Dieter Keuten** (VB): Mijnheer de staatssecretaris, voor de digitale transformatie van de overheidsdiensten wordt, gelukkig maar, een beroep gedaan op externe spelers.

Overheidsopdrachten worden helaas vaak uitgeschreven met een reeds vastgelegde technologiekeuze. Nochtans kunnen jonge innovatieve technologiebedrijven veelal een oplossing op maat ontwikkelen die beter aansluit bij de noden van de overheid. Nu worden zij vaak ontmoedigd om

deel te nemen aan dergelijke tenders. Bovendien diskwalificeren de strenge vereisten vaak de kleinere spelers die ons land rijk is.

Mijnheer de staatssecretaris, kunt u, ten eerste, toelichting geven bij de gevolgde werkwijze voor overheidsopdrachten in het kader van de digitalisering van de overheidsdiensten?

Ten tweede, welk aandeel van de gegunde opdrachten kwam daarbij terecht bij innovatieve spelers uit Vlaanderen, respectievelijk Wallonië en Brussel?

02.02 **Mathieu Michel**, secrétaire d'État: Monsieur le président, je voudrais vous informer que j'ai prévu les réponses les plus complètes possible pour mes collègues députés. Je risque donc de dépasser les deux minutes. Ces quatre dernières années, je ne me suis jamais appliqué cette règle que je ne connaissais pas. Je vais donc essayer de parler vite.

De overheidsinstellingen zijn verplicht om de Belgische en de Europese regelgeving inzake overheidsopdrachten strikt na te leven. Bij de ontwikkeling van elk digitaal project wordt een zorgvuldige analyse uitgevoerd om te bepalen of het gebruik van een oplossing out of the box aangewezen is dan wel of het verkieslijk is software op maat te gebruiken. Standaardapplicaties zijn doorgaans goedkoper, terwijl maatwerkoplossingen beter aansluiten bij de vereisten. Momenteel worden bijvoorbeeld bij het DG Vereenvoudiging & Digitalisering van de FOD BOSA heel wat toepassingen, onder meer de eBox, ontwikkeld.

Om kleine en middelgrote ondernemingen aan te moedigen om in te schrijven op overheidsopdrachten worden contracten opgesplitst in kleinere percelen. Dankzij die aanpak kunnen de financiële en technische vereisten van de aanbestedingen worden aangepast, waardoor de opdrachten toegankelijker worden voor kmo's en de concurrentie wordt versterkt.

Wat innovatieve spelers betreft, worden bij gebrek aan een strikte definitie alle bedrijven die betrokken zijn bij de ontwikkeling van toepassingen als zodanig beschouwd. Innovatie is voor de bedrijven een must, als ze concurrerend willen blijven. Wij zorgen ervoor dat onze aanbestedingen blijven evolueren, zodat nieuwe innovatieve en flexibele actoren hierop zouden kunnen inspelen.

Volgens FEDCOM, het boekhoudsysteem van de FOD's en de POD's, gunden de federale overheidsdiensten in 2023 overheidsopdrachten aan meer dan 120 bedrijven, waarvan 54 % in Brussel, 36 % in Vlaanderen, hoofdzakelijk in Mechelen en Zaventem, en 10 % in Wallonië zijn gevestigd.

02.03 **Dieter Keuten** (VB): Bedankt voor het antwoord en de cijfers. Ik ben blij dat grote opdrachten worden gesplitst, zodat kleinere bedrijven kunnen kandideren.

Ik hoop dat u er aandacht aan blijft schenken om onze eigen ontwikkelaars in Vlaanderen, Brussel of Wallonië kansen te geven en dat u voor hen kiest, ook al gaat het om maatwerk. Dat kan op lange termijn betere oplossingen bieden dan soft- of hardware die elders ontwikkeld is.

Het incident is gesloten.
L'incident est clos.

03 Vraag van Dieter Keuten aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Het nationaal convergentieplan voor de ontwikkeling van artificiële intelligentie" (56000159C)
03 Question de Dieter Keuten à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "Le Plan national de convergence pour le développement de l'intelligence artificielle" (56000159C)

03.01 **Dieter Keuten** (VB): Mijnheer de staatssecretaris, het nationaal convergentieplan voor de ontwikkeling van artificiële intelligentie wil van België een smart AI nation maken. Het plan bevat doelstellingen en actiepunten waarop de federale overheid, samen met haar partners, de komende jaren wil focussen. Om de uitvoering van dat plan te begeleiden, werd een sturingscomité opgericht. Dat comité zou voorstellen formuleren over de werking van AI en optreden als centraal contactpunt voor AI-gerelateerde kwesties.

