DOC 55 **2401/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

21 décembre 2021

PROPOSITION DE LOI

modifiant la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en vue de soumettre les fournisseurs de services essentiels du service public qui dépendent des réseaux et des systèmes d'information à certaines exigences en matière de sécurité et de notification

(déposée par M. Michael Freilich et consorts)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

21 december 2021

WETSVOORSTEL

tot wijziging van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, teneinde de aanbieders van essentiële diensten in de publieke sector die afhankelijk zijn van netwerk- en informatiesystemen te onderwerpen aan bepaalde eisen inzake beveiliging en meldingen

(ingediend door de heer Michael Freilich c.s.)

RÉSUMÉ

Dans de nombreux secteurs, les fournisseurs de services essentiels qui dépendent des réseaux et des systèmes d'information sont déjà soumis à plusieurs exigences en matière de sécurité et de notification. Pour le secteur public, ce n'est pas encore le cas, à moins que les fournisseurs puissent être considérés comme faisant partie d'un autre (sous-)secteur. Pourtant le secteur public est de plus en plus souvent touché par des cyberattaques et des cyberincidents et l'infrastructure informatique des services publics belges joue un rôle essentiel dans le bon fonctionnement du pays.

Cette proposition de loi vise par conséquent à intégrer le secteur public dans le champ d'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

SAMENVATTING

In veel sectoren zijn de aanbieders van essentiële diensten die afhankelijk zijn van netwerk- en informatiesystemen reeds onderworpen aan bepaalde eisen inzake beveiliging en meldingen. Voor de publieke sector is dat nog niet het geval, tenzij de aanbieders tot een andere (deel)sector kunnen worden gerekend. Nochtans wordt de overheidssector in toenemende mate getroffen door ernstige cyberaanvallen en -incidenten en is de ICT-infrastructuur van de Belgische overheidsdiensten essentieel voor de goede werking van het land.

Dit wetsvoorstel strekt er daarom toe om de overheidssector onder te brengen binnen het toepassingsgebied van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

06037

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*
cdH	:	*centre démocrate Humaniste*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de numering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document 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 et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het defi nitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénaire*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La directive européenne NIS

La directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union se fonde sur la considération que, dès lors que les réseaux et les services et systèmes d'information jouent un rôle crucial dans la société, leur fiabilité et leur sécurité sont essentielles aux fonctions économiques et sociétales.

L'Union européenne a observé que l'ampleur, la fréquence et les conséquences des incidents de sécurité ne cessaient de croître, ces incidents représentant une menace majeure pour le bon fonctionnement des réseaux et des systèmes d'information. Ces systèmes peuvent aussi devenir des cibles pour des actions intentionnelles malveillantes qui visent la détérioration ou l'interruption de leur fonctionnement. C'est pourquoi la directive NIS a défini plusieurs exigences en matière de sécurité et de notification afin de promouvoir une culture de gestion des risques et de faire en sorte que les incidents les plus graves soient signalés.[1]

Les États membres ont été chargés d'identifier les entités qui remplissent les critères de la définition d'un opérateur de services essentiels. Dans le cadre de ce processus d'identification, les États membres devaient évaluer, au moins pour chaque sous-secteur visé par ladite directive, quels services doivent être considérés comme essentiels au maintien de fonctions sociétales et économiques critiques. En outre, ils devaient démontrer que la fourniture du service essentiel dépend des réseaux et des systèmes d'information. En effet, les opérateurs de services essentiels ne sont soumis aux exigences de sécurité spécifiques que pour autant que les services concernés dépendent des réseaux et des systèmes d'information.[2]

Cette directive n'était applicable qu'aux administrations publiques identifiées comme opérateurs de services essentiels dans les (sous-) secteurs mentionnés dans ladite directive. Il était de la responsabilité des États membres de garantir la sécurité des réseaux et des

1 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, Journal officiel de l'Union européenne, L 194/p. 1 et 2.

2 *Idem*, p. 4.

TOELICHTING

DAMES EN HEREN,

Europese NIS-richtlijn

Aan Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie ("NIS-richtlijn") ligt de overweging ten grondslag dat netwerk- en informatiesystemen en -diensten een cruciale rol spelen in de samenleving. De betrouwbaarheid en beveiliging ervan zijn essentieel voor economische en maatschappelijke activiteiten.

De Europese Unie (EU) zag de omvang, de frequentie en de gevolgen van beveiligingsincidenten toenemen. Die incidenten vormen een grote bedreiging voor de goede werking van netwerk- en informatiesystemen. De systemen kunnen het doelwit worden van opzettelijke schadelijke acties, met de bedoeling de werking ervan te verstoren of te onderbreken. De NIS-richtlijn stelde daarom bepaalde eisen inzake beveiliging en meldingen, van toepassing op aanbieders van essentiële diensten, om een cultuur van risicobeheer te bevorderen en ervoor te zorgen dat de ernstigste incidenten worden gemeld.[1]

De lidstaten kregen de opdracht om te bepalen welke entiteiten aan de criteria van de definitie van "aanbieder van essentiële diensten" voldoen. In dat identificatieproces moeten de lidstaten, ten minste voor elke in de richtlijn vermelde (deel)sector, nagaan welke diensten als essentieel voor de instandhouding van kritieke maatschappelijke en economische activiteiten moeten worden beschouwd. Er moet ook worden aangetoond dat de verlening van de essentiële dienst afhankelijk is van netwerk- en informatiesystemen: aanbieders van essentiële diensten worden immers enkel onderworpen aan de specifieke beveiligingsvereisten als de betreffende diensten afhankelijk zijn van netwerk- en informatiesystemen.[2]

De richtlijn was enkel van toepassing op overheidsdiensten die worden aangemerkt als aanbieders van essentiële diensten binnen de vermelde (deel)sectoren in de richtlijn. Het was de verantwoordelijkheid van de lidstaten om te zorgen voor de beveiliging van

1 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, Publicatieblad van de Europese Unie, L 194/p. 1 en 2.

