CRIV 55 **COM 1017**

DE KAMER BE
LA CHAMBRE BE

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

COMPTE RENDU INTÉGRAL
AVEC
COMPTE RENDU ANALYTIQUE TRADUIT

INTEGRAAL VERSLAG
MET
VERTAALD BEKNOPT VERSLAG

Commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique

Commissie voor Economie, Consumentenbescherming en Digitale Agenda

Mercredi

08-03-2023

Après-midi

Woensdag

08-03-2023

Namiddag

N-VA	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	*Parti Socialiste*
VB	*Vlaams Belang*
MR	*Mouvement Réformateur*
CD&V	*Christen-Democratisch en Vlaams*
PVDA-PTB	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	*Open Vlaamse Liberalen en Democraten*
Vooruit	*Vooruit*
Les Engagés	*Les Engagés*
DéFI	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications :		*Afkortingen bij de nummering van de publicaties* :	
DOC 55 0000/000	*Document parlementaire de la 55e législature, suivi du n° de base et du n° consécutif*	*DOC 55 0000/000*	*Parlementair stuk van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral définitif et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (op beigekleurig papier)*

Publications officielles éditées par la Chambre des représentants
Commandes :
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
e-mail : publications@lachambre.be

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers
Bestellingen :
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

SOMMAIRE

Question de Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "La cybersécurité" (55033396C) 1

Orateurs: **Erik Gilissen, Mathieu Michel**, secrétaire d'État à la Digitalisation, chargé de la Simplification administrative, de la Protection de la vie privée, de la Régie des Bâtiments, adjoint au premier ministre

Questions jointes de 3

- Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "Les perturbations sur les sites internet des pouvoirs publics" (55034393C) 3

- Erik Gilissen à Petra De Sutter (VPM Fonction publique et Entreprises publiques, Télécoms et Poste) sur "Les perturbations sur les sites des pouvoirs publics" (55034394C) 3

Orateurs: **Erik Gilissen, Mathieu Michel**, secrétaire d'État à la Digitalisation, chargé de la Simplification administrative, de la Protection de la vie privée, de la Régie des Bâtiments, adjoint au premier ministre

Questions jointes de 4

- Michael Freilich à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "Blockchain4Belgium" (55034460C) 4

- Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "L'initiative Blockchain4Belgium" (55034484C) 4

Orateurs: **Michael Freilich, Erik Gilissen, Mathieu Michel**, secrétaire d'État à la Digitalisation, chargé de la Simplification administrative, de la Protection de la vie privée, de la Régie des Bâtiments, adjoint au premier ministre

Question de Kathleen Verhelst à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "L'accessibilité des multinationales/géants de l'internet" (55034463C) 7

Orateurs: **Kathleen Verhelst, Mathieu Michel**, secrétaire d'État à la Digitalisation, chargé de la Simplification administrative, de la Protection de la vie privée, de la Régie des Bâtiments, adjoint au premier ministre

INHOUD

Vraag van Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Cybersecurity" (55033396C) 1

Sprekers: **Erik Gilissen, Mathieu Michel**, staatssecretaris voor Digitalisering, belast met Administratieve Vereenvoudiging, Privacy, de Regie der Gebouwen, toegevoegd aan de eerste minister

Samengevoegde vragen van 3

- Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Storingen bij overheidswebsites" (55034393C) 3

- Erik Gilissen aan Petra De Sutter (VEM Ambtenarenzaken en Overheidsbedrijven, Telecommunicatie en Post) over "Storingen bij overheidswebsites" (55034394C) 3

Sprekers: **Erik Gilissen, Mathieu Michel**, staatssecretaris voor Digitalisering, belast met Administratieve Vereenvoudiging, Privacy, de Regie der Gebouwen, toegevoegd aan de eerste minister

Samengevoegde vragen van 4

- Michael Freilich aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Blockchain4Belgium" (55034460C) 4

- Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Het Blockchain4Belgium-initiatief" (55034484C) 4

Sprekers: **Michael Freilich, Erik Gilissen, Mathieu Michel**, staatssecretaris voor Digitalisering, belast met Administratieve Vereenvoudiging, Privacy, de Regie der Gebouwen, toegevoegd aan de eerste minister

Vraag van Kathleen Verhelst aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "De bereikbaarheid van multinationals/internetgiganten" (55034463C) 7

Sprekers: **Kathleen Verhelst, Mathieu Michel**, staatssecretaris voor Digitalisering, belast met Administratieve Vereenvoudiging, Privacy, de Regie der Gebouwen, toegevoegd aan de eerste minister

Commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique

du

MERCREDI 8 MARS 2023

Après-midi

_____

Commissie voor Economie, Consumentenbescherming en Digitale Agenda

van

WOENSDAG 8 MAART 2023

Namiddag

_____

De openbare commissievergadering wordt geopend om 13.39 uur en voorgezeten door de heer Stefaan Van Hecke.
La réunion publique de commission est ouverte à 13 h 39 et présidée par M. Stefaan Van Hecke.

