31765 Kwaliteit van zorg

27529 Informatie- en Communicatietechnologie (ICT) in de Zorg

Nr. 275 Brief van de minister van Volksgezondheid, Welzijn en Sport

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 juni 2017

In mijn brief[1] van 15 december jl. over informatiebeveiliging in de zorg heb ik aangegeven er naar te streven voor de zomer gezamenlijk met branchepartijen een actieplan (informatie)beveiliging patiëntgegevens uit te werken. Met deze brief informeer ik u over de stand van zaken.

1. Aanleiding

Zorginstellingen worden regelmatig geconfronteerd met risico's op het gebied van informatiebeveiliging en privacybescherming. Dit illustreert onder andere de ransomware aanval[2] van 12 mei jl. Ik heb naar aanleiding hiervan de leden van het Informatieberaad Zorg een brief[3] gestuurd, waarin ik de leden van het informatieberaad Zorg en bestuurders in de zorg nogmaals oproep om adequate maatregelen te nemen om informatiebeveiliging verder te versterken. Ik ga er vanuit dat brancheorganisaties deze verantwoordelijkheid ook nemen en hun achterban ondersteunen bij het (nog) verder aanscherpen van technische maatregelen en verbeteren van de informatiebeveiliging. Hoewel ik geen signalen heb gekregen dat de Nederlandse gezondheidszorg gevolgen heeft ondervonden van deze aanval, toont deze aanval wel de urgentie van het onderwerp informatiebeveiliging aan.

Op 15 december jl. heb ik het PBLQ rapport over beveiliging van patiëntgegevens aan uw Kamer gestuurd. De koepelorganisaties in de medisch specialistische zorg en geestelijke gezondheidszorg (ggz) onderschrijven de conclusies en aanbevelingen uit het PBLQ rapport en hebben dit aangegrepen om met VWS te bezien welke additionele activiteiten kunnen worden genomen in aanvulling, of als uitbouw van acties die in de sector al worden opgepakt. Dit overleg tussen VWS en branchepartijen in de medisch-specialistische zorg en ggz heeft geleid tot bijgevoegd actieplan[4].

---

[1] Kamerstuk 31 765, nr. 259

[2] Ransomware is software die de bestanden versleutelt van een systeem waardoor deze niet meer leesbaar zijn. Met een digitale sleutel zijn de bestanden weer leesbaar te maken. Voor deze digitale sleutel moet vaak 'losgeld' betaald worden, vandaar dat ransomware ook wel gijzelsoftware wordt genoemd.

[3] Brief Informatieberaad Zorg 19 mei 2017 Informatiebeveiliging in de zorg, kernmerk 1135669-163960-DICIO

[4] Raadpleegbaar via www.tweedekamer.nl

2. Opzet actieplan

Het plan is in nauwe samenwerking met de Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU), GGZ Nederland en Zelfstandige Klinieken Nederland (ZKN) tot stand gekomen. Het voornaamste doel is om op korte termijn te komen tot een structurele verbetering van de informatiebeveiliging en privacybescherming in de dagelijkse werkpraktijk bij ziekenhuizen, zelfstandige klinieken en ggz-instellingen. In het plan zijn concrete activiteiten benoemd waarmee koepelorganisaties en/of zorgaanbieders al aan de slag zijn, of gaan, of die in de komende periode breder worden toegepast. Het gaat daarbij bijvoorbeeld om het breed inzetten van bewustwordingscampagnes, het bieden van ondersteuning aan leden en aanpassen van bewerkersovereenkomsten vooruitlopend op de komst van de Algemene Verordening Gegevensbescherming (AVG).

De insteek van het actieplan is om de focus allereerst te richten op het inventariseren, delen en implementeren van de in de praktijk bewezen 'good practices' die gebruikt kunnen worden voor een zorgbrede implementatie. Het kan hierbij gaan om het verspreiden van goed werkende instrumenten onder het management van zorgaanbieders, voorlichtingsbijeenkomsten en verspreiden van e-learningmodules. Hierbij is het van belang zowel in te zetten op cultuur, structuur als compliance ten aanzien van regelgeving. Omdat relevant is hoe personen binnen de zorgaanbieder handelen, het thema is verankerd in de organisatie en op welke wijze wordt geanticipeerd op (nieuwe) regelgeving zoals de Algemene Verordening Gegevensbescherming.

In het PBLQ-rapport is uitvoerig aandacht besteed aan de wijze waarop ziekenhuizen[5] en instellingen voor geestelijke gezondheidszorg in de dagelijkse praktijk omgaan met de beveiliging van hun patiëntgegevens en hoe hierin verbetering kan worden aangebracht. De aanbevelingen uit dit rapport hebben gediend als uitgangspunt voor de activiteiten die de brancheorganisaties in de medisch-specialistische zorg en ggz gaan ondernemen om informatiebeveiliging verder op orde te krijgen.