2 *Ibidem*, p. 4.

systèmes d'information des administrations publiques ne relevant pas du champ d'application de ladite directive.[3] Le législateur belge est donc compétent pour élaborer un cadre légal pour la sécurité des réseaux et des systèmes d'information des administrations publiques ne relevant pas du champ d'application de ladite directive. Tel est l'objet de la présente proposition de loi.

La loi NIS belge

La directive européenne NIS a été transposée dans la législation belge par la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (loi NIS). Cette loi prévoyait l'identification des services essentiels de notre pays, ainsi que des fournisseurs de ces services qui dépendent des réseaux et des systèmes d'information (*Network and Information Security*, NIS). Cette loi devait garantir que ces fournisseurs prendraient des mesures de sécurité suffisantes et disposait également que les fournisseurs de services essentiels devaient notifier aux autorités nationales chargées de la cybersécurité tout incident ayant des répercussions significatives, par exemple toute cyberattaque. En effet, la notification de ces incidents permet de mieux coopérer et d'identifier les menaces. Le champ d'application de la loi NIS se limitait aux fournisseurs de services essentiels dans les secteurs énumérés dans la directive NIS (secteurs de l'énergie, des transports, des finances, des soins de santé, de la distribution d'eau potable, des infrastructures numériques).[4] Nous souhaitons à présent élargir son champ d'application aux fournisseurs de services essentiels du secteur public qui ne relèvent pas de ces secteurs.

Accord de gouvernement

L'accord de gouvernement garantit la poursuite de la mise en œuvre effective de la directive NIS, qui constitue un instrument important pour le renforcement des capacités de défense informatique de nos services essentiels. Il prévoit que le gouvernement entend également élaborer un dispositif légal pour empêcher toute intrusion étrangère malveillante dans nos infrastructures critiques.[5] Dans sa note de politique générale, le Premier ministre a indiqué que la Belgique sera l'un des pays européens les moins vulnérables dans le domaine de la cybersécurité à l'horizon 2024. Pour y parvenir, le gouvernement misera notamment sur la protection

[3] *Ibidem*, p. 7.

[4] CERT, "*Transposition de la directive NIS en droit belge*", accessible sur *https://cert.be/fr/news/transposition-de-la-directive-nis-en-droit-belge*.

[5] Paul Magnette & Alexander De Croo, "*Rapport des formateurs*", Bruxelles, 30 septembre 2020, p. 64.

netwerk- en informatiesystemen van overheidsdiensten die niet binnen de werkingssfeer van deze richtlijn vallen.[3] De Belgische wetgever is dus bevoegd om een wettelijk kader uit te werken voor de beveiliging van netwerk- en informatiesystemen van essentiële overheidsdiensten die buiten de werkingssfeer van de richtlijn vallen. Dat is het opzet van het voorliggend wetsvoorstel.

Belgische NIS-wet

De Europese NIS-richtlijn werd in het Belgische recht omgezet door middel van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid ("NIS-wet"). De wet voorzag in het identificeren van de essentiële diensten in ons land en van de aanbieders ervan die afhankelijk zijn van netwerk- en informatiesystemen ("NIS"). Hij moest verzekeren dat die aanbieders voldoende veiligheidsmaatregelen nemen en bepaalde eveneens dat de aanbieders van essentiële diensten significante incidenten, zoals bijvoorbeeld een cyberaanval, aan de nationale autoriteiten voor cyberveiligheid melden. Het melden van incidenten laat toe om beter samen te werken en dreigingen in kaart te brengen. De NIS-wet beperkte zich tot de aanbieders van essentiële diensten in de sectoren opgesomd in de NIS-richtlijn (energie, vervoer, financiën, gezondheidszorg, drinkwater en digitale infrastructuren).[4] Wij wensen het toepassingsgebied van de NIS-wet uit te breiden tot de aanbieders van essentiële diensten in de publieke sector die niet onder deze sectoren vallen.

Regeerakkoord

In het regeerakkoord verzekert de regering de verdere effectieve implementatie van de NIS-richtlijn, die een belangrijk instrument is om de paraatheid van onze essentiële diensten in de cyberwereld te versterken. De regering wil ook werk maken van een wettelijke regeling om buitenlandse kwaadaardige inmenging in onze kritieke infrastructuren te verhinderen.[5] In zijn beleidsnota stelde de premier dat België tegen 2024 in het cyberdomein één van de minst kwetsbare landen van Europa moet worden. Daartoe zou de regering onder meer inzetten op het beschermen van organisaties van vitaal belang tegen nieuwe cyberdreigingen en het versterken van het

[3] *Ibidem*, p. 7.

[4] CERT, "*De Europese NIS-richtlijn wordt omgezet in Belgische wetgeving*", te raadplegen op *https://cert.be/nl/news/de-europese-nis-richtlijn-wordt-omgezet-belgische-wetgeving*.

[5] Paul Magnette & Alexander De Croo, "*Verslag van de formateurs*", Brussel, 30 september 2020, p. 64.

des opérateurs d'importance vitale contre les nouvelles cybermenaces et le renforcement du Centre pour la Cybersécurité Belgique (CCB), afin de pouvoir réagir aux cyberincidents et cybermenaces.[6]

Stratégie cybersécurité Belgique 2.0 2021-2025

Dans sa stratégie en matière de cybersécurité, le CCB indique que les organisations d'intérêt vital (OIV) pour notre pays doivent bénéficier d'une protection optimale contre les cyberattaques. Les incidents liés à ces organisations peuvent avoir un impact national à grande échelle. Le CCB définit les OIV comme les entités publiques et privées qui fournissent un service essentiel à la population belge, en utilisant les réseaux et les systèmes d'information. Le terme est destiné à évoluer et couvre les secteurs de l'énergie, de la mobilité, des télécommunications, le secteur financier, celui de l'eau potable, de la santé publique, des fournisseurs de services numériques et les autorités publiques.[7]