Les textes figurant en italique dans le Compte rendu intégral n'ont pas été prononcés et sont la reproduction exacte des textes déposés par les auteurs.
De teksten die in cursief zijn opgenomen in het Integraal Verslag werden niet uitgesproken en steunen uitsluitend op de tekst die de spreker heeft ingediend.

01 Vraag van Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Cybersecurity" (55033396C)
01 Question de Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "La cybersécurité" (55033396C)

01.01 **Erik Gilissen** (VB): Mijnheer de voorzitter, mijnheer de staatssecretaris, een goede beschermingsstrategie is van essentieel belang voor alle organisaties, zowel voor scholen als voor bedrijven en lokale besturen. Bij een onvoldoende weerbaarheid vormen die immers een gemakkelijke prooi voor ransomwareaanvallen.

De bescherming komt met een aanzienlijk kostenplaatje. Dus wordt de afweging gemaakt tussen de graad van bescherming en het beschikbare budget. Idealiter zijn de IT-systemen na een aanval meteen opnieuw volledig operationeel, maar dat kost handenvol geld.

Daarom opteren veel organisaties voor back-upsystemen, waarbij het herstel veel langer op zich laat wachten. Een dergelijke back-upstrategie moet er ook rekening mee houden dat de downtime van de facturatie bijvoorbeeld niet langer uitvalt dan de cashflow toelaat.

Mijn vragen zijn de volgende.

Hoeveel cyberincidenten werden in 2022 gerapporteerd bij grote ondernemingen, kmo's, scholen en lokale besturen? Hoeveel van die organisaties beschikken over een cyberverzekering? Welke controles zijn er op de degelijkheid van hun databeschermingsstrategieën? In welke mate staat het risico van ransomwareaanvallen de digitale transformatieplannen van organisaties in de weg? Ten slotte, hoeveel organisaties rapporteren moeilijkheden na de heropstart van hun IT-systemen?

01.01 **Erik Gilissen** (VB): Si elles veulent éviter les attaques par rançongiciel, les organisations doivent s'équiper d'un système de protection efficace. Ces systèmes sont toutefois très onéreux. C'est pourquoi de nombreuses organisations optent pour des systèmes de sauvegarde, mais cette stratégie demande beaucoup plus de temps pour se remettre après une attaque.

En 2022, combien a-t-on enregistré de cyberincidents dans des grandes entreprises, des PME, des écoles et des administrations locales? Combien de ces organisations ont-elles souscrit une cyberassurance? Comment la robustesse des systèmes de protection des données est-elle contrôlée? Dans quelle mesure le risque d'attaques par rançongiciel gêne-t-il les plans de transformation numérique des organisations? Combien d'organisations font-elles état de difficultés après le redémarrage de leurs systèmes informatiques?

01.02 Staatssecretaris **Mathieu Michel**: Mijnheer de voorzitter, mijnheer Gilissen, ik dank u voor uw vraag. Na het Centre for Cybersecurity Belgium te hebben geraadpleegd, kan ik u het volgende mededelen.

Inzake het aantal cyberaanvallen heeft in 2022 het federaal Computer Emergency Response Team of het CERT, zijnde de operationele dienst van het CCB, 24 grote cyberaanvallen behandeld waarvoor technische bijstand werd gevraagd. Het ging om drie aanvallen bij lokale besturen, elf aanvallen bij administratieve diensten, vier aanvallen bij ziekenhuizen en zes aanvallen bij diverse industrieën.

Deze gegevens houden geen rekening met meldingen en/of adviezen van het CCB die een cyberaanval tegenhielden of kleinschaliger waren. Er is geen informatie over het aantal organisaties met een cyberverzekering. Audits van gegevensbeschermingsstrategieën zijn momenteel slechts beperkt vereist. In het kader van de NIS-verordening zijn verplichtingen opgelegd die door de sectorale autoriteiten worden gecontroleerd.

Daarnaast is er nu een vrijwillige ISO 27001-certificeringsregeling, waarmee bedrijven de omvang van hun informatiebeveiligingsmaatregelen kunnen aantonen. Het CCB houdt, als bevoegde autoriteit, toezicht op de certificeringsinstanties die deze certificering onder accreditatie aanbieden.

Om verschillende belanghebbenden, zoals bedrijven, overheden en andere organisaties, in staat te stellen hun gegevensbeschermingsstrategieën op evenredige wijze te ontwikkelen, heeft het CCB het cyberfundamentalskader ontwikkeld en openbaar gemaakt. Dit kader moet bedrijven niet alleen in staat stellen hun cyberveiligheid te verbeteren, maar ook om in de toekomst de robuustheid van de beschermingsmaatregelen te controleren en aan te tonen aan klanten en overheden, door middel van een geaccrediteerde nalevingsbeoordeling.

Cyberincidenten, zoals aanvallen met ransomware, hebben al dan niet een directe impact op het vertrouwen van digitale gebruikers. Daarom is het belangrijk om aandacht te besteden aan cyberbeveiliging, om ervoor te zorgen dat het vertrouwen in digitale transformatie niet wordt ondermijnd.