Mijnheer de staatssecretaris, hoe werden de leden van dat sturingscomité geselecteerd? Is dat comité paritair samengesteld?

Welk overleg heeft het comité reeds gehad met de gewesten en de wetenschappelijke instellingen? Kunt u de bevindingen van het overleg toelichten?

Welke streefdata stelt u voorop om de geformuleerde doelstellingen te verwezenlijken?

03.02 Staatssecretaris **Mathieu Michel**: Mijnheer de voorzitter, ik zal proberen te antwoorden, ook al heeft de heer Keuten aan de twee ingediende vragen een vraag toegevoegd, namelijk over de samenstelling van het comité.

Er werden, in uitvoering van het nationaal convergentieplan van eind 2022 al verschillende concrete acties aangevat, waaronder de oprichting van een federaal ethisch comité, de opmaak van wetgeving rond de transparantie van algoritmen en van een handvest voor het gebruik van AI en de uitwerking van een *ethical assessment tool*.

Wat specifiek het sturingscomité betreft, sinds zijn oprichting eind 2023 heeft dat reeds vier keer vergaderd. Een ontwerp van huishoudelijk reglement werd op de tweede vergadering voorgelegd. De goedkeuring van dat reglement staat op de agenda van de volgende vergadering van het comité begin november.

De vertegenwoordigers van de in het koninklijk besluit opgesomde instellingen hebben aan die vergaderingen deelgenomen. Op de vierde bijeenkomst waren ook enkele experten uitgenodigd om hun expertise te delen over agendapunten rond de AI Act, met name de testomgeving van regelgeving, de zogenaamde *regulatory sandboxes*, de benoeming van de aanmeldende autoriteiten en nazichtautoriteiten en de concrete toepassing van de transparantievereisten bij de ontwikkeling van AI-oplossingen.

Algemeen wordt er regelmatig een stand van zaken gegeven aan het comité over de verschillende acties die in het nationaal convergentieplan zijn opgenomen, bijvoorbeeld wat de doelstellingen betreft om betrouwbare AI te bevorderen of om burgers over AI te informeren. Er wordt ook gewerkt aan de governance van AI, die rekening zal houden met de implementatie van de AI Act, die op 1 augustus 2024 is gepubliceerd.

Ten slotte, geleidelijk aan zullen alle actiepunten van de andere hoofdstukken van het plan worden aangepakt. Een nieuwe stand van zaken is gepland voor 2025.

Wie zullen er zitting in hebben? Dat zijn een vertegenwoordiger van de minister en/of de staatssecretaris die op federaal niveau bevoegd is voor digitalisering, een vertegenwoordiger van de minister van Economie, een vertegenwoordiger van de minister die bevoegd is voor telecommunicatie, een vertegenwoordiger van de FOD BOSA, een vertegenwoordiger van de FOD Economie, twee vertegenwoordigers van de universiteiten, een Nederlandstalige en een Franstalige, twee vertegenwoordigers van de Nationale Arbeidsraad, een Nederlandstalige en een Franstalige, een vertegenwoordiger van de OISZ, een vertegenwoordiger van het BIPT en een vertegenwoordiger van het CCB. Ook de gemeenschappen nemen deel.

03.03 **Dieter Keuten** (VB): Mijnheer de staatssecretaris, ik ben blij te horen dat ook de gemeenschappen vertegenwoordigd zijn in het sturingscomité, dat het comité al viermaal samen is gekomen en dat het een huishoudelijk reglement heeft opgesteld, dat hopelijk zal worden goedgekeurd.

Ik kijk uit naar concrete actiepunten en de tijdslijn voor de uitvoering ervan.

Het incident is gesloten.
L'incident est clos.

04 Vraag van Dieter Keuten aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "De aanval op Belgische overheidswebstekken" (56000436C)
04 Question de Dieter Keuten à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "L'attaque contre des sites internet de pouvoirs publics belges" (56000436C)

04.01 **Dieter Keuten** (VB): Mijnheer de voorzitter, mijn laatste vraag is meteen ook de meest actuele vraag en gaat over de Denial of service-aanvallen.