Le CCB fait observer que les OIV sont confrontées à des cybermenaces de plus en plus fortes et sophistiquées. Étant donné que les cyberattaques contre ces organisations peuvent avoir un impact significatif sur notre société et sur la sécurité nationale, il est crucial de les soutenir dans leur protection de manière adéquate. En tant qu'autorité nationale chargée de la cybersécurité, le CCB reçoit de ses partenaires toutes les informations pertinentes concernant les menaces. Il analyse en permanence les informations reçues et envoie des alertes. Ainsi, les OIV sont informées en permanence des menaces, vulnérabilités ou incidents en matière de cybersécurité pertinents. Pour lutter rapidement contre la cybercriminalité croissante et les menaces à l'encontre des autorités, il convient d'investir dans l'identification rapide des menaces qui pèsent sur notre population, notre économie ou les OIV.[8]

Bien que les organisations fournissant des services essentiels au sein du secteur public entrent dans le champ d'application visé par le concept d'OIV, un cadre clair de cybergouvernance pour ces secteurs doit d'abord être développé.[9] De nombreuses autorités publiques utilisent les services numériques visés par la loi NIS,

Centrum voor Cybersecurity België ("CCB"), om zo te kunnen reageren op de cyberdreiging en -incidenten.[6]

Cybersecurity Strategie België 2.0 2021-2025

In haar cybersecurity-strategie stelt het CCB dat de Organisaties van Vitaal Belang (OVI's) voor ons land optimaal dienen te worden beschermd tegen cyberaanvallen. Incidenten ten aanzien van deze organisaties kunnen een grootschalige, nationale impact hebben. OVI's zijn volgens het CCB de publieke en private entiteiten die een essentiële dienst verlenen ten aanzien van de Belgische bevolking en die daarvoor gebruik maken van netwerk- en informatiesystemen. De term is evolutief bedoeld en omvat de sectoren van energie, mobiliteit, telecom, de financiële sector, drinkbaar water, volksgezondheid, digitale dienstverleners en de overheid.[7]

Het CCB merkt op dat de OVI's worden geconfronteerd met een sterk toenemende en meer geavanceerde cyberdreiging. Het is cruciaal hen op gepaste wijze te ondersteunen in hun bescherming: cyberaanvallen tegen die organisaties kunnen immers een aanzienlijke impact hebben op onze maatschappij en op de nationale veiligheid. Het CCB ontvangt als nationale autoriteit voor cyberveiligheid alle pertinente dreigingsinformatie, analyseert die en stuurt waarschuwingen uit. De OVI's worden op die manier permanent geïnformeerd over relevante cybersecurity-dreigingen, kwetsbaarheden of incidenten. Om cybercriminaliteit en overheidsdreigingen snel te kunnen aanpakken, moet er worden geïnvesteerd in de snelle identificatie van en reactie op bedreigingen met gevaar voor onze bevolking, voor onze economie of voor OVI's.[8]

Hoewel de organisaties die essentiële diensten leveren in de overheidssector binnen de beoogde scope van OVI's vallen, moet eerst een governance-kader op gebied van cyberveiligheid voor die sectoren worden ontwikkeld.[9] Tal van overheden gebruiken de in de NIS-wet bedoelde digitale diensten in het kader van hun opdrachten van

6 Alexander De Croo, "*Note de politique générale*", Chambre des représentants, 4 novembre 2020, DOC 55 1580/005, p. 13.

7 Centre pour la Cybersécurité Belgique, '*Stratégie cybersécurité Belgique 2.0 2021-2025'*, Bruxelles, mai 2021, p. 11.

8 *Ibidem*, p. 26-28.

9 Centre pour la Cybersécurité Belgique, '*Stratégie cybersécurité Belgique 2.0 2021-2025'*, Bruxelles, mai 2021, p.11.

6 Alexander De Croo, "*Algemene beleidsnota*", Kamer van volksvertegenwoordigers, 4 november 2020, DOC 55 1580/005, p. 13.

7 Centrum voor Cybersecurity België, *'Cybersecurity Strategie België 2.0 2021-2025'*, Brussel, mei 2021, p. 11.

8 *Ibidem*, pag. 26-28.

9 Centrum voor Cybersecurity België, *'Cybersecurity Strategie België 2.0 2021-2025'*, Brussel, mei 2021, p. 11.

dans le cadre de leurs missions d'intérêt général.[10] La présente proposition de loi vise à créer ce cadre de gouvernance indispensable.

Élargissement de la loi NIS

Depuis novembre 2019, les opérateurs de services essentiels identifiés ont l'obligation de notifier tous les incidents ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'ils fournissent. En 2020, dix incidents NIS ont été notifiés auprès des autorités compétentes. Ce chiffre est comparable au nombre moyen de notifications similaires au sein d'autres États membres de l'UE. Au cours des six premiers mois de 2021, quatre incidents NIS ont déjà été notifiés.[11]

Pour l'heure, les services publics ne sont pas tenus de signaler les incidents en matière de cybersécurité. Nous estimons que les opérateurs de services essentiels pour notre pays relevant du secteur public devraient être contraints de signaler les incident significatifs au CCB. C'est pourquoi nous entendons étendre au secteur public l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Il va de soi que les entités publiques offrent également des services essentiels au maintien d'activités sociales et/ou économiques critiques dans le cadre de leurs tâches de service public. L'infrastructure informatique des services publics belges joue un rôle essentiel dans le bon fonctionnement du pays.

Dans le cadre des travaux préparatoires de la loi NIS, le CCB avait proposé que le service public soit inclus dans la liste des opérateurs de services essentiels.[12] Au cours de l'audition sur les cyberattaques menées contre les systèmes IT de l'État et des services publics, M. Frédéric Van Leeuw, procureur fédéral, a indiqué que la législation NIS devrait également être appliquée au secteur public.[13] Selon Wim Van Langenhove, Head of

10 "*Projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*", DOC 54 3340/001, p. 4.