Om de cyberveiligheid te versterken en van België een van de minst kwetsbare landen in Europa te maken, verzamelt het CCB voortdurend informatie over de kwetsbare systemen in ons land. Het doet dat in vier fasen: monitoring van de belangrijkste kwetsbaarheden, de identificatie van de kwetsbare systemen, de identificatie van de eigenaar van het kwetsbare systeem en het waarschuwen en informeren van de eigenaar van het kwetsbare systeem.

Verschillende CCB-projecten verstrekken informatie aan bedrijven over de door aanvallers uitgebuite kwetsbaarheden.

Voor kritieke dienstverleners beheert het CCB een systeem voor vroegtijdige waarschuwing dat verschillende van de bovengenoemde fases automatiseert. Het CCB werkt ook aan een project om verschillende van deze waarschuwingsdiensten vanaf eind dit jaar aan te bieden aan alle organisaties in ons land, via een nieuw portaal, SafeOnWeb @Work.

In antwoord op uw laatste vraag, volgens het CCB had ten minste een derde van de incidenten waarbij het moest ingrijpen een grote of zeer

01.02 **Mathieu Michel**, secrétaire d'État: En 2022, la Cyber Emergency Response Team (CERT) a fourni une assistance technique lors de 24 cyberattaques majeures. Sur ces 24 attaques, 3 ont touché des administrations locales, 11 des services administratifs, 4 des hôpitaux et 6 des industries diverses.

En outre, le Centre pour la Cybersécurité Belgique (CCB) fournit des conseils qui peuvent arrêter ou limiter les cyberattaques.

Je ne dispose d'aucune information sur le nombre d'organisations disposant d'une cyberassurance. Les audits des stratégies de protection des données ne sont exigés que dans une mesure limitée. Le règlement NIS impose des obligations qui sont contrôlées par les autorités sectorielles. La certification volontaire ISO 27001 permet aux entreprises de démontrer l'étendue de leur sécurité informatique. Le CCB supervise les organismes qui proposent cette certification.

Le CCB a élaboré un cadre des éléments principaux pour la cybersécurité, qui aide les organisations à élaborer une stratégie de protection des données. Grâce à une évaluation de conformité accréditée, elles seront également en mesure, à l'avenir, de contrôler et de démontrer à leurs clients la solidité de leurs mesures de protection. L'attention portée à la cybersécurité est nécessaire pour préserver la confiance des utilisateurs dans la transformation numérique.

Le CCB collecte en permanence des informations sur les systèmes vulnérables présents dans notre pays, et ce en assurant un suivi des principales vulnérabilités, en identifiant les systèmes vulnérables, en mettant en garde et en informant leurs propriétaires. Il fournit également des informations aux entreprises sur les fragilités exploitées par les pirates.

Pour les prestataires de services critiques, le CCB gère un système

grote impact op de getroffen organisatie.

d'alerte précoce. À partir de la fin de cette année, le centre veut proposer, par le biais du nouveau portail Safeonweb at work, différents services d'alerte à l'ensemble des organisations actives dans notre pays.

Selon le CCB, un tiers des incidents pour lesquels il a dû intervenir ont eu une grande, voire une très grande incidence sur l'organisation touchée.

01.03 **Erik Gilissen** (VB): Mijnheer de staatssecretaris, dank u voor uw antwoorden.

Dat ransomware en hacking bij onze bedrijven, besturen en ziekenhuizen voor heel wat financieel verlies zorgt door het lekken van gegevens, is voor iedereen wel duidelijk. Het niet operationeel zijn van servers en het stilleggen van hele bedrijven en productieprocessen kost onze bedrijven, besturen en ook onze economie handenvol geld.

U zei dat u geen informatie hebt over hoeveel bedrijven een cyberverzekering hebben. Het lijkt mij in deze tijden toch een goede zaak zo'n verzekering af te sluiten.

Nog al te vaak is er sprake van een slechte beveiliging in bedrijven. Wij hebben al berichten gehoord over te zwakke wachtwoorden. De mazen in het net moeten worden verkleind door de telecomoperatoren, met hulp van het CCB, die de kennis hebben hoe de cyberveiligheid te verbeteren, maar daarnaast moeten wij ook inzetten op sensibilisering.

01.03 **Erik Gilissen** (VB): Aujourd'hui, de trop nombreuses entreprises sont encore mal protégées. Les opérateurs de télécommunications doivent resserrer les mailles du filet, par le biais d'une collaboration avec le CCB, mais aussi en sensibilisant le public.

Het incident is gesloten.
L'incident est clos.

