Van checklist naar certificering

Auteurs: Aart Bitter en Dave Hagenaars

De gezondheidszorg gebruikt NEN 7510 tot nu toe als een checklist voor informatiebeveiliging. In navolging van het bedrijfsleven zou de zorg moeten overstappen naar de invoering van een managementsysteem met bijbehorende certificering op basis van ISO/IEC 27001.

De laatste tijd is er in de media veel aandacht voor informatiebeveiliging in de zorg. Aanleiding zijn onder meer de invoering van het landelijk elektronisch patiëntendossier (EPD) en een onderzoek van de Inspectie voor de Gezondheidszorg naar de status van informatiebeveiliging binnen ziekenhuizen. Duidelijk is dat er nog veel moet gebeuren om NEN 7510, de norm voor informatiebeveiliging in de zorg, in te voeren. Een interessante vraag hierbij is of zorginstellingen op de goede weg zijn om informatiebeveiliging binnen hun organisatie te implementeren en te borgen. Tijd voor een vergelijking met ontwikkelingen op het gebied van informatiebeveiliging in andere sectoren.

De NEN 7510 is sinds 2004 de standaard op het gebied van informatiebeveiliging, die speciaal voor de Nederlandse zorginstellingen is ontwikkeld. Deze norm is gebaseerd op de internationale standaard ISO 27002, die in Nederland beter bekend is onder de naam 'Code voor Informatiebeveiliging'.

De 'Code' stamt uit 1993 en bevat een overzicht van allerlei mogelijke beveiligingsmaatregelen die organisaties kunnen nemen om verstoringen in hun informatievoorziening te voorkomen en eventuele schade te beperken. Deze norm wordt sindsdien massaal door het bedrijfsleven als een soort checklist gebruikt om beveiligingsmaatregelen te treffen.

Toch werd al snel duidelijk dat er meer nodig is dan een checklist om informatiebeveiliging binnen een organisatie goed te kunnen implementeren. Onlosmakelijk verbonden met de Code werd een standaard opgesteld die de eisen aan een zogeheten 'Information Security Management System' (SMS) beschrijft. Een dergelijk managementsysteem is bedoeld om informatiebeveiliging binnen organisaties te kunnen implementeren, beheren, controleren en verbeteren. Deze internationaal erkende standaard is bekend onder de naam ISO/IEC 27001.

Meerwaarde

De grote meerwaarde van ISO 27001 ligt in de daarin beschreven aanpak voor het invoeren van informatiebeveiliging. Deze aanpak gaat uit van het inrichten van een managementsysteem voor informatiebeveiliging door een procesbenadering op basis van de Demingcirkel. Hierdoor wordt de kern van informatiebeveiliging geraakt, namelijk het beheersen van risico's door het nemen van maatregelen en het bewaken van de werking van deze maatregelen. De mogelijke beveiligingsmaatregelen zijn opgenomen in ISO 27001 en uitvoerig beschreven in ISO 27002 (en specifiek voor de gezondheidszorg in NEN 7510).

Er is meer nodig dan een checklist om informatiebeveiliging te implementeren

Een interessant aspect van ISO 27001 is dat het een zogenaamde toetsbare norm is. Daardoor is het mogelijk om te certificeren tegen deze standaard. Organisaties kunnen daarmee aantonen dat zij informatiebeveiliging hebben geïmplementeerd en dat zij in staat zijn om dat adequaat te onderhouden en verbeteren.

De afgelopen jaren is de populariteit van het certificaat sterk toegenomen. Het aantal uitgegeven certificaten steeg wereldwijd van ongeveer 1500 in 2005 naar ruim 5600 in 2009. Deze stijging is mede te danken aan het feit dat een gecertificeerde organisatie op deze manier verantwoording kan afleggen en aan externe belanghebbenden vertrouwen kan geven, dat aan de relevante eisen en verwachtingen wordt voldaan.

De gezondheidszorg heeft NEN 7510 tot op heden als een soort checklist gebruikt voor informatiebeveiliging. Er is weliswaar een toetsbare norm ontwikkeld in de vorm van NEN 7511, echter hierin zijn geen eisen gesteld aan een managementsysteem.

In navolging van het bedrijfsleven is het zeker de moeite waard voor de zorgsector om over te stappen naar invoering van een managementsysteem en bijbehorende certificering op basis van ISO/IEC 27001. Op deze manier kan ook de gezondheidszorg zich gemakkelijker extern verantwoorden over een uitgevoerde procesmatige benadering van informatiebeveiliging op basis van een internationaal erkende standaard. Bovendien kan hiermee worden aangetoond dat men continu voldoet aan alle eisen van NEN 7510 en dat de controlemaatregelen voor informatiebeveiliging aantoonbaar zijn geïmplementeerd. <

Aart Bitter is ISO 27001 Lead Auditor en Dave Hagenaars is managing director van BSI Management Systems B.V. BSI is grondlegger van de ISO/IEC 27001