11 Chambre des représentants, "*Bulletins des questions et réponses écrites*", 11 août 2021, QRVA 55 061, p. 140.

12 Centre d'Informatique pour la Région Bruxelloise et Bruxelles Prévention & Sécurité, "*Vers un plan régional de cybersécurité. Protéger et servir la population, les entreprises et les administrations dans leurs activités numériques*", septembre 2018, p. 28 (consulté le 22 octobre 2021), voir: *https://cirb.brussels/fr/quoi-de-neuf/publications/cahiers/vers-un-plan-regional-de-cybersecurite-septembre-2018*.

13 Chambre des représentants, *rapport de l'audition sur "Les cyberattaques menées contre les systèmes IT de l'État et des services publics"*, 1er septembre 2021, DOC 55 2169/001, p. 12.

algemeen belang.[10] Door dit wetsvoorstel wensen wij werk te maken van dat noodzakelijke bestuurskader.

Uitbreiding van de NIS-wet

Sinds november 2019 zijn de geïdentificeerde aanbieders van essentiële diensten verplicht om alle incidenten te melden die aanzienlijke gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hen verleende essentiële dienst of diensten afhankelijk zijn. In 2020 werden tien NIS-incidenten gemeld bij de betrokken overheden. Dit cijfer ligt in lijn met het gemiddeld aantal dergelijke meldingen in andere Europese lidstaten. In de eerste zes maanden van 2021 werden reeds vier NIS-incidenten gemeld.[11]

Op dit moment zijn overheidsdiensten niet verplicht om cyberincidenten te melden. Wij zijn van oordeel dat de aanbieders van essentiële diensten voor ons land die tot de publieke sector behoren, zouden moeten worden verplicht om significante incidenten te melden aan het CCB. Daarom willen wij het toepassingsgebied van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, uitbreiden tot de publieke sector. Het ligt voor de hand dat publieke entiteiten ook essentiële diensten verlenen voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten, in het kader van hun taken van openbare dienst. De ICT-infrastructuur van de Belgische overheidsdiensten is essentieel voor de goede werking van het land.

In het kader van de voorbereidende werkzaamheden van de NIS-wet had het CCB voorgesteld om de overheid op te nemen in de lijst van aanbieders van essentiële diensten.[12] De heer Frédéric Van Leeuw, federaal procureur, stelde tijdens de hoorzitting over de cyberaanvallen op het IT-systeem van de Staat en de overheidsdiensten dat de NIS-wetgeving ook op de overheidssector zou moeten worden toegepast.[13] Voor

10 "*Wetsontwerp tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid*", DOC 54 3340/001, p. 4.

11 Kamer van volksvertegenwoordigers, "*Schriftelijke vragen en antwoorden*", 11 augustus 2021, QRVA 55 061, p. 140.

12 Centrum voor Informatica van het Brussels Gewest & Brussel Preventie en Bescherming, "*Naar een gewestelijk cyberveiligheidsplan. Burgers, bedrijven en besturen veilig online*", september 2018, p. 28 (geraadpleegd op 22 oktober 2021), zie: *https://cibg.brussels/nl/nieuws/publicaties/katernen/naar-een-gewestelijk-cyberveiligheidsplan-september-2018*.

13 Kamer van volksvertegenwoordigers, verslag van de hoorzitting over "*De cyberaanvallen op het IT-systeem van de staat en de overheidsdiensten*", 1 september 2021, DOC 55 2169/001, p. 12.

Cybersecurity Advisory auprès d'Orange Cyberdefense, l'absence des services publics de la liste constitue une lacune de la loi NIS. Un expert de l'industrie de l'eau a fait observer que la loi NIS les contraint à partager des données critiques sur leur sécurité avec les autorités et que le secteur se tient à cette obligation. Les experts s'inquiètent des conséquences qu'aurait un piratage du SPF Intérieur. En effet, si certaines informations tombent entre les mauvaises mains, les conséquences peuvent être importantes. Ce SPF partage-t-il des informations sensibles avec une infrastructure qui est moins bien sécurisée que celle de l'industrie de l'eau?[14] Nous sommes d'avis que l'absence des services publics de la liste constitue en effet une lacune de la loi NIS justifiant une modification de la loi en question.

La Belgique doit identifier les services du secteur public qui doivent être considérés comme essentiels au maintien des activités sociales et économiques critiques. Il convient également de démontrer que la fourniture du service essentiel dépend des réseaux et des systèmes d'information. Ces fournisseurs de services essentiels doivent prendre des mesures de sécurité suffisantes et signaler les incidents notables, tels qu'une cyberattaque, aux autorités nationales chargées de la cybersécurité. Nous laissons au Roi le soin de déterminer les services du secteur public qui peuvent être désignés comme étant des fournisseurs de services essentiels qui dépendent à cette fin des réseaux et des systèmes d'information.

Des individus mal intentionnés n'ont besoin que de quelques heures pour mettre hors service une administration sur laquelle comptent des utilisateurs, sans parler des attaques qui visent la stabilité d'un pays. Les cyberattaques peuvent être dangereuses pour la stabilité d'un pays et de son économie. Le cyberespace n'est pas seulement le théâtre d'opération de la part des cybercriminels. Il est également devenu le nouveau terrain d'action des services de renseignement. Les États ont la capacité de provoquer une déstabilisation par le biais de cyberattaques. Les possibilités de propagation des cyberattaques se sont multipliées depuis le développement des réseaux informatiques. Notre dépendance croissante à l'égard du web et des technologies de l'information et de la communication est devenue l'une des principales sources de risques. Le secteur public n'est évidemment pas épargné.