02 Samengevoegde vragen van
- Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Storingen bij overheidswebsites" (55034393C)
- Erik Gilissen aan Petra De Sutter (VEM Ambtenarenzaken en Overheidsbedrijven, Telecommunicatie en Post) over "Storingen bij overheidswebsites" (55034394C)
02 Questions jointes de
- Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "Les perturbations sur les sites internet des pouvoirs publics" (55034393C)
- Erik Gilissen à Petra De Sutter (VPM Fonction publique et Entreprises publiques, Télécoms et Poste) sur "Les perturbations sur les sites des pouvoirs publics" (55034394C)

02.01 **Erik Gilissen** (VB): Mijnheer de staatssecretaris, de e-governmenttoepassingen moeten toelaten om ook buiten de kantooruren administratieve verrichtingen met de overheid te doen. Op 15 februari 2023 waren er problemen met verschillende overheidstoepassingen. Een aantal websites was moeilijk of niet bereikbaar en ook de identificatie via de Federal Authentification Service, dat de toegang tot de beveiligde toepassingen regelt, werkte niet naar behoren. Volgens BOSA werden de problemen veroorzaakt door het slecht functioneren werking van het netwerk.

Kunt u verduidelijken wat er precies aan de hand was? Welke maatregelen zult u nemen om gelijkaardige incidenten te voorkomen?

02.01 **Erik Gilissen** (VB): Les applications d'e-government doivent permettre d'effectuer des opérations administratives avec les autorités même en dehors des heures de bureau. Le 15 février dernier, plusieurs applications ont connu des problèmes.

Que s'est-il passé précisément? Que compte faire le secrétaire d'État pour éviter des incidents similaires?

02.02 Staatssecretaris **Mathieu Michel**: Mijnheer Gilissen, ondanks goed voorbereid onderhoud is er in de infrastructuur van het FOD BOSA-datacenter een manuele fout opgetreden op DNS-niveau, waardoor de interne communicatie van de diensten in het datacenter werd verstoord. Hierdoor waren bepaalde diensten zoals websites en de FAS niet of nauwelijks beschikbaar voor de eindgebruiker.

De FOD BOSA constateerde op 15 februari 2023 tussen 11.15 uur en 12.00 uur een probleem waardoor de diensten niet beschikbaar waren voor de eindgebruikers tussen 12.00 uur en 13.40 uur. Terwijl de configuratie en de interne communicatie werden hersteld, waren de diensten beperkt beschikbaar, wat de gebruikerservaring voor de eindgebruiker beïnvloedde. Tegen 13.40 uur waren alle diensten weer beschikbaar en tegen 15.00 uur was de volledige capaciteit van het datacenter hersteld.

Daar het om een manuele fout ging, zal de procedure worden geoptimaliseerd om dergelijke manuele fouten uit te sluiten. Parallel daarmee worden de scenario's beter afgesteld om in geval van gelijkaardige incidenten de *business continuity* te verbeteren en de robuustheid van de datacenterinfrastructuur te versterken.

02.02 **Mathieu Michel**, secrétaire d'État: Une erreur manuelle est survenue au niveau du DNS dans l'infrastructure du centre de données du SPF BOSA, ce qui a perturbé la communication interne des services et rendu certains services totalement ou quasiment indisponibles pour les utilisateurs finaux. Le 15 février, le SPF BOSA a constaté un problème entre 11 h 15 et 12 h 00, entraînant une indisponibilité des services entre 12 h 00 et 13 h 40. À 13 h 40, tous les services étaient à nouveau disponibles et à 15 h 00, la capacité du centre de données était entièrement rétablie.

La procédure sera encore optimisée afin de pouvoir exclure de telles erreurs manuelles à l'avenir. Les scénarios seront affinés afin d'améliorer la continuité du service lors de tels incidents et de renforcer la solidité de l'infrastructure du centre de données.

02.03 **Erik Gilissen** (VB): Dank u, mijnheer de staatssecretaris. De overheid zet alsmaar meer in op digitalisatie en de burger moet zijn administratieve verrichtingen steeds vaker zelf doen. Administraties zijn ook steeds moelijker bereikbaar via de telefoon of andere traditionele kanalen. Wanneer de digitale diensten van e-government dan niet beschikbaar zijn, zorgt dat voor problemen. Wat gebeurt er als cruciale diensten, om welke reden dan ook, voor langere tijd niet beschikbaar zijn? Ligt dan het hele land plat? Zijn er hier wel noodprotocollen voor?

Ook al hoeft u mij als ICT'er geenszins te overtuigen van de voordelen van digitalisatie, ik ben me bewust van mogelijke gevaren. Ik hoop dat ook u zich daar bewust van bent.

Het incident is gesloten.
L'incident est clos.

02.03 **Erik Gilissen** (VB): Existe-t-il des protocoles d'urgence pour de tels incidents?

03 Samengevoegde vragen van
- Michael Freilich aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Blockchain4Belgium" (55034460C)
- Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "Het Blockchain4Belgium-initiatief" (55034484C)
03 Questions jointes de
- Michael Freilich à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "Blockchain4Belgium" (55034460C)
- Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "L'initiative Blockchain4Belgium" (55034484C)

03.01 **Michael Freilich** (N-VA): Mijnheer de staatssecretaris, ik verwijs naar mijn ingediende vraag.

Mijnheer de staatssecretaris, u wil het debat over de uitdagingen van

03.01 **Michael Freilich** (N-VA): *Avec son initiative Blockchain4Belgium, le secrétaire d'État entend permettre aux acteurs belges de*

Web3, blockchain en digitale activa aanwakkeren. Ze hebben alle drie een enorm potentieel. Hun wereldwijde markt groeit al enkele jaren exponentieel. De prognoses voor de komende jaren zijn positief.

