Regeling van de Minister van Volksgezondheid, Welzijn en Sport, van [datum], nr. PM, houdende regels ter uitvoering van de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit voor de sector Gezondheidszorg en de subsector Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek (Cyberbeveiligingsregeling zorg)

[KetenID WGK028136]

de Minister van Volksgezondheid, Welzijn en Sport,

Gelet op de artikelen 2, tweede lid, 20, 24, eerste lid, 27 en 29 van het Cyberbeveiligingsbesluit;

Handelend na overleg met de minister van Veiligheid en Justitie;

Besluit:

Hoofdstuk 1. Algemene bepalingen

Artikel 1.1 Begripsbepaling
In deze regeling wordt verstaan onder
kritisch bedrijfsproces: Een proces dat noodzakelijk is voor de instandhouding van de dienstverlening van een essentiële of belangrijke entiteit.
de Minister: de minister van Volksgezondheid, Welzijn en Sport;

Artikel 1.2 Reikwijdte
Deze regeling is van toepassing op de sector Gezondheidszorg en de subsector Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek, bedoeld in bijlage 1 en 2 van de wet.

Hoofdstuk 2. CSIRT

Artikel 2.1 Aanwijzing CSIRT
Stichting Z-CERT is het CSIRT voor de sector Gezondheidszorg en de subsector Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek.

Artikel 2.2 Governance
Stichting Z-CERT draagt zorg voor:
a. het instellen van een raad van toezicht die voldoet aan bij statuten te stellen eisen van deskundigheid en onafhankelijkheid;
b. het in de statuten en in het reglement vastleggen van de wijze waarop toezicht wordt gehouden door de raad van toezicht;
c. de bevoegdheid van de raad van toezicht tot het benoemen van het bestuur;
d. de bevoegdheid van de raad van toezicht om het bestuur of een bestuurslid te kunnen ontslaan wegens verwaarlozing van de taak, wegens andere gewichtige redenen of wegens ingrijpende wijziging van de omstandigheden;
e. het vastleggen in de statuten dat een wijziging van de statuten eerst mogelijk is nadat de Minister daarmee heeft ingestemd; en
f. het vastleggen in de statuten dat de stichting niet wordt opgeheven voordat de Minister daarmee heeft ingestemd.

Artikel 2.3 Verantwoording
1. Stichting Z-CERT stelt jaarlijks een begroting en een jaarplan op en zendt deze voor 1 december van het aankomende begrotingsjaar naar de Minister.
2. Stichting Z-CERT zendt de Minister onverwijld een kopie van de vastgestelde jaarrekening en het bestuursverslag.
3. De controle van de jaarrekening en het bestuursverslag geschiedt overeenkomstig artikel 2:393 Burgerlijk Wetboek.
4. Indien stichting Z-CERT naast de taken op grond van de wet ook andere werkzaamheden verricht, geeft de stichting de Minister jaarlijks inzage in de aard en omvang van deze andere werkzaamheden.

5. Het bestuur van de stichting Z-CERT organiseert ten minste eenmaal per jaar een overleg met de Minister over het jaarplan, de taakuitoefening, de financiële positie van het de stichting en andere aangelegenheden die voor de taakuitvoering als CSIRT van belang zijn.
6. De raad van toezicht van stichting Z-CERT overlegt met de Minister indien de Minister dat noodzakelijk acht.
7. Stichting Z-CERT verstrekt aan de Minister desgevraagd alle inlichtingen die van belang zijn voor de taakuitoefening van de Minister of voor de taakuitoefening van door de Minister aangewezen toezichthouders.
8. Stichting Z-CERT informeert de Minister schriftelijk vooraf over te nemen besluiten die van wezenlijke invloed zijn op de uitoefening van de taken als CSIRT.

Artikel 2.4 Taakverwaarlozing
Indien de Stichting Z-CERT haar wettelijke taken ernstig verwaarloost, kan de Minister algemene en specifieke aanwijzingen geven om de goede taakuitoefening te waarborgen.

Artikel 2.5 Andere activiteiten
Stichting Z-CERT verricht geen activiteiten die de uitvoering van de wettelijke taken belemmeren of anderszins beïnvloedden.

Artikel 2.6 Continuïteit
Indien stichting Z-CERT wordt opgeheven of indien haar wettelijke taken door de Minister worden overgedragen aan een andere organisatie, verstrekt stichting Z-CERT de archiefbescheiden en systemen die noodzakelijk zijn voor de uitvoering van de wettelijke taken aan de Minister.

Hoofdstuk 3. Nadere regels cyberbeveiliging

Artikel 3.1 Maatregelen
De maatregelen, bedoeld in artikel 21, eerste lid, van de wet :
a. voldoen aan het bepaalde in NEN 7510, uitgegeven in 2024;
b. voldoen aan het bepaalde de NEN-ISO-IEC 27001 en NEN-ISO-IEC-27002 uitgegeven in 2022; of
c. hebben een gelijkwaardig beschermingsniveau.