Begin oktober 2024, meer bepaald vanaf 4 oktober 2024 tot ongeveer 11 oktober 2024 hebben verschillende aanvallen plaatsgevonden op Belgische websites. Ze zijn breed gerapporteerd in de pers. Zelfs de website van dit Huis, de Kamer, de Senaat, het koningshuis en Belga.Press zijn aangevallen. Ook privésites, zoals de sites van de haven van Antwerpen-Brugge, mediaconcerns, provinciale websites en lokale websites van steden en gemeenten zijn platgelegd door die DDoS-aanvallen. Als gevolg daarvan waren heel veel websitepagina's tijdelijk onbruikbaar voor onze burgers. Behalve burgers hebben ook ondernemingen en zelfs wij, politici, daarvan hinder ondervonden.

Het Centrum voor Cybersecurity is nota bene zelf aangevallen. Zijn website was tijdelijk buiten gebruik. Volgens het centrum werden echter geen data of gegevens buitgemaakt en zorgden de aanvallen enkel voor een tijdelijk ongemak.

DDoS-aanvallen zijn echter niks nieuws. Ze komen al bijna tien jaar regelmatig in de actualiteit. Sinds de start van de oorlog in Oekraïne wordt de tactiek zowel door Rusland als door het Oekraïense leger toegepast om elkaars online-infrastructuur aan te vallen. Ze zijn dus niets nieuws.

Ik kom tot mijn concrete vragen, om te peilen naar wat u doet om preventief op te treden.

Ten eerste, bent u van oordeel dat burgers recht hebben op een correcte dienstverlening die altijd beschikbaar is?

Ten tweede, hoe zult u het vertrouwen in de *smart nation* bewerkstelligen, indien dergelijke hacks blijven gebeuren?

Ten derde, hoe komt het dat de beveiliging van Belgische overheidswebsites blijft tekortschieten, hoewel dergelijke aanvallen niets nieuws zijn?

Ten vierde, welke maatregelen hebt u getroffen om de beveiliging van die websites, zoals de website van de Kamer, op te schroeven?

Ten vijfde, kunt u garanderen dat persoonlijke gegevens op die websites nooit zullen worden gecompromitteerd door DDoS-aanvallen?

Ten zesde, kunt u de analyse van de aanvallen op die sites, die zou zijn gebeurd, met ons delen?

Graag hadden wij gehad dat u die analyse met het hele Parlement deelt. Er bestaan namelijk verschillende soorten DDoS-aanvallen, telkens met een specifieke preventie- en verweermethode.

Ten slotte, zijn er privépartners die u bijstaan om onze website of overheidswebsites te verweren tegen dergelijke hackings?

04.02 Staatssecretaris **Mathieu Michel**: Mijnheer het Kamerlid, vooraf is het belangrijk om te benadrukken dat elke instelling of organisatie en elk bedrijf verantwoordelijk zijn voor de beveiliging van zijn digitale installaties. DDoS-aanvallen zijn erop gericht systemen te verzadigen door een enorme stroom verzoeken, zodat ze tijdelijk niet beschikbaar zijn. Het doel is niet om gegevens te stelen maar om de beschikbaarheid van de service te verstoren.

Dit soort aanvallen brengt drie belangrijke uitdagingen met zich mee. Ten eerste, onvoorspelbaarheid. Het is extreem moeilijk om deze aanvallen van tevoren te detecteren en te voorkomen. Ten tweede, de verscheidenheid aan technieken die gebruikt worden om die aanvallen uit te voeren. Het is vaak

ingewikkeld om een onderscheid te maken tussen legitiem verkeer en kwaadwillige verzoeken. Tot slot kunnen de kosten van beschermingsmaatregelen tegen DDoS-aanvallen hoog zijn. Het is dus cruciaal dat deze investeringen in verhouding staan tot de potentiële impact van een onderbreking van de dienst.

Naast de Europese initiatieven die al in een eerdere vraag werden vernoemd, zoals de Cyber Resilience Act en de NIS2-richtlijn die op 18 oktober 2024 in België van kracht is gegaan, en ondanks het feit dat het moeilijk is om DDoS-aanvallen volledig te voorkomen, kunnen er maatregelen worden genomen om de impact te beperken, eens de aanval gestart is. Geen van die maatregelen garandeert echter een volledige beschikbaarheid van de diensten. Het Centrum voor Cybersecurity België (CCB) speelt in deze context een centrale en coördinerende rol door ondersteuning te bieden aan bedrijven, organisaties en overheden. De ondersteuning door het CCB neemt de vorm aan van informatietools en advies om hun cyberbeveiliging te versterken.

