Basisbeveiligingsmodel Care

Een handreiking informatieveiligheid voor de caresector

Voorjaar 2019

Het Basisbeveiligingsmodel Care (BBMCare) is een standaardaanpak om informatie bij zorginstellingen te beveiligen. Uitgangspunt is een op de caresector toegesneden basisniveau van beveiliging volgens de Nederlandse beveiligingsnorm NEN 7510. BBMCare is vanaf 2019 zonder kosten beschikbaar voor zorginstellingen.

Cliëntinformatie beter beveiligen

De beveiliging van cliëntinformatie is vaak minder goed geregeld dan de NEN 7510 voorschrijft. Organisaties hebben hun risico's niet altijd goed in beeld, omdat het uitvoeren van een hiervoor benodigd onderzoek veelal als lastig en tijdrovend wordt ervaren. Het Basisbeveiligingsmodel Care (BBMCare) helpt je bij het maken van deze risicoafweging. Met dit model kun je op een praktische manier stap voor stap je informatiebeveiliging inrichten volgens de NEN 7510.

Wij hebben het voorwerk al gedaan

Centraal staan de begrippen inventariseren (bedrijfsactiviteiten met ondersteunende informatieobjecten), classificeren (in welke mate beveiligen?) en selecteren (met welke beveiligingsmaatregelen?). Het model gaat uit van een risicoafweging die gebaseerd is op het proces ouderenzorg en houdt rekening met de geldende wetten en regels.

Het vervolg doe je zelf

Natuurlijk is elke zorginstelling uniek. Daarom vergelijk je de algemeen geldende risicoafweging uit het model met de situatie van jouw instelling. Eventuele verschillen verwerk je in het model en zo voer je gaandeweg je eigen risicoanalyse uit! Ook leg je in de zogenaamde nulmeting vast voor welke normelementen van NEN 7510 je al beveiligingsmaatregelen hebt getroffen. Je ziet dan vanzelf voor welke normelementen nog aanvullende maatregelen nodig zijn (gap-analyse).

Belang NEN 7510

Vanaf 2018 is onderstaande wet- en regelgeving in relatie tot NEN 7510 van belang.

Besluit elektronische gegevensuitwisseling in de zorg

In dit besluit onder anderen de verplichting om te voldoen aan de veiligheids- en zorgvuldigheidseisen van NEN 7510.

Toetsingskader IGJ Inzet van e-health door zorgaanbieders

Thema 5 stelt 'de inspectie verwacht dat zorgaanbieders aantoonbaar werk maken van een managementsysteem voor informatiebeveiliging dat voldoet aan de wettelijke norm' (NEN 7510 § 4.4).

Gefaseerde aanpak

Je kunt ervoor kiezen een informatiebeveiligingsplan in stappen in te richten. Eerst het beveiligingsniveau Laag: de belangrijkste beveiligingsmaatregelen zoals ook genoemd in het *Praktijkboek NEN 7510*. Daarna niveau Gemiddeld, op basis van *best practices* en uiteindelijk niveau Hoog, afgestemd op de situatie van de instelling. Informatiebeveiliging die volgens deze werkwijze tot stand komt laat bij iedere stap zien in welke mate de instelling *aantoonbaar* voldoet aan de NEN 7510.

Hulpmiddelen

Het model maakt gebruik van twee documenten:

- Het *Inventarisatie- en Classificatiedocument Informatiebeveiliging* (I&Cdoc) brengt bedrijfsactiviteiten met ondersteunende informatiemiddelen en mogelijke kwetsbaarheden in kaart. Aan de informatiemiddelen zijn betrouwbaarheidsvereisten beschikbaarheid, integriteit en vertrouwelijkheid gekoppeld en geclassificeerd. Kwetsbaarheden kunnen worden uitgewerkt in risicoscenario's. Ook is er aandacht voor de fysieke beveiliging van gebouwen en objecten. Er is een template beschikbaar om een zorglocatie in te delen in beveiligingszones openbaar, beschermd, beveiligd en vitaal.
- Het *Werkdocument NEN 7510* beschrijft alle normelementen van de NEN 7510, in eerste instantie voor de nulmeting om daarna de verbeteracties toe te voegen. Het werkdocument bevat verwijzingen naar zowel de algemene inventarisatie als die welke speciaal voor de instelling is toegevoegd.