U heeft besloten het Blockchain4Belgium-initiatief te lanceren. Dat moet de verschillende Belgische spelers in staat stellen een reeks bevindingen en aanbevelingen op te stellen voor de regering, met het oog op het opstellen van een plan. Blockchain4Belgium wordt, via de FOD BOSA, een platform voor spelers uit de industrie, academici, het maatschappelijk middenveld en de verschillende betrokken overheden (economie, financiën, justitie, ...).

Meer dan 500 professionals zouden zich reeds hebben aangemeld en steunen het initiatief. Twee belangrijke werkpunten werden geïdentificeerd. Het eerste richt zich op innovatie in de particuliere sector en zal met verschillende werkgroepen aanbevelingen opstellen. De tweede werkt vooral op het gebruik van deze innovatieve technologieën binnen de overheid door verschillende use cases voor te stellen in verschillende domeinen.

Vandaar volgende vragen:

1.Welk budget werd voorzien voor het Blockchain4Belgium-initiatief? Waarvoor moet het allemaal dienen?
2.Welke spelers uit de industrie, de academische wereld, het maatschappelijk middenveld en de verschillende overheden (economie, financiën, justitie, ...) zijn bij het project betrokken? Hoe zullen ze in de praktijk samenwerken?
3.Wordt er vanaf het begin samengewerkt met het CCB en de GBA? Wat is hun rol in het project?
4.Kan u de rol van de FOD BOSA toelichten? Wat is uw rol in het project?
5.Hoeveel werkgroepen zijn er binnen het initiatief? Wat gaan zij specifiek onderzoeken?
6.Wanneer worden de bevindingen en aanbevelingen overgemaakt aan de regering? Wanneer mogen we het plan verwachten?

formuler des observations et des recommandations au gouvernement en vue de l'établissement d'un plan. Blockchain4Belgium sera une plateforme mise à la disposition des acteurs de l'industrie, des universitaires, de la société civile et de toutes les autorités concernées, par le biais du SPF BOSA.

Quel budget est alloué à cette initiative? Quel en est l'objectif? Quels acteurs sont associés à ce projet? Comment vont-ils collaborer en pratique? Une collaboration a-t-elle déjà été mise en place avec le Centre pour la Cybersécurité Belgique (CCB) et l'Autorité de protection des données (APD)? Quel est leur rôle? Quel est le rôle du SPF BOSA? Combien y a-t-il de groupes de travail et quelles seront leurs tâches? Quand le plan sera-t-il prêt?

03.02 **Erik Gilissen** (VB): Mijnheer de staatssecretaris, ik verwijs naar mijn ingediende vraag.

U hebt recent het Blockchain4Belgium-initiatief gelanceerd en aangekondigd dat het de bedoeling is om van België het Zwitserland van de blockchain te maken.

Met dit initiatief kunnen verschillende spelers een reeks aanbevelingen opstellen voor de regering om een bottom-up ecosysteem te creëren met betrekking tot Blockchain, digitale activa en Web3-technologieën.

1.Op welke financiering via de programma's van de Europese Commissie kan u rekenen?
2.Welke bedrijven zijn al betrokken bij dit project?
3.Wat zijn de taken, onderzoeksopdrachten en deliverables van de aangemelde bedrijven?
4.Hoeveel middelen gaat er naar deze bedrijven?
5.Wat is het voorziene tijdspad?
6.Welke waarborgen zijn er t.a.v. digitaal kwetsbaren?

03.02 **Erik Gilissen** (VB): *Le secrétaire d'État a récemment lancé l'initiative Blockchain4Belgium avec l'ambition de faire de la Belgique "la Suisse de la blockchain".*

Quels moyens proviendront-ils de la Commission européenne? Quelles sont les entreprises participant au projet? Quelles sont leurs tâches, leurs missions et quels sont les résultats attendus? Quel montant leur sera-t-il alloué? Quel est le calendrier? Quelles garanties existe-t-il pour les utilisateurs en situation de vulnérabilité numérique?

03.03 Staatssecretaris **Mathieu Michel**: Geachte Kamerleden, Blockchain4Belgium is een open ecosysteem dat vanuit het terrein is ontstaan en dat ik heb gesteund nadat ik de noodzaak zag om het debat

03.03 **Mathieu Michel**, secrétaire d'État: Blockchain4Belgium est un écosystème ouvert. Ses acteurs

in ons land over die kwestie te verduidelijken. De actoren en de coalitie zijn divers, afkomstig uit de privésector, de academische wereld, overheidsdiensten en het maatschappelijk middenveld. Tot heden brengt Blockchain4Belgium meer dan 1.000 mensen samen. Ook met het CCB en de GBA werden al contacten gelegd.