[14] Jens Jonkers, "*Cybersecurity in België: is ons land klaar voor een volgende cyberaanval?*", 7 juin 2021 (consulté le 22 octobre 2021), voir: *https://business.techpulse.be/interview/271168/cybersecurity-belgie-is-ons-land-klaar/*.

Wim Van Langenhove, *Head of* Cyber*security Advisory* bij Orange Cyberdefense, is het ontbreken van overheidsdiensten een hiaat in de huidige NIS-wet. Een expert uit de waterindustrie merkte op dat de NIS-wet hen ertoe verplicht om kritieke data over hun beveiliging te delen met de overheid en dat de sector zich daaraan houdt. Als de FOD Binnenlandse Zaken wordt gehackt, dan baart dat de expert zorgen; als bepaalde informatie in verkeerde handen valt, kan dat immers grote gevolgen hebben. Deelt die FOD gevoelige informatie met een infrastructuur die minder goed beveiligd is dan die van de waterindustrie?[14] Het ontbreken van overheidsdiensten is volgens ons inderdaad een lacune in de huidige NIS-wet, die een wijziging van de aangehaalde wet verantwoord maakt.

België moet nagaan welke diensten van de publieke sector als essentieel voor de instandhouding van kritieke maatschappelijke en economische activiteiten moeten worden beschouwd. Er moet ook worden aangetoond dat de verlening van de essentiële dienst afhankelijk is van netwerk- en informatiesystemen. Deze aanbieders van essentiële diensten moeten voldoende veiligheidsmaatregelen nemen en significante incidenten, zoals bijvoorbeeld een cyberaanval, melden aan de nationale autoriteiten voor cyberveiligheid. De indiener laat het aan de Koning om te bepalen welke diensten van de publieke sector kunnen worden aangewezen als aanbieders van essentiële diensten die daarvoor afhankelijk zijn van netwerk- en informatiesystemen.

Personen met minder goede bedoelingen hebben niet meer dan enkele uren nodig om een administratie waar gebruikers op rekenen buiten dienst te stellen, om nog maar te zwijgen van aanvallen die de stabiliteit van een land zelf viseren. Cyberaanvallen kunnen gevaarlijk zijn voor de stabiliteit van een land en zijn economie. Cyberspace is niet alleen het werkterrein van cybercriminelen; het is evenzeer het nieuwe werkterrein van inlichtingendiensten geworden. Staten hebben het vermogen om door middel van cyberaanvallen destabilisering te provoceren. De mogelijkheden om cyberaanvallen te verspreiden, hebben zich vermenigvuldigd sinds de ontwikkeling van informaticanetwerken. Onze toenemende afhankelijkheid van het internet en informatie- en communicatietechnologie is uitgegroeid tot een van de grootste risicobronnen. De publieke sector blijft uiteraard niet gespaard.

[14] Jens Jonkers, "*Cybersecurity in België: is ons land klaar voor een volgende cyberaanval?*", 7 juni 2021 (geraadpleegd op 22 oktober 2021), zie: *https://business.techpulse.be/interview/271168/cybersecurity-belgie-is-ons-land-klaar/*.

Cyberattaques contre les services publics

Les services publics préfèrent ne pas ébruiter les cyberincidents qui les touchent. De nombreuses cyberattaques contre les autorités publiques ne sont pas rendues publiques, mais l'infrastructure des services publics fédéraux essuie des attaques quotidiennes. Ces attaques sont en outre de plus en plus professionnelles et de plus en plus complexes.

En 2013, nous avons été confrontés à plusieurs révélations embarrassantes concernant des cyberattaques contre les pouvoirs publics. En 2011, des programmes malveillants ont été détectés sur des ordinateurs du SPF Affaires étrangères, puis supprimés avec l'aide de la Défense. Le service de renseignement militaire, le SPF Justice et Belgacom ont également été victimes de cyberattaques.[15]

Trois ans plus tard, il est apparu que le nombre de cyberattaques perpétrées contre les services publics fédéraux était passé de 405 en 2014 à 666 en 2015.[16] Au début de l'année 2017, il s'est à nouveau avéré que l'administration fédérale était de plus en plus ciblée par des cyberattaques. La diplomatie belge en était la principale cible (4 000 attaques par mois, soit près de 130 par jour). Ces attaques ont également visé l'Agence fédérale pour la sécurité de la chaîne alimentaire (6 000 tentatives par an), le Registre national, un site web du Centre de crise, le SPF Économie, l'ONEm, l'ONSS, l'INASTI, le SPF Santé publique et l'armée.[17]

Selon une enquête menée auprès de tous les ministres fédéraux en 2018, les services publics fédéraux sont confrontés à au moins une cyberattaque ciblée chaque semaine. Au SPF Finances, des ordinateurs ont été pris en otage et paralysés et ces attaques ont également visé la Chancellerie, l'Institut géographique national et le Service fédéral des Pensions. Cette enquête a toutefois révélé que seuls quelques services publics avaient spécifiquement chargé du personnel de leur sécurité informatique, et que comme la qualité de la sécurité y dépendait de l'intérêt des personnes qui en étaient chargées, certains services publics étaient beaucoup plus vulnérables que d'autres.[18]

Plus récemment, en mars 2021, nous avons encore été frappés par deux cyberincidents de grande ampleur dans les pouvoirs publics. En juin 2021, une attaque

15 SVL, "*Cyberaanval Buitenlandse Zaken topje van ijsberg*", *De Morgen*, 20 septembre 2013, p. 6.
16 Yves Lambrix, "*Federale overheid paradijs voor hackers*", *Gazet van Antwerpen*, 7 mars 2016, p. 4.
17 Lars Bové, "*Computers overheid steeds vaker onder vuur*", *De Tijd*, 9 février 2017, p. 1.
18 Lars Bové, "*Elke week cyberaanval op federale overheidsdienst*", *De Tijd*, 29 août 2018, p. 6.