Het CCB heeft in samenwerking met Belnet ook een leidraad gepubliceerd om de IT-managers van overheidsdiensten, bedrijven en organisaties te informeren en te ondersteunen om zich te beschermen tegen DDoS-aanvallen.

Het CCB werkt ook aan structurele oplossingen om overheidsinstellingen beter te beschermen via de Active Cyber Protection-aanpak (ACP). Die is erop gericht organisaties proactief zoveel mogelijk geautomatiseerd en gepersonaliseerd te ondersteunen en te versterken, waarbij de nadruk ligt op samenwerking. Een belangrijk onderdeel van die aanpak is het Early Warning System (EWS), dat vitale organisaties zoals de federale diensten voorziet van gerichte en tijdige waarschuwingen over kwetsbaarheden en dreigingen.

Meer in het algemeen heeft het CCB een technische leidraad voor 2024 beschikbaar gesteld, waarin organisaties en overheden worden geadviseerd om een rampenplan voor cyberveiligheid te ontwikkelen, bij te werken en regelmatig te testen. In dat document worden ook aanbevelingen gedaan om de beveiliging te versterken en zich beter voor te bereiden op DDoS-aanvallen.

De recente aanvallen werden aangekondigd en uitgevoerd door een groep pro-Russische activisten die zich richten op Europese en NAVO-gerelateerde doelen. De groep heeft het in het bijzonder gemunt op overheidsinstanties, de media en particuliere bedrijven, met als doel de aandacht van de media te trekken.

Het CCB is momenteel niet in staat om het Parlement een volledige analyse van die aanvallen te geven. Dat komt omdat elk overheidsdepartement verantwoordelijk is voor zijn eigen analyse van de DDoS-aanval op zijn website en het CCB op dit moment nog geen analyserapporten heeft ontvangen. Gezien de complexiteit van de aanvallen kan het nog wel even duren voordat een volledige analyse beschikbaar is.

Ten slotte zijn er ook partnerschappen tussen spelers zoals het CCB, Proximus, Belnet en de FOD BOSA om een gecoördineerde reactie op bedreigingen van onze kritieke infrastructuur te garanderen.

04.03 **Dieter Keuten** (VB): Mijnheer de staatssecretaris, ik begrijp de centrale coördinerende rol van het CCB in dezen en ik kijk uit naar hun rampenplan met betrekking tot cybersecurity. Het wordt natuurlijk wel moeilijk voor het CCB om die coördinerende rol uit te voeren als het zelf wordt aangevallen en succesvol wordt platgelegd. U zei dat er hoge kosten verbonden zijn aan preventieve maatregelen en dat voorkomen zeer moeilijk is, maar in het geval van het CCB, dat hier een centrale positie inneemt, is dat toch aangewezen.

Ik kijk ook uit naar de langetermijnanalyse van deze aanvallen per federaal overheidsdepartement.

Het incident is gesloten.
L'incident est clos.

05 Vraag van Lode Vereeck aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "De afschaffing van de 'Federal Learning Account'" (56000496C)
05 Question de Lode Vereeck à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "La suppression du compte fédéral de formation" (56000496C)

05.01 **Lode Vereeck** (VB): Mijnheer de staatssecretaris, het doel van permanente professionele vorming van werknemers of levenslang leren staat niet ter discussie, het is immers noodzakelijk voor de productiviteit van onze economie en om de groei van onze productiviteit op peil te houden. Macro-economisch is het ook nodig voor het individu, dat zo vaardigheden blijft ontwikkelen en aldus relevant blijft op de arbeidsmarkt.

Mijn vraag gaat niet zozeer over het beleid, maar over de beleidstool waarvoor u hebt gekozen: de Federal Learning Account (FLA). Het betreft een onlinetool waarin de bedrijven alle formele en informele opleidingen moeten registreren, naast de registratie van de op te stellen opleidingsplannen en van de sociale balans. Die onlinetool is heel onduidelijk en omslachtig, en brengt aanzienlijke nieuwe en hogere administratieve lasten met zich mee voor de bedrijven, alsook hogere beheerskosten voor de overheid, geschat op 4,4 miljoen euro.

Ik stel mijn vraag hier mondeling in de commissie en niet schriftelijk, omdat op 30 november de bedrijven al hun opleidingen van dit jaar geregistreerd zullen moeten hebben, van de jobstudent over de flexi-jobber tot het vaste personeel. Uit cijfers van de werkgeversorganisatie UNIZO blijkt dat 99 % van de kmo's dat nog niet heeft gedaan.