Het initiatief Blockchain4Belgium wordt ondersteund door de FOD BOSA, DG Vereenvoudiging & Digitalisering. De FOD BOSA organiseert, ondersteunt en coördineert de thematische werkgroepen rond de zonet vermelde thema's. Daarnaast worden verschillende evenementen voorbereid om ervaringen uit te wisselen en te delen. Momenteel werkt één voltijds equivalent daaraan. Dat faciliteert het werk van de thematische groepen om aanbevelingen voor de overheid te formuleren over de uitdagingen van Web3, blockchain en digitale activa.

Er zijn verschillende Europese projectoproepen die een alternatieve financiering bieden. Het platform beoordeelt de mogelijkheid om daaraan deel te nemen en verspreidt informatie onder de belanghebbenden, bijvoorbeeld in het kader van het Digital Europe Programme 2023-2024, een programma uitgaand van EBSI, het Digital Decade Policy Programme en het Next Generation Internet initiative. De verschillende thema's van Blockchain4Belgium zijn te vinden op de website www.blockchain4belgium.eu. De leden nemen deel op vrijwillige basis.

Er zijn acht themagroepen gedefinieerd die in de komende maanden hun aanbevelingen zullen indienen. De thema's die aan bod zullen komen, zijn België en zijn financiering aantrekkelijk maken, internationale referentie, de oprichting van het blockchainecosysteem aanmoedigen, de blockchaintechnologie demystificeren, dus begrijpen, opleiden en communiceren, de evolutie van de juridische aspecten, het gebruik van blockchain- en Web3-technologieën in onze economie bevorderen, de verduidelijking van het fiscaal kader en de overheid, dus de definiëring van *use cases*.

In hun aanbevelingen zullen de groepen aandacht moeten besteden aan de digitale kloof en inclusie, met inbegrip van bewustmaking, opleiding en onderwijs in de thematische werkgroep demystificatie van blockchaintechnologie, dus begrijpen, opleiden en communiceren.

émanent du secteur privé, du monde universitaire, des services publics et de la société civile. Actuellement, Blockchain4Belgium rassemble plus de 1 000 personnes. Des contacts en la matière sont également établis avec le CCB et l'APD. L'initiative est soutenue par le SPF BOSA, en particulier par la DG Simplification et Digitalisation. Le SPF organise, soutient et coordonne les groupes de travail thématiques. En outre, un certain nombre d'événements sont préparés pour un échange d'expériences. À l'heure actuelle, seul un travailleur à temps plein aide les groupes thématiques à formuler des recommandations sur les défis de Web3, de la technologie blockchain et des actifs numériques.

Plusieurs appels à projets européens proposent des financements alternatifs. La plateforme évalue la possibilité d'y participer et diffuse des informations dans le cadre du programme pour une Europe numérique 2023-2024, d'un programme de l'Infrastructure européenne de services de chaîne de blocs (EBSI), du programme politique de la Décennie numérique et de l'Initiative Internet de la prochaine génération. Les thèmes de Blockchain4Belgium sont disponibles sur le site web www.blockchain4belgium.eu. Les membres participent sur une base volontaire.

Huit groupes thématiques soumettront leurs recommandations dans les prochains mois. Les thèmes sont les suivants: le renforcement de l'attractivité de la Belgique et de son financement, la référence internationale, la création de l'écosystème blockchain, la démystification de la technologie blockchain, l'évolution des aspects juridiques, la promotion des technologies blockchain et Web3 au sein de notre économie, ainsi que la clarification du cadre fiscal et les autorités publiques. Dans leurs recommandations, les groupes devront être attentifs à la fracture numérique et à l'inclusion.

03.04 **Michael Freilich** (N-VA): Mijnheer de staatssecretaris, proficiat,

03.04 **Michael Freilich** (N-VA): Il

u hebt nog iets gelanceerd. Aan de krant zei u dat u wenst dat ons land het Zwitserland van de blockchain wordt. Ik ben evenwel teleurgesteld, want u opent een nieuwe praatbarak. Er zullen 500 actoren bij deze zaak worden betrokken. Er zullen aanbevelingen worden geformuleerd in werkgroepen enzovoort. De legislatuur duurt nog iets meer dan een jaar. Dat proces zal nu starten en over een jaar zullen er aanbevelingen zijn, die dan gedistilleerd moeten worden. U weet wel hoe dat gaat. Hoe meer spelers erbij betrokken worden, hoe moeilijker het wordt om tot een consensus te komen. In plaats van zelf te bepalen welke richting we uitgaan en zelf met uw administratie te bekijken wat u in de resterende vijftien maanden kunt realiseren, is dit een tweede *Digital Minds*. Dat was ook een van uw paradepaardjes, maar ik heb daar uiteindelijk niets meer van gehoord, behalve dat enkele groepsleden vertrokken zijn omdat ze vonden dat het de verkeerde kant uitging.

Ik ben dus teleurgesteld want ik had meer verwacht. Het is een initiatief zoals er zoveel zijn, maar ik vrees dat we opnieuw in het niets zullen verzanden. Er zijn 500 participanten voor verschillende werkgroepen en thema's: dat zal niets opleveren.

semble que le secrétaire d'État lance un nouveau lieu de palabres stériles avec 500 acteurs formulant des recommandations, etc. Il serait préférable qu'il définisse lui-même une orientation et examine avec l'administration ce qu'il est encore possible de réaliser durant le reste de la législature. S'agit-il d'un deuxième *Digital Minds*, autre cheval de bataille du secrétaire d'État? Cette initiative me déçoit.