In het actieplan worden in lijn met de aanbevelingen:

a. Krachten gebundeld door het zorgbreed doorvoeren en implementeren van 'good practices', zoals het NFU-normenkader rond informatiebeveiliging en de jaarlijkse ZEKER[6] campagnes van de NVZ rond informatiebeveiliging, waaraan in 2017 ook GGZ Nederland meedoet;
b. Activiteiten opgezet die er voor zorgen dat wet- en regelgeving goed begrepen

[5] inclusief privéklinieken, zelfstandige behandelcentra en revalidatiecentra
[6] ZEKER is een initiatief van de NVZ en haar leden. De campagne wijst medewerkers op het belang van informatiebeveiliging in de zorg en geeft medewerkers handvatten hoe om te gaan met gevoelige informatie www.zorgzekeren.nl

wordt door iedereen die in deze sectoren werkzaam is. Bijvoorbeeld door de Toolkit privacybescherming en informatieveiligheid/-beveiliging (PBIV) ggz van GGZ Nederland;

c. Activiteiten ondernomen om wet- en regelgeving beter te implementeren en te anticiperen op de komst van de Algemene Verordening Gegevensbescherming. Dit gebeurt bijvoorbeeld door publicatie van relevante informatie op websites van brancheorganisaties of aanbieders, de Handreiking voor naleving meldplicht datalekken van de KNMG en de informatie op de website van de Autoriteit Persoonsgegevens (AP).

In het plan zijn ook doelen en voornemens benoemd die nadere uitwerking en verankering behoeven. In de komende periode dient die uitwerking nader plaats te vinden. Ik zal hierop monitoren en uw Kamer hierover begin 2018 informeren.

Ik vind het belangrijk dat brancheorganisaties hun kennis en ervaring rond de beveiliging en bescherming van patiëntgegevens met elkaar te delen en goede voorbeelden zorgbreed beschikbaar te stellen. In de afgelopen maanden is in verschillende sessies met de koepelorganisaties geïnventariseerd welke acties op de korte en op de lange termijn verbreed kunnen worden. Hierbij is sprake van een fasering. De ZEKER-campagne van de NVZ kan bijvoorbeeld al op korte termijn breed toegepast worden en ook worden ingezet in de ggz. E-learning modules die door individuele zorgaanbieders zijn ontwikkeld dienen eerst geïnventariseerd te worden en indien bruikbaar breder verspreid.

Omdat in alle lagen van de zorgorganisatie van Raad van Bestuur tot aan de helpdesk en balie wordt gewerkt met (patiëntgevoelige) informatie richt het plan zich op al deze lagen.

Bestuur en management
Informatiebeveiliging en bescherming van persoonsgegevens zijn onderdeel van de integrale managementverantwoordelijkheid. Door de verspreiding van factsheets en informatie, maar ook door het aansluiten op de Z-CERT kan beter invulling worden gegeven aan deze verantwoordelijkheid. Daarnaast is het relevant dat bestuurders goede bewerkersovereenkomsten afsluiten en gebruik kunnen maken van een modelbewerkersovereenkomst.

Functionaris gegevensbescherming (FG) en Information Security Officer (ISO)
FG's en ISO's moeten beschikken over voldoende kennis en vaardigheden en positie hebben in de organisatie. Door activiteiten uit het actieplan, zoals het werken naar een passend opleidingsaanbod en organiseren van intervisiebijeenkomsten worden deze functionarissen meer in stelling gebracht.

Medewerker
Blijvende en geborgde awareness voor informatiebeveiliging en bescherming van persoonsgegevens bij medewerkers is van groot belang. Om kleine en grote datalekken te voorkomen, zal de NVZ en GGZ Nederland de campagne ZEKER in oktober gelijktijdig starten met de campagne Alert Online[7]. De ZEKER campagne zal op verschillende niveaus managers en medewerkers van zorginstellingen op een toegankelijke en aansprekende manier bewust maken hoe ze datalekken kunnen voorkomen. Deze campagne wordt mogelijk verbreed naar zelfstandige klinieken en UMC's, zodat optimaal gebruik kan worden gemaakt van de kennis en ervaring die de NVZ reeds heeft opgebouwd. Ook kan de awareness worden versterkt door e-learning tools beschikbaar te stellen aan medewerkers die werken met digitale patiëntendossiers.

Cliënten
Bewustzijn van rechten en verantwoordelijkheden met betrekking tot informatiebeveiliging en gegevensbescherming wordt vergroot door cliënten te informeren over eigen verantwoordelijkheid, maar ook aan te geven waar ze bij een zorginstelling terecht kunnen om privacylekken te melden. Koepelorganisaties spreken hun leden hier op aan.

