Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 925

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 10 oktober 2022

Hierbij bied ik u de Nederlandse Cybersecuritystrategie (NLCS) aan namens het kabinet, vanuit mijn coördinerende verantwoordelijkheid voor cybersecurity. Met mijn brief van 4 juli 2022 heeft u het Cybersecuritybeeld Nederland 2022 (CSBN2022) ontvangen.[1] De NLCS is de reactie van het kabinet hierop en beschrijft de cybersecurityaanpak voor de komende zes jaar.

Tevens bied ik u de kabinetsreactie aan op het rapport «Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix» van de Onderzoeksraad voor Veiligheid (OVV), vanwege de samenhang met de beleidsprioriteiten op het gebied van cybersecurity in de NLCS.

Met de aanbieding van de voorliggende strategie voldoe ik aan mijn toezegging om de investeringen in cybersecurity toe te lichten. Ook zijn de beoogde stelselwijzigingen toegelicht en waar mogelijk schematisch weergegeven.[2] Een stelselwijziging betreft de integratie van het Nationaal Cybersecurity Centrum (NCSC) van het Ministerie van Justitie en Veiligheid (J&V), het Digital Trust Center (DTC) en het Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP), beiden van het Ministerie van Economische Zaken en Klimaat (EZK). U bent hier recentelijk over geïnformeerd per brief van 7 september 2022.[3] Eveneens relevant in relatie tot het efficiënter en effectiever inzetten van schaarse cybersecuritycapaciteit is het bijgevoegde rapport met de werktitel Cyclotron. Dit is het eindrapport van een verkenning naar de mogelijkheden van een publiek-privaat samenwerkingsplatform om sneller en gerichter gezamenlijk informatie te delen rondom (dreigende) cyberincidenten met als doel cyberslachtoffers te voorkomen. Het inzichtelijk

[1] Kamerstuk 26 643, nr. 891

[2] Hiermee geef ik invulling aan mijn toezegging aan het lid Van Ginneken, Kamerstuk 26 643, nr. 849 om de investeringen op cybersecurity verder toe te lichten en uit te werken.

[3] Brief van de d.d. 7 september 2022

kst-26643-925
ISSN 0921 - 7371
's-Gravenhage 2022

maken van de benodigde stappen om te komen tot de realisatie van deze twee stelselwijzigingen, en de uitvoering hiervan, zijn (langlopende) acties van de NLCS.

Tot slot geef ik met de NLCS invulling aan mijn toezegging aan het lid Leijten over de regie van het kabinet op cybersecuritybeleid, de onderliggende investeringen en de verantwoording daarover richting de Kamer.[4] Deze regie zal plaatsvinden via de Raad Defensie, Internationale, Nationale en Economische Veiligheid (RDINEV). Er wordt geen aparte onderraad voor Digitale Zaken ingericht.
Voor een volledig overzicht van toezeggingen aan uw Kamer en hoe deze zijn opgenomen in de NLCS verwijs ik u graag naar de bijlage van deze brief.

Cybersecurity: randvoorwaarde voor digitalisering

Cybersecurity is een essentiële randvoorwaarde voor een veilige en steeds meer digitaliserende maatschappij. Onze toenemende afhankelijkheid van digitale processen, toegenomen dreiging en het toenemende aantal incidenten onderstrepen het belang van een hoog cybersecurityniveau. Daarmee zijn we als Nederland in staat op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en tegelijkertijd onze veiligheid en publieke waarden te beschermen.

In de NLCS staan de ambities van het kabinet op het gebied van cybersecurity voor de komende zes jaar In de visie van het kabinet is digitale veiligheid voor iedereen een vanzelfsprekendheid. De NLCS beschrijft deze stip op de horizon en de keuzes die het kabinet maakt om daar te komen.
Vanuit vrijwel alle beleidsterreinen van het kabinet wordt bijgedragen aan de versterking van de digitale veiligheid zoals omschreven in de NLCS. In nauwe aansluiting op de NLCS wordt in verdiepende strategische agenda's en plannen een nadere uitwerking gepresenteerd van de inzet op hun specifieke beleidsterrein. Naast de NLCS ontvangt uw Kamer dit jaar de Internationale Cybersecuritystrategie (ICS) van de Minister van Buitenlandse Zaken en de Werkagenda Digitalisering van de Staatssecretaris van Koninkrijkrelaties en Digitalisering.