Cyberaanvallen op overheidsdiensten

Overheidsdiensten geven liever geen ruchtbaarheid aan de cyberincidenten die zij meemaken. Veel cyberaanvallen tegen de overheid worden niet publiek gemaakt, maar er zijn dagelijks wel aanvalspogingen op infrastructuur van de federale overheidsdiensten. Die aanvallen worden ook professioneler en complexer.

In 2013 werden we geconfronteerd met een aantal pijnlijke onthullingen over cyberaanvallen op de overheid. Op computers van de FOD Buitenlandse Zaken waren in 2011 schadelijke programma's aangetroffen die met de hulp van Defensie waren verwijderd. Andere slachtoffers van cyberaanvallen waren de militaire inlichtingendienst, de FOD Justitie en Belgacom.[15]

Drie jaar later bleek dat het aantal cyberaanvallen op de federale overheidsdiensten was toegenomen van 405 in 2014 naar 666 in 2015.[16] Begin 2017 bleek opnieuw dat de federale overheidsdiensten steeds vaker het doelwit zijn van cyberaanvallen. De Belgische diplomatie was het belangrijkste doelwit (4 000 aanvallen per maand of bijna 130 per dag). Andere slachtoffers waren het Federaal Agentschap voor de Veiligheid van de Voedselketen (6 000 pogingen per jaar), het Rijksregister, een website van het Crisiscentrum, de FOD Economie, de RVA, het RIZIV, de RSZ, De FOD Volksgezondheid en het leger.[17]

Uit een rondvraag bij alle federale ministers in 2018 bleek dat de federale overheidsdiensten minstens elke week met een gerichte cyberaanval te maken krijgen. Bij de FOD Financiën werden computers gegijzeld en lamgelegd; andere slachtoffers waren de Kanselarij, het Nationaal Geografisch Instituut en de Federale Pensioendienst. Toch bleek uit de rondvraag dat maar enkele overheidsdiensten specifieke personeelsleden hadden aangesteld voor informaticabeveiliging. Doordat de kwaliteit van de beveiliging afhankelijk was van de interesse van de personen die er werken, waren bepaalde overheidsdiensten veel kwetsbaarder dan andere.[18]

Meer recent werden we in maart 2021 nog opgeschrikt door twee grote cyberincidenten bij de overheid. Eerst was er de *Distributed Denial of Sevice*-aanval ('DDoS-aanval')

15 SVL, "*Cyberaanval Buitenlandse Zaken topje van ijsberg*", *De Morgen*, 20 september 2013, p. 6.
16 Yves Lambrix, "*Federale overheid paradijs voor hackers*", *Gazet van Antwerpen*, 7 maart 2016, p. 4.
17 Lars Bové, "*Computers overheid steeds vaker onder vuur*", *De Tijd*, 9 februari 2017, p. 1.
18 Lars Bové, "*Elke week cyberaanval op federale overheidsdienst*", *De Tijd*, 29 augustus 2018, p. 6.

Distributed Denial of Sevice (attaque DDoS) visant le réseau Belnet a complètement bloqué différents sites web publics. Il est ensuite apparu que le SPF Intérieur avait été espionné durant deux ans par des pirates informatiques (supposément étrangers).

Le mardi 4 mai 2021, Belnet, le réseau internet des autorités belges, a été victime d'une cyberattaque majeure. Deux cents organisations connectées au réseau Belnet, notamment des universités, des services publics et des instituts de recherche, ont été touchées. Cette attaque a paralysé plusieurs services publics, par exemple le site web des impôts Tax-on-web et la plateforme permettant de réserver un créneau de vaccination. Les fonctionnaires qui télétravaillaient n'ont pas pu se connecter. Les réunions des commissions du Parlement fédéral ont été annulées. La STIB a dû ouvrir les portes d'entrée des stations de métro parce que les distributeurs automatiques de billets ne répondaient pas, et la chaîne publique VRT a également été touchée.

Il s'agissait donc d'une attaque DDoS, au cours de laquelle des cyberattaquants ont délibérément inondé des sites web ou des serveurs de demandes inutiles, saturant ainsi le réseau. Si des attaques DDoS sont fréquentes, l'ampleur de cet incident était toutefois inédite. Il était impossible d'empêcher cet incident à l'aide des moyens actuels. L'objectif des attaquants était en tout cas de paralyser le réseau le plus longtemps possible. Il semble que l'intention était de nuire le plus possible aux pouvoirs publics belges.[19] L'attaque ciblant Belnet a été lancée à partir de 257 000 adresses IP situées dans 29 pays (dont la Tchéquie, le Bahrein, les États-Unis, l'Afrique du Sud et la Russie).[20]

En mars 2021, on a découvert que le SPF Intérieur était devenu la cible d'un piratage informatique de grande envergure, en cours depuis déjà deux ans, à savoir depuis avril 2019. Une très grande expertise s'est avérée nécessaire pour nettoyer complètement et rétablir les serveurs de l'Intérieur. Les auteurs entendaient manifestement pénétrer dans le système du SPF Intérieur et s'y installer durablement. Dans ce cadre, ils ont accédé

[19] Marie Van Oost & Wim De Preter, *"Ongeziene cyberaanval treft België"*, *De Tijd*, 5 mai 2021, p. 1; Peter De Lobel, *"Cyberaanval legt overheid en parlement lam"*, *De Standaard*, 5 mai 2021, p. 5; Werner Rommers, *"Ongeziene cyberaanval legt overheidswebsites urenlang plat"*, *Het Belang van Limburg*, 5 mai 2021, p. 6; Dario Van Fleteren, *"Grote cyberaanval legt websites overheid plat"*, *De Morgen*, 5 mai 2021, p. 3; Kenneth Dée & Bieke Cornillie, *"Van parlement tot belastingen: alles plat door ongezien grote cyberaanval"*, *Het Laatste Nieuws*, 5 mai 2021, p. 2 et Ben Serrure, *"Risico's op zware cyberaanval zijn fout ingeschat"*, *De Tijd*, 6 mai 2021, p. 5.