3. Uitvoeren en implementeren van actieplan

Sinds 1 april 2017 is een sectorale CERT voor de zorg, Z-CERT, actief die helpt bij ICT-incidenten in de zorg. De Z-CERT is een voorziening om bij cyberincidenten snel in actie te kunnen komen, om detectie te versnellen en kennisdeling over informatie-beveiligingsincidenten te vergroten en hiermee de impact van dergelijke incidenten te beperken. Alle ziekenhuizen, GGZ-instellingen en categorale instellingen kunnen hieraan deelnemen en door een groeimodel kunnen op termijn alle zorgaanbieders zich aanmelden. VWS heeft dit initiatief ondersteund door een opstartsubsidie te verlenen. Mede gezien de rol die de Z-CERT momenteel vervult en de urgentie om op korte termijn zorginstellingen te ondersteunen met concrete hulpmiddelen heb ik de Z-CERT gevraagd om de instrumenten en informatie die bij aanbieders beschikbaar zijn, en breed inzetbaar kunnen zijn of een vliegwiel kunnen creëren, te inventariseren en breder te verspreiden en in te zetten. Om de initiatieven vanuit de sector te faciliteren en ondersteunen en bij te dragen aan de invulling van de verantwoordelijkheid van de sector wil ik de programmaorganisatie bij de Z-CERT voor de inventarisatie en implementatie van beschikbare instrumenten financieel ondersteunen. Dit om een breed gedragen overkoepelend palet aan aanvullende concrete instrumenten op korte termijn beschikbaar te hebben voor alle zorginstellingen. De komende maanden zal de programmaorganisatie bij de Z-CERT de door de koepels

[7] Landelijke campagne van twee weken waarbij diverse activiteiten gelanceerd worden om cyberskills te vergroten en Nederland digitaal veiliger te maken

aangedragen actiepunten nader uitwerken en zo snel mogelijk zorgbreed beschikbaar stellen.
Voor deze ondersteuning en ondersteuning van andere overkoepelende initiatieven stel ik totaal € 0,6 miljoen beschikbaar over een periode van drie jaar vanaf 2017.

Ik heb het voornemen het actieplan en activiteiten om informatiebeveiliging op te schalen uit te breiden naar andere sectoren. Ik zal uw Kamer hierover nader informeren. Tevens houd ik vinger aan de pols en zal u, zoals aangegeven, begin 2018 informeren over de invulling en uitvoering van acties.

Zorginstellingen en zorgverleners zijn in eerste plaats zelf verantwoordelijk voor informatiebeveiliging en moeten voldoen aan Europese en nationale wettelijke voorschriften. Door actiepunten te benoemen, hebben koepels invulling gegeven aan deze verantwoordelijkheid. Ook de IGZ en AP zullen hun bijdrage leveren. De AP zal eventuele onduidelijkheden in wet- en regelgeving nader duiden. De IGZ zal wanneer zij daar aanleiding toe ziet relevante toezichtinformatie over risico's en risicobeheersing breed beschikbaar maken, bijvoorbeeld in de reguliere overleggen met partijen, via de eigen website, een artikel of een circulaire. Om het zorgveld voor te bereiden op de komst van de Algemene Verordening Gegevensbescherming zal VWS een ondersteunende rol bieden door aan brancheorganisaties in de zorg uitleg, goede voorbeelden en eventuele hulpmiddelen beschikbaar te stellen en te fungeren als informatiepunt voor de brancheorganisaties voor zorgspecifieke vragen. De AP wordt hierbij betrokken.

De Z-CERT zal, zoals aangegeven, haar dienstverlening de komende maanden verder uitbreiden. De Z-CERT zie ik als een belangrijke extra waarborg om bij informatiebeveiligingsincidenten snel in actie te kunnen komen. Ik roep bestuurders, die nog niet zijn aangesloten bij de Z-CERT, dit wel te doen.

Ik wil tot slot benadrukken dat patiënten er op moeten kunnen vertrouwen dat de bescherming van medische gegevens maximaal is geregeld door de zorginstellingen. Dit is noodzakelijk voor de vertrouwensrelatie met de zorgverlener. Beveiliging van patiëntgegevens is een doorlopend punt van aandacht en zal altijd een onderwerp blijven waar alle partijen zich voor moeten hardmaken. Met het Actieplan (informatie)beveiliging patiëntgegevens heeft de sector een belangrijke stap gezet om de bescherming van medische gegevens verder te verbeteren.

De minister van Volksgezondheid, Welzijn en Sport,
E.I. Schippers