In het bijgevoegde actieplan staan de maatregelen waarmee deze ambities worden gerealiseerd en wie daarvoor verantwoordelijk is.[5] In het actieplan zijn eveneens activiteiten op het gebied van cybersecurity opgenomen die voorvloeien uit het in opdracht van het Ministerie van Economische Zaken en Klimaat, onlangs opgeleverd rapport «Samen veilig: de toekomst van mobiel online». Dit rapport bieden wij u namens de Minister van Economische Zaken en Klimaat aan in de bijlage. Met dit rapport is voldaan aan de toezegging aan het lid Van Dijk om een analyse te maken van de rol van cyberveiligheid bij het gebruik van apps en mobiele toestellen, en risico's en kwetsbaarheden in kaart te brengen.[6] Het rapport toont aan dat de afhankelijkheden en kwetsbaarheden niet louter betrekking hebben op mobiele toestellen en apps maar aan grotere vraagstukken over de digitale wereld raakt waarbij het speelveld door snelle technologische ontwikkelingen voortdurend verandert.

---

[4] Commissiedebat Online veiligheid en cybersecurity, Kamerstuk 26 643, nr. 807

[5] Hiermee geef ik onder andere invulling aan de motie van het lid Van Ginneken over het dichten van bekende kwetsbaarheden door sectorale patchbrigades, Kamerstuk 26 643, nr. 843

[6] Hiermee wordt invulling gegeven aan de motie van het lid Inge van Dijk in het commissiedebat Buitenlandse spionage via mobiele Netwerken van 29 juni jl. om een analyse te maken van de rol van cyberveiligheid bij (het gebruik van) apps en mobiele toestellen, en risico's en kwetsbaarheden in kaart te brengen, Kamerstuk 30 821, nr. 148

Het actieplan 2022–2023 is het startpunt. Het actieplan wordt jaarlijks geactualiseerd, waardoor adequaat ingespeeld kan worden op de snelle ontwikkeling van het cybersecurity domein en bijgestuurd kan worden als hier aanleiding toe is. De komende jaren geeft het kabinet samen met medeoverheden, bedrijfsleven en wetenschap invulling aan de noodzakelijke vervolgstappen richting een digitaal veilig Nederland.

De financiële middelen die het kabinet in het coalitieakkoord aanvullend ter beschikking heeft gesteld dragen bij aan de realisatie van de NLCS. In de financiële bijlage bij de NLCS vindt u een nadere toelichting bij deze investeringen.

U wordt jaarlijks geïnformeerd over de voortgang van de cybersecuritystrategie en ontvangt jaarlijks het Cybersecurity Beeld Nederland.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

BIJLAGE 1

Overzicht verwerking toezeggingen en verzoeken Tweede Kamer in de Nederlandse cybersecuritystrategie

Datum & debat	Partij	Toezegging	Verwerkt in NLCS
Wetgevingsoverleg 26 september 2022 (Kamerstuk 36 084)	D66	De specifieke acties en investeringen zijn opgenomen in de NLCS. Hierin zullen de extra financiële middelen voor het NCSC uiteen worden gezet.	Opgenomen in de financiële appendix.
	Volt	Er zal in de NLCS aandacht worden besteed aan het stimuleren van schakelorganisaties. Ook wordt er gekeken naar het zo klein mogelijk maken van de beslisboom. In de strategie zal ook aandacht worden besteed aan organisaties die momenteel nog niet op een bestaande schakelorganisatie zijn aangesloten.	Opgenomen in Pijler I + actieplan
	SP	We zullen in de strategie aandacht besteden aan het communiceren van de urgentie van betere cybersecurity.	Opgenomen in Pijler IV + actieplan
	SP	De oproep van de SP is om aandacht te besteden aan mogelijke dubbelingen van taken, of dat juist niemand een taak uitvoert omdat er teveel versnippering is en deze taken in een grijs gebied belanden.	Opgenomen in Pijler I, Pijler III + actieplan
	SP	Een verzoek van de SP om de rol van de AIVD en NCTV goed mee te nemen in de strategie.	Opgenomen in Pijler III voor zover dit raakt aan de taken van de Minister van Justitie en Veiligheid. De AIVD en het bijbehorende takenpakket valt onder de verantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijkrelaties.
Commissiedebat 14 september 2022 (Kamerstuk 26 643, nr. 918)	Volt, p. 6	(..) onlineveiligheid en cybersecurity. Naar mijn idee zou je het grofweg in twee categorieën kunnen indelen (..) boze buitenwereld en datazuchtige overheid. Ik hoop, en dat is ook mijn vraag aan de minister, dat er in de cybersecuritystrategie over beide categorieën is nagedacht.	Opgenomen in het visiehoofdstuk voor zover dit raakt aan cybersecurity.
	Volt, p. 6	Toezicht op techbedrijven	Deels opgenomen in deze strategie onder Pijler II. Deels raakt dit aan AVG, algoritmes en digitale autonomie deze onderwerpen komen terug in andere strategieën (bv. Rijksbrede Veiligheidsstrategie)
	D66, p. 8	In de strategie ingaan op jaarverslag plichtige bedrijven ook verplicht kunnen worden om daarin een cybersecurityhoofdstuk op te nemen	Opgenomen in beleidsreactie OVV + actieplan