Artikel 3.2 Criteria significante incidenten
1. Van een significant incident is sprake indien als gevolg van het incident:
   a. een kritisch bedrijfsproces langer dan 4 uur gedeeltelijk of geheel stil ligt;
   b. netwerk- en informatiesystemen die cruciaal zijn voor de instandhouding van de dienstverlening of productie van de belangrijke of essentiële entiteit zijn gecompromitteerd of vernietigd;
   c. de integriteit, vertrouwelijkheid of beschikbaarheid van bedrijfsgevoelige informatie ernstig is aangetast;
   d. de vertrouwelijkheid van bijzondere persoonsgegevens of BSN-nummers ten gevolge van een vermoedelijke kwaadwillende handeling ernstig zijn aangetast; of
   e. sprake is van blijvend letsel, ziekenhuisopname of overlijden van een persoon.
2. Van een significant incident is tevens sprake indien een incident de gevolgen omschreven in het eerste lid kan veroorzaken.
3. Dit artikel is niet van toepassing indien sprake is van geplande gevolgen van geplande onderhoudswerkzaamheden die door of namens de essentiële entiteit of belangrijke entiteit worden uitgevoerd.

Artikel 3.3 Vroegtijdige waarschuwing
1. In aanvulling op artikel 26, eerste lid, van de wet en artikel 25 van het Cyberbeveiligingsbesluit bevat de vroegtijdige waarschuwing eveneens hoe het incident is ontdekt en de ondersteuning die nodig is vanuit het CSIRT om het incident te beheersen.
2. De in artikel 25, onder b, van het Cyberbeveiligingsbesluit bedoelde gegevens betreffen:
a. de gevolgen die zijn geïdentificeerd voor het primaire proces en voor zover bekend bij de leveranciers van de entiteit, die de melding doet en afnemers van producten en diensten van die entiteit; en
b. de netwerk- en informatiesystemen en vestigingen die zijn geraakt door het incident.

Artikel 3.4 Melding
De gegevens die verstrekt worden bij een melding als bedoeld in artikel 27 van de wet bevatten, voor zover bekend:

a. de oorzaak van het incident;
b. de netwerken en systemen die zijn geraakt door het incident;
c. de gevolgen voor het primaire proces;
d. de gevolgen voor leveranciers aan de entiteit, die de melding doet en afnemers van producten en diensten van die entiteit; en
e. de gevolgen voor de integriteit, beschikbaarheid en vertrouwelijkheid van bijzondere persoonsgegevens, BSN-nummers en bedrijfsgevoelige informatie.

Artikel 3.5 Voortgangs- en eindverslag
Het voortgangsverslag en het eindverslag, bedoeld in artikel 29, eerste en tweede lid, van de wet, omvatten naast de gegevens genoemd in dat artikel, tevens:
a. een beschrijving in hoeverre in de risicoanalyses die voorafgaand aan het incident waren uitgevoerd de in het kader van het incident opgetreden gebeurtenissen waren voorzien, de maatregelen die naar aanleiding van die risicoanalyses zijn genomen en in hoeverre die maatregelen hebben bijgedragen aan het voorkomen of beperken van het incident;
b. de wijze waarop het continuïteitsplan is gebruikt en de mate waarin dit plan effectief is gebleken;
c. de betrokkenheid van bij het incident betrokken leveranciers van netwerk- en informatiesystemen, waaronder de:
    1°. afspraken die met deze partijen zijn gemaakt over het voorkomen van cyberincidenten en over het handelen in geval van een cyberincident;
    2°. wijze waarop is gehandeld om het nakomen van deze afspraken te controleren;
    3°. wijze waarop de afspraken zijn nagekomen; en
    4°. gezamenlijke evaluatie van het incident; en
d. de lessen die door de entiteit zijn getrokken uit het incident en tot welke maatregelen dit heeft geleid.

Hoofdstuk 4. Aanwijzing autoriteit en toezichthouder

Artikel 4.1 Aanwijzingen autoriteit

Als autoriteit als bedoeld in artikel 51, tweede lid, onderdeel i, van de wet, worden aangewezen de ambtenaren van de Inspectie Gezondheidszorg en Jeugd die zijn die belast met het toezicht op de naleving van deze wet voor wat betreft de sector Gezondheidszorg en de subsector Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek, bedoeld in bijlage 1 en bijlage 2 van de wet.

Artikel 4.2 Aanwijzing toezichthouder

Als toezichthouders als bedoeld in artikel 68, eerste lid, van de wet, worden aangewezen de ambtenaren van de Inspectie Gezondheidszorg en Jeugd.

Hoofdstuk 5. Slotbepalingen

Artikel 5.1 Inwerkingtreding
Deze regeling treedt in werking op het tijdstip waarop artikel 16 van de wet in werking treedt.

Artikel 5.2 Citeertitel
Deze regeling wordt aangehaald als: Cyberbeveiligingsregeling zorg.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Minister van Volksgezondheid, Welzijn en Sport