[redacted]

9|2|25

Ministerie van Volksgezondheid, Welzijn en Sport

[redacted]

TER BESLISSING

Directie Informatiebeleid - CIO

Opgesteld door

[redacted]

Aan Minister VWS
cc Staatssecretaris LMZ

Deadline: 11-02-2025

nota

BNC fiche Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders

Datum
6 februari 2025

Kenmerk
4060935-1078850-IZ

Bijlage(n)
2

1. Aanleiding

Op 15 januari publiceerde de Europese Commissie een actieplan om cyberbeveiliging van ziekenhuizen en zorgverleners in Europa te verbeteren (zie bijlage 1). Hiervoor dient een Beoordeling Nieuwe Commissievoorstellen (BNC) fiche te worden aangeboden aan de Eerste en Tweede Kamer binnen zes weken na publicatie, met daarin de beoordeling door het kabinet. Het ministerie van Justitie en Veiligheid heeft in nauwe samenwerking met VWS het BNC-fiche opgesteld.

Het BNC-fiche wordt, zoals gebruikelijk, door het ministerie van Buitenlandse Zaken naar de Tweede Kamer gestuurd. Hierbij wordt de beslisnota van VWS meegezonden.

2. Geadviseerd besluit

- Uiterlijk dinsdag 11 februari a.s. akkoord te gaan met de conceptbeoordeling (zie BNC-fiche in bijlage 2) van het Actieplan omtrent cyberbeveiliging van ziekenhuizen en zorgverleners.
- Deze uiterlijke datum is relevant omdat het fiche op 12 februari interdepartementaal wordt besproken (BNC-comité) in aanloop naar besluitvorming in de Ministerraad van 21 februari.

Het fiche wordt aan MVWS voorgelegd gezien de verantwoordelijkheid voor digitalisering in de zorg. Aangezien het actieplan ook zorgaanbieders in de langdurige zorg raakt ontvangt SLMZ een afschrift.

3. Kernpunten

Doel van dit actieplan is het verbeteren van de cyberbeveiliging van ziekenhuizen en zorginstellingen. In het plan ligt de focus op het versterken van de sector capaciteit om cybersecurity-incidenten te voorkomen, informatie-uitwisseling en detectie van cyberdreigingen te versterken, en snellere respons op incidenten en herstel hiervan mogelijk te maken.

Het actieplan bevat hiertoe verschillende voorgestelde maatregelen:

- Het opzetten van een *European Cybersecurity Support Centre for hospitals and healthcare providers* (hierna: "Steuncentrum") binnen het Europese agentschap ENISA om lidstaten te ondersteunen bij uitdagingen op het gebied van cybersecurity in de zorg.

- Het inzetten op preventie met maatregelen zoals cyberbeveiligingsvouchers, administratieve lastenverlichting, een ID-Wallet, paraatheidstesten, risicoanalyses en de oprichting van een Europees *Chief Information Security Officer (CISO)* -netwerk.
- Het verbeteren van detectie door het delen van cyberincidentmeldingen, een EU-breed early-warning systeem en extra steun voor het Europees Zorg ISAC. Voor een snelle respons bij cyberaanvallen wordt een *Rapid Response Service* opgezet binnen de EU Cybersecurity Reserve en komen er draaiboeken voor *ransomware*-aanvallen.

Beoordeling
Over het algemeen zijn de aanbevelingen in lijn met het Nederlandse beleid. Het actieplan sluit aan bij de doelen van het kabinet om de digitale weerbaarheid van de EU te vergroten. Beoordeling van het plan op hoofdlijnen is als volgt:

- Aangezien de zorginstellingen dicht bij de burger staan en geavanceerde cyberaanvallen grote consequenties hebben op patiëntveiligheid en de samenleving, is het van groot belang digitale weerbaarheid van zorginstellingen en ziekenhuizen te vergroten.
- Het actieplan sluit daarnaast aan door de aandacht voor de kleine zorgaanbieders, aangezien deze de zwakste schakels vormen in een keten van verbonden zorgsystemen.
- De inzet op training en bewustwordingsactiviteiten in het actieplan heeft grote meerwaarde voor de zorgsector.
- De uitwerking van het plan verschilt met Nederlands beleid wat betreft de oprichting van het steuncentrum en plaatst een kanttekening in hoe dit zich zal verhouden met nationale taken en verantwoordelijkheden.
- De grondhouding wat betreft bevoegdheid, subsidiariteit en proportionaliteit is positief.

Proces
Na bespreking in de BNC op 12 februari, zal het fiche op 18 februari in de CoCo besproken worden. Op 21 februari volgt behandeling in MR, waarna het BNC-fiche door de minister van Buitenlandse Zaken aan de Eerste en Tweede Kamer wordt gezonden. Op EU-niveau bespreken de lidstaten de aanbeveling in de Horizontale Werkgroep cybervraagstukken.

4. Toelichting

a. Draagvlak politiek
De kabinetsbrede inzet voor het realiseren van een digitaal veilige en weerbare samenleving wordt uiteengezet in de Nederlandse Cybersecurity Strategie (hierna NLCS). De internationale samenwerking zowel in EU- en NAVO-verband als daarbuiten wordt benadrukt in deze strategie, dit gezien het grensoverschrijdende karakter van cyberdreigingen. Het actieplan sluit aan bij de doelen van het kabinet omschreven in de NLCS om de digitale weerbaarheid van de EU te vergroten.

b. Draagvlak maatschappelijk en eenduidige communicatie
N.v.t

c. Financiële en personele gevolgen
Het is nog niet mogelijk de gevolgen voor de EU-begroting in te schatten.

d. Juridische aspecten haalbaarheid
De maatregelen hebben geen directe invloed in wet- en regelgeving.

e. Afstemming (intern, interdepartementaal en met veldpartijen)
Intern afgestemd met IZ, DICIO en PDWZ; interdepartementaal met het ministerie van J&V, BZ, FIN, EZ en BZK.

f. Gevolgen administratieve lasten
N.v.t

g. Toezeggingen
N.v.t

h. Fraudetoets
N.v.t

5. Informatie die niet openbaar gemaakt kan worden

a. Motivering
Tot personen herleidbare gegevens zijn onleesbaar gemaakt vanwege de bescherming van de persoonlijke levenssfeer.