Datum & debat	Partij	Toezegging	Verwerkt in NLCS
	D66, p8.	Lange termijn risico economische spionage	Niet opgenomen. Komt terug in voortgangsbrief statelijke dreigingen en Rijksbrede Veiligheidsstrategie.
Commissiedebat 7 april 2022 (Kamerstuk 26 643, nr. 849)	MJenV, p. 15	MJ&V zegt toe dat er in de strategie aandacht zal zijn voor stelselvraagstukken.	Opgenomen in visie + Pijler I
	MJenV, p.15	MJenV zegt toe dat er in de strategie aandacht zal zijn voor certificeren.	Opgenomen in Pijler II
	VVD, p. 4	VVD vraagt om in strategie mee te nemen dat: NCSC en DTC (..) dichter naar elkaar toe gaan.	Opgenomen in visie + Pijler I
	VVD, p. 4	De VVD wil graag dat rijksoverheid plannen gaat maken voor een Rijks-ABDO.	Opgenomen in Pijler II + actieplan
	VVD, p. 4	De VVD wil aandacht voor structurele, cross-sectorale oefenagenda voor cyberaanvallen. Grote alsook kleinschalige oefeningen worden meerdere keren per jaar uitgevoerd.	Opgenomen in Pijler I + actieplan
	VVD, p. 4	De VVD vraagt om één algemeen keurmerk, zoals het keurmerk CYRA.	Deels opgenomen in Pijler II. Geen concrete voorstellen voor één keurmerk maar wel duidelijke beleidsinzet in EU context.
	D66, p. 20	Er zal een gedetailleerd overzicht met de NLCS worden meegestuurd over de financiële middelen die voor cybersecurity worden vrijgemaakt.	Opgenomen in Appendix
	MJenV, p. 21	Toezegging om in de NLCS nader in te gaan op wat de internationale samenwerking.	Opgenomen in Pijler I, II en III + actieplan
	CDA, p. 30	De resultaten van het onderzoek / evaluatie naar de Roadmap Digitaal Veilige Hard- en Software worden meegenomen in de NLCS.	Opgenomen in Pijler II
	VVD, p. 31	In de strategie zal er ook wat staan over oefeningen.	Opgenomen in Pijler I
	VVD, p. 34	NIB-2 duurt te lang, cybercriminelen zullen niet wachten. Kunnen we onafhankelijk van de EU nu al stappen zetten.	Opgenomen in Pijler I + actieplan. Maatregelen die bijdragen aan verhogen bredere weerbaarheid.
	Allen, p. 35	Er zal een schematische weergave van de stelselwijzigingen worden weergegeven.	Deels opgenomen in cyclotron rapport. Daarnaast lopen er nog verschillende trajecten waarbinnen keuzes gemaakt zullen worden die invloed zullen hebben op het stelsel. Na het afronden van deze trajecten zal deze toezegging helemaal kunnen worden afgedaan.

Datum & debat	Partij	Toezegging	Verwerkt in NLCS
CD VKC DiZa, 1 december 2021 (Kamerstuk 26 643, nr. 807)	PvdA, p. 41	Kan in de Cybersecurity Agenda een spoor worden opgenomen dat gaat over die werkgelegenheid en dus over opleiden, herscholen, omscholen, zodat we in de breedte voldoende mensen hebben?	Opgenomen in Pijler IV.