03.05 **Erik Gilissen** (VB): Mijnheer de staatssecretaris, iedereen aan de blockchain, dat lijkt tegenwoordig zowat de leuze. We hebben daarover recent nog een reeks zittingen van het adviescomité voor wetenschappelijke en technologische vraagstukken gehad. In welke mate denkt u dat de gemiddelde Belg zit te wachten op de blockchaintechnologie en de blockchainwallet? Het overgrote deel van de Belgen weet niet eens wat dat is of heeft vaag gehoord dat dit iets met bitcoin te maken heeft. Ik begrijp dat u een early adopter, een voortrekker wil zijn en in deze legislatuur nog iets verwezenlijkt wil hebben, maar welk nut zal dit hebben voor de helft van de bevolking die digitaal kwetsbaar is? De digitale kloof in de maatschappij lijkt steeds groter te worden. Ik denk dat we in de eerste plaats daarop moeten focussen.

03.05 **Erik Gilissen** (VB): Dans quelle mesure le Belge moyen attend-il avec impatience la technologie de la blockchain? Quelle sera l'utilité de cette technologie pour la partie de la population en situation de vulnérabilité numérique? Ne devrions-nous pas nous concentrer d'abord sur la suppression de la fracture numérique?

Het incident is gesloten.
L'incident est clos.

04 Vraag van Kathleen Verhelst aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen) over "De bereikbaarheid van multinationals/internetgiganten" (55034463C)
04 Question de Kathleen Verhelst à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments) sur "L'accessibilité des multinationales/géants de l'internet" (55034463C)

04.01 **Kathleen Verhelst** (Open Vld): Mijnheer de staatssecretaris, wij zijn vandaag meer dan ooit geconnecteerd en netwerken breiden zich uit, zowel voor consumenten als voor b2b. De risico's op misbruik zijn echter ook legio.

Gelet op de misbruiken is een fysiek of minstens een telefonisch aanspreekpunt van internetgiganten als Microsoft, Amazon, Facebook en Instagram voor mij heel belangrijk, maar dat blijkt eigenlijk onbestaande. Ik ken ondernemers van wie de Instagramaccount na hacking permanent geblokkeerd werd, waardoor zij hun hele klantenbestand verloren zagen gaan. Ik ken klanten die het slachtoffer zijn van malafide verkopers, via bijvoorbeeld Amazon, maar bij Amazon kan niemand worden bereikt. Ik ken ook een groot bedrijf waarvan het paswoord van zijn Microsoftaccount en van zijn leverancier van zijn ICT-materiaal werd gehackt. Hij had daar zelf geen enkel uitstaans mee, maar hij kreeg wel een factuur van 360.000 euro van Microsoft voor een week hacking. Nochtans kan de onderneming daar niets aan doen

04.01 **Kathleen Verhelst** (Open Vld): La connectivité et les réseaux sociaux sont d'une importance considérable, tant pour les entreprises que pour les particuliers. Malheureusement, ceux-ci sont également souvent victimes de piratage, ce qui peut parfois avoir de très graves conséquences. Les géants de l'internet, comme Microsoft, Amazon, Facebook et Instagram, aident encore trop peu leurs clients à cet égard. Ils sont très puissants, mais ils ne prennent guère leurs responsabilités en cas de problèmes.

en besefte zij de hacking zelfs niet. Er zijn dus echt grote en angstaanjagende cases.

Het begint bij de klantvriendelijkheid en bereikbaarheid van de betrokken internetgiganten, zodat problemen vlugger worden geïdentificeerd, oplossingen kunnen worden aangereikt, herhaling van dergelijk misbruik wordt vermeden en misschien zelfs eerste stappen kunnen worden gezet in de richting van vervolging van fraudeurs. Marktmacht komt ook met verantwoordelijkheid.

Ontvangt uw administratie op eender welke wijze klachten over de gebrekkige bereikbaarheid van internetgiganten? Zo ja, hoeveel waren er dat jaarlijks sinds 2020? Is een trend vast te stellen?

Wat is het wettelijk kader voor de bereikbaarheid en de verantwoordelijkheden van internetgiganten, als de gebruiker het slachtoffer wordt van illegale activiteiten? Bestaan er sancties voor de internetbedrijven die duidelijk onvoldoende inspanningen leveren?

Le ministre reçoit-il des plaintes sur les difficultés à se mettre en contact avec les géants de l'internet? Existe-t-il un cadre légal en matière d'accessibilité et de responsabilités des géants de l'internet lorsque l'utilisateur est victime d'activités illégales? Peuvent-ils être sanctionnés s'ils consentent des efforts insuffisants en la matière?