[20] Yannick Verbreckmoes, *"Aanval op overheid met 257 000 computers"*, *De Morgen*, 6 mai 2021, p. 6 et Guy Stevens, *"Cyberaanval kwam vanuit 29 landen"*, *Het Nieuwsblad*, 6 mai 2021, p. 7.

op Belnet, die verschillende overheidswebsites volledig platlegde. Daarna bleek dat de FOD Binnenlandse Zaken twee jaar lang werd bespioneerd door (vermoedelijk buitenlandse) hackers.

Op dinsdag 4 mei 2021 werd Belnet, het internetnetwerk van de Belgische overheid, het slachtoffer van een grote cyberaanval. Tweehonderd organisaties die op het netwerk van Belnet zijn aangesloten, waaronder universiteiten, overheidsdiensten en onderzoeksinstellingen, werden getroffen. Als gevolg van die aanval reageerden meerdere overheidsdiensten niet, zoals de belastingwebsite Tax-on-web en het platform om een vaccinatieslot te reserveren. Ambtenaren die telewerkten, konden niet inloggen. De commissievergaderingen in het federaal parlement werden geannuleerd, de MIVB moest de toegangspoortjes in de metrostations openzetten omdat de ticketautomaten niet reageerden en ook de openbare omroep VRT ondervond hinder.

Het ging dus om een DDoS-aanval, waarbij cyberaanvallers websites of servers met opzet bestoken met nutteloze aanvragen, waardoor het netwerk verzadigd raakt. DDoS-aanvallen komen vaker voor, maar de omvang van dit incident was ongezien. Met de huidige middelen was dit incident niet te voorkomen. Het was alvast de bedoeling van de aanvallers om het netwerk plat te leggen en dat zo lang mogelijk zo te houden. De intentie leek te zijn dat de Belgische overheid zoveel mogelijk werd geschaad.[19] Via 257 000 IP-adressen uit 29 landen (waaronder Tsjechië, Bahrein, de VS, Zuid-Afrika en Rusland) werd de aanval op Belnet uitgevoerd.[20]

In maart 2021 werd ontdekt dat de FOD Binnenlandse Zaken het doelwit was geworden van een ingrijpende computerhacking, die al twee jaar, vanaf april 2019, aan de gang was. Er was heel wat expertise nodig om de servers van Binnenlandse Zaken volledig schoon te maken en opnieuw in orde te brengen. De daders wilden kennelijk binnendringen in het systeem van de FOD Binnenlandse Zaken en daar lange tijd aanwezig

[19] Marie Van Oost & Wim De Preter, "*Ongeziene cyberaanval treft België*", *De Tijd*, 5 mei 2021, p. 1; Peter De Lobel, *"Cyberaanval legt overheid en parlement lam"*, *De Standaard*, 5 mei 2021, p. 5; Werner Rommers, *"Ongeziene cyberaanval legt overheidswebsites urenlang plat"*, *Het Belang van Limburg*, 5 mei 2021, p. 6; Dario Van Fleteren, *"Grote cyberaanval legt websites overheid plat"*, *De Morgen*, 5 mei 2021, p. 3; Kenneth Dée & Bieke Cornillie, *"Van parlement tot belastingen: alles plat door ongezien grote cyberaanval"*, *Het Laatste Nieuws*, 5 mei 2021, p. 2 en Ben Serrure, *"Risico's op zware cyberaanval zijn fout ingeschat"*, *De Tijd*, 6 mei 2021, p. 5.

[20] Yannick Verbreckmoes, *"Aanval op overheid met 257 000 computers"*, *De Morgen*, 6 mei 2021, p. 6 en Guy Stevens, "*Cyberaanval kwam vanuit 29 landen"*, *Het Nieuwsblad*, 6 mei 2021, p. 7.

à toutes les données internes du SPF Intérieur et ont pu tranquillement espionner le service public qui est au cœur de la gestion et de la sécurisation de notre pays (banques de données des services de police, organisation des élections, gestion de crise et délivrance des cartes d'identité). Cette intrusion informatique a été la première à être traitée comme une crise nationale; d'autres services publics ont également dû prendre des mesures pour se protéger.[21]

La reconstruction des systèmes informatiques après une cyberattaque a un coût. Pour la reconstruction des systèmes informatiques à la suite du cyberincident de 2021, des crédits d'investissement supplémentaires ont été dégagés à titre unique en 2022, à savoir 6,5 millions d'euros.

Les exemples précités illustrent qu'il ne serait pas superflu d'étendre le champ d'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, et en particulier d'intégrer le secteur public dans cette loi.

COMMENTAIRE DES ARTICLES

Article 1er

Cet article fixe le fondement constitutionnel de la proposition de loi.

Art. 2

L'absence des services publics constitue une lacune de l'actuelle loi NIS qui pourrait être comblée en intégrant explicitement le secteur public dans le champ d'application de la loi.

Conformément à l'article 3 de la loi NIS, cette loi s'applique aux opérateurs de services essentiels, tels que définis à l'article 6, 11°, l'opérateur de services essentiels étant défini comme "une entité publique ou privée active en Belgique dans l'un des secteurs repris à l'annexe I de la présente loi, qui répond aux critères

[21] Lars Bové, *"Binnenlandse Zaken twee jaar lang ongemerkt gehackt"*, *De Tijd*, 25 mai 2021 (consulté le 23 octobre 2021), à l'adresse: *https://www.tijd.be/politiek-economie/belgie/federaal/binnenlandse-zaken-twee-jaar-lang-ongemerkt-gehackt/10308489.html*; Luc Beernaert, *"Alles wijst naar China"*, *Het Laatste Nieuws,* 26 mai 2021, p. 5; Stavros Kelepouris, *"Binnenlandse Zaken twee jaar gehackt"*, *De Morgen*, 26 mai 2021, p. 1; Nikolas Vanhecke, *"Cyberaanval: Zijn we twee jaar lang gehackt door China?"*, *Gazet van Antwerpen*, 26 mai 2021, p. 7.