In het gelekte onderhandelingsdocument van de arizonaonderhandelaars staat dat men de Federal Learning Account wil afschaffen. Ook collega Ronse heeft blijkbaar een voorstel om de tool af te schaffen. Maar de nieuwe regering is er nog niet en de tijd dringt, want 30 november is vanaf nu nog vijf weken.

Ten eerste, zijn de administratieve lasten van de onlinetool in kaart gebracht of gemeten? In uw plannen werd de tool voorgesteld als een administratieve vereenvoudiging, waarna dat is teruggetrokken. Die administratieve lasten zijn eigenlijk nooit gemeten. Soms gaat het over duizenden of tienduizenden euro per bedrijf. Hebt u daar een macro-economisch zicht op? Werden die lasten ooit door de FOD BOSA berekend? Zo niet, waarom niet?

Ten tweede, bent u van plan om de Federal Learning Account te behouden en vooral te handhaven? 99 % van de kmo's heeft dat niet ingevuld en zal dat ook niet invullen en de volgende regering wil dat afschaffen. Zult u, gelet op die feiten, dat handhaven op 30 november, gesteld dat u dan nog aan het bewind bent? Zo ja, zult u dan toch nog sancties voorzien? Welke sancties gelden voor bedrijven die de deadline niet halen? Zo niet, bent u van plan om een vereenvoudiging of uitstel door te voeren of het misschien zelfs af te schaffen?

05.02 Staatssecretaris **Mathieu Michel**: Mijnheer de voorzitter, mijnheer het Kamerlid, misschien is het u bekend dat daarover wordt gesproken in de commissie voor Sociale Zaken, er was daarvoor immers een tweede lezing gevraagd. Die vergadering is nog bezig, meen ik. U kunt de werkzaamheden van de commissie voor Sociale Zaken volgen.

Wat de administratieve lasten betreft, de administratieve lasten die gepaard gaan met de onlinetool van de Federal Learning Account zijn nog niet gemeten. Door het lage aantal registraties is het momenteel inderdaad moeilijk om een maatstaf vast te stellen voor de administratieve lasten die de FLA voor ondernemers met zich zou meebrengen. Tot op heden is het nog steeds niet mogelijk om een representatieve steekproef te verkrijgen op basis van het huidige aantal registraties. Er wordt aangenomen dat de pool van registraties pas voldoende groot zal worden wanneer de verplichting van kracht wordt. Dat is precies het onderwerp van bespreking in de commissie voor Sociale Zaken.

De inhoud van dat instrument in zijn huidige vorm is, zoals u zegt, een zaak voor de volgende regering.

Tot slot, wat betreft de mogelijke sancties en het toezicht op dat instrument, nodig ik u uit om die vragen aan mijn collega-minister Dermagne te stellen, aangezien hij daarvoor verantwoordelijk is.

05.03 **Lode Vereeck** (VB): Mijnheer de staatssecretaris, dit is een heel verwonderlijk antwoord. U zegt immers eigenlijk dat u bij een wetsontwerp niet in staat bent de administratieve lasten te meten. Dat is natuurlijk wel een essentieel onderdeel van een reguleringsimpactanalyse. Die lasten moeten op voorhand worden gemeten. Het is niet zo dat u eerst een relevante steekproef moet hebben, u moet dat op voorhand kunnen meten. Indien u dat had gedaan, had u misschien ontdekt dat dat geen al te beste zaak is.

Het begin van uw antwoord heb ik niet zo goed gehoord, maar u zegt dat het een zaak is voor de volgende regering. U zegt daarmee eigenlijk dat er volgens u op 30 november een volgende regering is. Op 1 december, wanneer u waarschijnlijk nog in het zadel zult zitten, zult u echter moeten beslissen wat u zult doen.

U verwijst naar de commissie voor Sociale Zaken en spreekt over een tweede lezing. Zal dat werkelijk voor 30 november gebeuren?

05.04 Staatssecretaris **Mathieu Michel**: Om 14.00 uur vergaderde de commissie voor Sociale Zaken en daarin werd er gesproken over de opheffing ervan.

05.05 **Lode Vereeck** (VB): Dat was dus op hetzelfde moment als deze commissie? Dan zal ik daar mijn licht opsteken.

Het incident is gesloten.
L'incident est clos.

Le **président**: Les questions n^{os} 56000564C et 56000565C de M. Nuino sont reportées à sa demande.

De openbare commissievergadering wordt gesloten om 15.38 uur.
La réunion publique de commission est levée à 15 h 38.