Als hulp bij de beveiligingswerkzaamheden is een *Stappenplan* en een uitgebreide *Handleiding* beschikbaar.

NEN 7510

§ 8.1.1 Inventariseren van bedrijfsmiddelen

Informatie en andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.

§ 8.2.1 Classificatie van informatie

Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijzigen.

§ 11.1.1 Fysieke beveiligingszones

Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.

Privacywetgeving

Het model ondersteunt twee belangrijke elementen van de Europese privacywetgeving (AVG), het Verwerkingsregister en de Privacy Impact Analyse (PIA).

- Als bij het inventariseren van informatiemiddelen ook persoonsgegevens zijn betrokken, kan er sprake zijn van een 'verwerking' van die gegevens. De bijbehorende bedrijfsactiviteit is dan het *verwerkingsdoel* en het bedrijfsmiddel de *verschijningsvorm*. Daar kunnen de overige register-specifieke gegevens aan worden toegevoegd.
- Als het een verwerking betreft met een groot privacy-risico kan een aanvullende PIA nodig zijn. Dit komt overeen met een risicoscenario uit het I&C-document. Zowel in een PIA als in een risicoscenario beschrijf je de relevante aspecten voor het selecteren van evenwichtige beveiligingsmaatregelen.

Waarom BBMCare?

- Het model doorbreekt de impasse van 'hoe te beginnen?'
- Het BBMCare is eenvoudig toe te passen; het is geen expertbenadering
- Het model staat voor een gefaseerde aanpak van informatiebeveiliging
- Het is een beheermodel waaraan auditacties kunnen worden toegevoegd
- Er is een uitgebreide handleiding met praktijkvoorbeelden beschikbaar

Of een BBMCare-onderdeel?

Heb je informatiebeveiliging al voor een groot deel ingericht, dan kun je gebruik maken van afzonderlijke onderdelen zoals:

- *inventarisatietabel informatie-gerelateerde componenten*; ben ik compleet?
- *werkdocument NEN7510*; onderhoud en inzicht in status beveiliging!
- *template gebiedsindeling zorglocaties*; óók werken aan fysieke beveiliging!

Overige hulpmiddelen

BBMCare biedt een werkwijze voor het inrichten en onderhouden van informatiebeveiliging volgens de NEN 7510. Voor het uitwerken van de verschillende normelementen zijn onderstaande hulpmiddelen beschikbaar.

- *Handvatten informatieveiligheid*: ondersteunt uitwerking van de 12 belangrijkste normelementen; beveiligingsniveau Laag
- *Template gebiedsindeling zorglocaties*: ondersteunt uitwerking normelementen fysieke beveiliging (11.1)
- *e-Learningcursussen 'Veilig omgaan met vertrouwelijke informatie'*: ondersteunt normelement bewustwording (7.2.2).

Aanschaf BBMCare kosteloos

Vanaf 2019 zijn de BBMCare-documenten gratis beschikbaar voor zorginstellingen. In overleg met brancheorganisaties care wordt onderzocht op welke wijze de doorontwikkeling en beschikbaarstelling van BBMCare en andere beveiligingshulpmiddelen kan plaatsvinden. Er wordt gedacht aan de oprichting van een non-profitorganisatie. De werktitel is Stichting Zorg voor Informatieveiligheid en Privacy in de care; ZIPcare.

Ondersteuning BBMCare

Alhoewel de aanschaf van BBMCare kosteloos is, wordt met nadruk geadviseerd minimaal één dagdeel te investeren in ondersteuning om de aangeboden hulpmiddelen en werkwijze optimaal te benutten. Gezien de uitgebreide handleiding kan de gebruiker al snel zelfstandig aan de slag maar aanvullende ondersteuning is uiteraard mogelijk.

Contactgegevens

Met uitzondering van de e-learningcursus informatieveiligheid kunnen BBMCare en de hiernaast genoemde beveiligingshulpmiddelen kosteloos worden aangevraagd. Ook is er een lijst beschikbaar van marktpartijen die BBMCare kunnen ondersteunen. Neem voor producten, diensten en vragen contact op via info@caresecure.nl.

BBMCare is een product van Douwe de Jong en Peter van der Zwan
Tekstredactie martijndegroot.com, vormgeving ellenbouma.nl