blijven. Zij verkregen daarbij toegang tot alle interne gegevens van de FOD Binnenlandse Zaken en konden ongestoord spioneren bij de overheidsdienst die centraal staat in het bestuur en de beveiliging van ons land (databanken van de politiediensten, organisatie van verkiezingen, crisisbeheer en uitreiking van identiteitskaarten). De inbraak werd voor het eerst behandeld als een nationale crisis; ook andere overheidsdiensten moesten extra maatregelen nemen om zich te beschermen.[21]

Aan de heropbouw van de IT-systemen na een cyberaanval hangt een prijskaartje. Voor de heropbouw van de IT-systemen van de FOD Binnenlandse Zaken na het cyberincident in 2021 werden eenmalig extra investeringskredieten uitgetrokken in 2022, namelijk 6,5 miljoen euro.

De bovenstaande voorbeelden tonen aan dat het geen overbodige luxe is om het toepassingsgebied van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, uit te breiden en meer bepaald de publieke sector te integreren in de wet.

TOELICHTING BIJ DE ARTIKELEN

Artikel 1

Dit artikel bevat de bevoegdheidsgrondslag van het wetsvoorstel.

Art. 2

Het ontbreken van de overheidsdiensten is een hiaat in de huidige NIS-wet. Die lacune kan worden weggewerkt door de sector van de overheid expliciet op te nemen in het toepassingsgebied van de wet.

Overeenkomstig artikel 3 van de NIS-wet is de wet van toepassing op de aanbieders van essentiële diensten, zoals gedefinieerd in artikel 6, 11°. Een aanbieder van essentiële diensten wordt gedefinieerd als "een publieke of private entiteit die actief is in België in een van de sectoren opgenomen in bijlage I bij deze wet, die aan

[21] Lars Bové, *"Binnenlandse Zaken twee jaar lang ongemerkt gehackt"*, *De Tijd*, 25 mei 2021 (geraadpleegd op 23 oktober 2021), zie: *https://www.tijd.be/politiek-economie/belgie/federaal/binnenlandse-zaken-twee-jaar-lang-ongemerkt-gehackt/10308489.html*; Luc Beernaert, *"Alles wijst naar China"*, *Het Laatste Nieuws*, 26 mei 2021, p. 5; Stavros Kelepouris, *"Binnenlandse Zaken twee jaar gehackt"*, *De Morgen*, 26 mei 2021, p. 1; Nikolas Vanhecke, *"Cyberaanval: Zijn we twee jaar lang gehackt door China?"*, *Gazet van Antwerpen*, 26 mei 2021, p. 7.

visés à l'article 12, § 1er, et qui est désignée comme telle par l'autorité sectorielle".

L'article 2 tend à insérer le secteur "Pouvoirs publics" dans l'annexe 1 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, où sont énumérés les types d'opérateurs de services essentiels. L'intégration du secteur "Pouvoirs publics" dans le champ d'application de la loi NIS vise à garantir que les opérateurs de services essentiels œuvrant dans ce secteur prennent suffisamment de mesures de sécurité et qu'ils signalent les incidents significatifs, par exemple toute cyberattaque, aux autorités nationales chargées de la cybersécurité, ce qui renforcera la "cyberpréparation" de ces services essentiels.

Art. 3

L'article 3 charge le Roi d'identifier les services du secteur public qu'il convient de considérer comme essentiels au maintien d'activités sociétales et économiques critiques. À cet égard, il conviendra également de prouver que la fourniture du service essentiel visé dépend des réseaux et des systèmes d'information.

de criteria bedoeld in artikel 12, § 1, voldoet en die als dusdanig is aangewezen door de sectorale overheid".

Artikel 2 beoogt de invoeging van de sector "Overheid" in bijlage 1 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, waarin de soorten aanbieders van essentiële diensten worden opgesomd. De opname van de sector overheid binnen het toepassingsgebied van de NIS-wet moet waarborgen dat de aanbieders van essentiële diensten in die sector voldoende veiligheidsmaatregelen nemen en dat zij significante incidenten, zoals bijvoorbeeld een cyberaanval, melden aan de nationale autoriteiten voor cyberveiligheid. Dat zal de "cyberparaatheid" van deze essentiële diensten versterken.

Art. 3

Artikel 3 bepaalt dat de Koning nagaat welke diensten van de publieke sector als essentieel voor de instandhouding van kritieke maatschappelijke en economische activiteiten moeten worden beschouwd. Er moet daarbij ook worden aangetoond dat de verlening van de essentiële dienst afhankelijk is van netwerk- en informatiesystemen.

Michael FREILICH (N-VA)
Theo FRANCKEN (N-VA)
Koen METSU (N-VA)
Joy DONNÉ (N-VA)
Darya SAFAI (N-VA)

PROPOSITION DE LOI

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

Dans l'annexe 1 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, dans la colonne "Secteur", il est inséré un point 7 intitulé:

"7. Pouvoirs publics"

Art. 3

Le Roi identifie les sous-secteurs et les types d'entités des opérateurs de services essentiels visés à l'article 2.

2 novembre 2021

WETSVOORSTEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

In bijlage 1 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt in de kolom "Sector" een punt 7 ingevoegd, luidende:

"7. Overheid"

Art. 3

De Koning identificeert de deelsectoren en de soorten entiteiten van de aanbieders van essentiële diensten binnen de sector bedoeld in artikel 2.

2 november 2021

Michael FREILICH (N-VA)
Theo FRANCKEN (N-VA)
Koen METSU (N-VA)
Joy DONNÉ (N-VA)
Darya SAFAI (N-VA)

Imprimerie centrale – Centrale drukkerij