

Evaluatie BBMCare

februari 2019

Najaar 2018 heeft de IGJ het Toetsingskader *Inzet van e-health door zorgaanbieders* gepubliceerd. Daarin staat bij thema 5 Informatiebeveiliging en continuïteit: 'de inspectie verwacht dat zorgaanbieders aantoonbaar werk maken van een managementsysteem voor informatiebeveiliging dat voldoet aan de wettelijke norm'. Dit was de aanleiding om het gebruik van BBMCare te evalueren; om zicht te krijgen op de succes- en faalfactoren.

Vijf BBMCare-gebruikers zijn gevraagd aan het onderzoek mee te werken. Bij twee organisaties was men wel begonnen met het instelling-specifiek maken van de generieke, op het proces ouderenzorg gerichte inventarisatie maar is men uiteindelijk afgehaakt. Response van juist deze organisaties is waardevol om zicht te krijgen op randvoorwaarden bij het inrichten én vooral onderhouden van informatiebeveiliging door gebruik te maken van BBMCare.

Hieronder een samenvatting van de evaluatieresultaten. Er zijn vele sterke punten genoemd, ook door de afvallers. De zwakke punten worden meegenomen bij de eerstvolgende revisieslag. Een belangrijke les is dat vooral kleine organisaties ondersteuning nodig hebben bij het inrichten van BBMCare. En dat het welslagen van BBMCare vooral te maken heeft met de betrokkenheid van de verantwoordelijke medewerker. Voor deze medewerker is kennis van ict en/of informatiebeveiliging beslist geen must; het is belangrijker dat de medewerker zich betrokken voelt en daar waar nodig ondersteund wordt door de benodigde disciplines.

Sterke punten BBMCare

Algemeen

- 1^e praktische beveiligingsproduct dat ik tegenkwam
- laagdrempelig; eenvoudige start; niet duur
- geeft inzicht in informatiebeveiliging; 'eindelijk heb ik het gevoel grip te hebben op IB!'
- IB snel 'tussen de oren' door uit te gaan van herkenbare processen (referentiedomeinenmodel care)
- door uit te gaan van alle care-processen (referentiedomeinenmodel care) kun je niets vergeten heb je het gevoel dat v.w.b. informatieveiligheid alles in beeld is
- helpt je beveiligingszaken in beeld te brengen en te ordenen
- IB wordt niet groter dan nodig! (niet klakkeloos uitgaan van *alle* NEN 7510 normelementen)
- aanvulling voor kwaliteitsfunctionaris
- eenvoudig te actualiseren i.v.m. onderhoud
- ondersteunt continuïteit / overdracht naar andere medewerkers.

Inhoudelijk

- kant en klare risicoanalyse waardevol
- ondersteunt inventarisatiefase informatiebeveiliging
- I&Cdoc IB is de trigger om risico's in kaart te brengen
- Werkdoc NEN 7510; duidelijk welke normelementen wel / niet uitwerken
- IB wordt stapje voor stapje beter
- je kunt de accountant iets laten zien en die is ook nog eens enthousiast

Zwakke punten BBMCare

- Procesmodel (referentiedomeinenmodel care) spreekt niet aan
- BBMCare smooit niet echt mooi; te veel handmatig onderhoud zoals verwijzingen tussen de BBMCare-documenten
- Te veel materiaal en werd te vaak bijgewerkt (*a.g.v. revisie NEN 7510:2017 en AVG*)
- Geen duidelijk werkkader (*Stappenplan BBMCare sloeg niet aan*)
- Nog wel aanvullende beveiligingsdocumenten nodig zoals Register verwerkingen en Voortgangsdokument (*kan, maar is vooral bij kleine organisaties niet nodig*).

Aanbevelingen

Voor de organisatie

- Aandacht voor de start: bespreek de randvoorwaarden in termen van benodigde capaciteit, kosten en vooral betrokkenheid bestuurders
- De start wellicht in de vorm van een formeel intakegesprek met verantwoordelijken
- Aandacht voor periodieke ondersteuning; vooral als de organisatie onzeker is en onvoldoende kennis heeft
- Regelmatig langs komen als stok achter de deur!
- Zorg dat er korte lijnen voor ondersteuning zijn; samen de rode draad vasthouden
- De FG-er kan een ingang zijn; wellicht als trekker om AVG te verbreden naar NEN 7510.

Algemeen

- Vanuit ActiZ netwerk IB inrichten? (*zoals bij VNZ wel is geregeld*) Of in BoZ-verband?
- Regionale intervisiegroepen om elkaar te ondersteunen?
- Zorg dat het model bekend is bij onafhankelijke dienstverleners van care-producten; vooral bij beheerdiensten meer aandacht voor informatieveiligheid!

Hoe verder met BBMCare?

Dit voorjaar staat het volgende op de agenda:

- Kennisoverdracht BBMCare naar marktpartijen
- Inrichten gebruikersgroep / deskundigheidsgroep BBMCare
- Informeren en eventueel samenwerken met niet-commerciële partijen zoals brancheorganisaties zorg / BoZ, Nictiz, Z-Cert, CIP-overheid en IGJ.

Ook komt er meer aandacht voor het gebruik van afzonderlijke BBMCare componenten in relatie tot de behoefte van de klant cq als aanvulling op de actuele beveiligingssituatie.

Tot slot

BBMCare is geen commercieel product; de documenten zijn vrij beschikbaar door te mailen naar info@caresecure.nl; contactpersonen zijn Peter van der Zwan en Douwe de Jong.

De folder staat ook op het ActiZnetwerk #HuisOpOrde.