04.02 Staatssecretaris **Mathieu Michel**: Eerst en vooral beschik ik niet over concrete cijfers over de meldingen inzake een gebrekkige toegankelijkheid van de internetgiganten. Trouwens, meldingen kunnen ons zeer verspreid bereiken, hetzij via een beleidscel, hetzij via meerdere administraties of nog via regulatoren zoals het BIPT.

De internetgiganten moeten, net als alle platformen, de wettelijke verplichtingen inzake elektronische handel en consumentenrechten naleven. Die verplichtingen vloeien voort uit de Europese richtlijn betreffende consumentenrechten, die werd omgezet in Belgisch recht, de Europese richtlijn die platformen verplicht de aard van de persoon met wie de consument de overeenkomst sluit, mee te delen, en de Europese richtlijn inzake elektronische handel die een algemene informatieverplichting bevat voor bedrijven die op het internet actief zijn. De bepalingen zijn omgezet in Belgisch recht en gaan gepaard met strafrechtelijke sancties.

Ook op Europees niveau zijn verschillende andere initiatieven genomen om zowel bedrijven als eindgebruikers in de zogenaamde platformeconomieën te beschermen. Allereerst werd op 20 juni 2019 een platform-to-businessverordening aangenomen. Die zal bepaalde schadelijke praktijken reguleren of zelfs verbieden. Platforms moeten ook zorgen voor een gemakkelijk toegankelijk klachtenbehandelingssysteem. Overtredingen van die verordening worden bestraft.

Daarnaast is er de Digital Services Act, die in oktober 2022 is aangenomen. Die biedt belangrijke middelen om bepaalde frauduleuze praktijken beter te bestrijden. Zo zal elke tussenpersoon verplicht zijn een enkel contactpunt aan te wijzen voor de afnemer van diensten, zullen marktplaatsen een zekere traceerbaarheid van professionele verkopers die op hun platform actief zijn, moeten vaststellen en zullen controles worden uitgevoerd op producten die als illegaal worden beschouwd.

Die tussenpersonen zullen ook de gebruiker die vermoedelijk een dergelijk illegaal product heeft gekocht, moeten informeren, met name over de identiteit van de verkoper en de mogelijke rechtsmiddelen.

Bij niet-naleving van de verplichtingen volgen er sancties, eventueel van financiële aard, die kunnen oplopen tot 6 % van de totale omzet van de betrokken tussenpersoon.

04.02 **Mathieu Michel**, secrétaire d'État: Je ne dispose pas de chiffres exacts concernant le nombre de signalements à ce propos. Les géants du web sont tenus de respecter les règles en matière de commerce électronique et de droits des consommateurs figurant dans plusieurs directives européennes. À l'échelon européen, plusieurs initiatives ont été prises pour protéger les entreprises et les utilisateurs des économies de plateformes. Les plateformes doivent mettre en place un système de gestion des plaintes accessible. Les infractions sont sanctionnées. Le règlement sur les services numériques (Digital Services Act) d'octobre 2022 aide à lutter contre les pratiques frauduleuses. Tout intermédiaire sera tenu de désigner un point de contact unique pour l'utilisateur des services, et les marchés devront être en mesure de tracer les vendeurs professionnels et d'effectuer des contrôles sur les produits vendus. Les sanctions pourront atteindre 6 % du chiffre d'affaire total.

Er zijn dus tal van juridische instrumenten voorhanden, die het mogelijk moeten maken om een betere toegankelijkheid te garanderen en de verantwoordelijkheid van de grote internetplatformen te versterken.

04.03 **Kathleen Verhelst** (Open Vld): Ik dank u voor uw antwoord. Ik had de vraag eveneens voorgelegd aan de staatssecretaris van Begroting en de minister van Economie.

Het is alvast duidelijk dat er veel middelen voorhanden zijn om het probleem te verhelpen.

Ik zou nog de volgende suggestie willen meegeven. De internetgiganten zijn niet massaal aanwezig in België. Het zou ons alvast een stap dichter brengen, mocht de overheid al eens bij de top 10 van hen in België nagaan of zij wel degelijk een telefoonnummer vermelden op hun website. Men maakt vaak geen gebruik van de rechtsmiddelen, omdat men zich de moeite ontziet een rechtszaak tegen die giganten in te spannen.

Ik roep de overheid op om minstens voor de top 5 of de top 10 ervan te controleren of ze de verplichting om bereikbaar zijn wel naleven.

04.03 **Kathleen Verhelst** (Open Vld): Il existe manifestement de nombreux outils permettant de gérer ce problème. Les pouvoirs publics vérifient-ils si les géants de l'internet dans notre pays mentionnent un numéro de téléphone sur leur site et respectent toutes les règles? Les consommateurs ne se donnent, en effet, souvent pas la peine d'intenter une action en justice contre ces multinationales.

Het incident is gesloten.
L'incident est clos.

De **voorzitter**: Aangezien de heer D'Amico afwezig is zonder verontschuldiging, vervalt zijn vraag nr. 55034771C.

De behandeling van de vragen en interpellaties eindigt om 14.03 uur.
Le développement des questions et interpellations se termine à 14 h 03.