M&I/Partners/

adviseurs voor management en informatie

Informatiebeveiliging naar hoger plan

De Scan NEN 7510 als vertrekpunt

Ziekenhuizen zijn ervan doordrongen dat informatiebeveiliging alle aandacht verdient. De komst van specifieke normen en de aankondiging van een externe audit door de Inspectie voor de Gezondheidszorg plaatsen het onderwerp extra hoog op de agenda. Wilt u uw informatiebeveiliging professionaliseren? Met de Scan NEN 7510 krijgt u naast een gedegen inzicht in het niveau van de informatiebeveiliging in uw ziekenhuis ook concrete adviezen om deze op een hoger plan te brengen.

Informatiebeveiliging is van alle tijden. Beschikbaarheid, integriteit en vertrouwelijkheid zijn de sleutelbegrippen. Dat was al zo in het papieren tijdperk, maar toen leek informatiebeveiliging niet zo'n issue. Juist nu de elektronische informatievoorziening in ziekenhuizen een vlucht neemt, staat informatiebeveiliging vol in de schijnwerpers.
Om op dit gebied duidelijke kaders te stellen, werd in 2004 de norm NEN 7510 geïntroduceerd. Enkele jaren later, in 2007, deed de Inspectie voor de Gezondheidszorg samen met het College Bescherming Persoonsgegevens bij twintig ziekenhuizen onderzoek naar de informatiebeveiliging. De titel van het rapport is veelzeggend: Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm (2008). De overige ziekenhuizen kregen de opdracht een Plan van Aanpak Informatiebeveiliging op te stellen. Ook werd een verplichte externe audit in 2010 aangekondigd. Tegen deze achtergrond én de maatschappelijke discussie rondom de invoering van het EPD mag het duidelijk zijn: informatiebeveiliging heeft voor ziekenhuizen hoge prioriteit.

Continue aandacht is vereist

Informatiebeveiliging vraagt niet om een eenmalige actie. De organisatie is immers niet statisch. Er doen zich doorlopend wijzigingen voor in de processen en daarmee in de informatievoorziening. Continue aandacht voor informatiebeveiliging is dus nodig, waarbij het ziekenhuis stap voor stap toegroeit naar een passend niveau van beveiliging. Een breed scala aan issues verdient de aandacht: van de organisatie van de informatiebeveiliging, de bewustwording van de medewerkers tot en met de fysieke beveiliging en de back-up van de digitale gegevensopslag. Is het passende niveau van informatiebeveiliging eenmaal bereikt, dan moet dat ook op peil blijven. Een audit is een prima manier om vast te stellen of de organisatie daarin slaagt. En de Scan NEN 7510 is uitstekend geschikt om in de aanloop naar een dergelijke audit de positie te bepalen.

Wat biedt de Scan NEN 7510?

De Scan NEN 7510 geeft op de 23 belangrijkste onderdelen van de NEN-norm (zie bijlage) een helder beeld van de informatiebeveiliging. Deze set omvat de onderdelen uit de NVZ-startnorm voor informatiebeveiliging en de onderdelen die zijn opgenomen in het Handboek NEN 7510. Daarnaast kunnen ziekenhuizen zelf enkele specifieke aspecten toevoegen. De scan toetst niet alle onderdelen van de norm, maar geeft niettemin een helder beeld van de informatiebeveiliging.

Per onderdeel krijgt u een rapportage op de volgende punten:

1) Beoordeling van het informatiebeveiligingsbeleid van het ziekenhuis.

2) Statusomschrijving van het onderdeel in termen van opzet, bestaan en werking.
3) Een puntenbeoordeling van het onderzochte onderdeel, waarmee de mate van compleetheid op het moment van de scan wordt weergegeven.
4) Bevindingen met een inhoudelijke toelichting bij de beoordeling.
5) In kwalitatieve termen een beoordeling van de risico's.
6) De maatregelen die getroffen kunnen worden om de risico's te verminderen.

De scan biedt meer dan sec een audit op de bovengenoemde onderdelen. De rapportage gaat - in samenhang - ook in op het informatiebeveiligingsbeleid, de organisatie van de informatiebeveiliging en op (onderdelen van) de risicoanalyse langs de lijn van organisatie, bedrijfsprocessen, gegevens, systemen en techniek.

Werkwijze en aanpak

De doorlooptijd van de scan hangt af van de beschikbaarheid van de medewerkers in het ziekenhuis. Doorgaans kunnen wij de scan in vier tot acht weken afnemen. Daarbij worden de volgende stappen doorlopen:

- Na opdrachtverstrekking vindt een kick-off plaats, waarbij alle praktische zaken worden besproken, zoals de beschikbare documentatie, de personen die geïnterviewd moeten worden, de site survey en de planning.
- De documenten worden geanalyseerd en de gespreksronde en site survey worden voorbereid.
- Op één dag worden de gesprekken gevoerd met de ziekenhuismedewerkers. Wie dat precies zijn, hangt af van de organisatie van het ziekenhuis. Daarnaast bezoeken wij een aantal locaties, zowel de ruimten met ICT-voorzieningen als andere ruimten in het ziekenhuis.
- Voor de oplevering van het definitieve rapport stellen wij een conceptrapport op, dat eerst met u wordt besproken.

Wat levert de Scan NEN 7510 u op?

De Scan NEN 7510 geeft u een heldere positiebepaling op de 23 belangrijkste onderdelen van de NEN-norm. U weet waar uw organisatie staat op het gebied van informatiebeveiliging en krijgt heldere suggesties en aanbevelingen om de informatiebeveiliging op een hoger plan te brengen. De adviseurs die de scan uitvoeren, beschikken over de kennis en ervaring om tot de kern van uw informatiebeveiliging door te dringen. Referenties van zowel binnen als buiten de zorg verstrekken wij u graag.

Wat is uw investering?

De investering voor de Scan NEN 7510 bedraagt € 7.500,- excl. btw.

Ook interessant voor u?

Uiteraard kunnen wij u ook ondersteunen bij het formuleren van het informatiebeveiligingsbeleid, het uitvoeren van businessimpactanalyses, het opstellen van risicoanalyses, en het prioriteren en implementeren van beveiligingsplannen.

Meer informatie

Wilt u gebruik maken van de Scan NEN 7510 of heeft u behoefte aan meer informatie? Neemt u dan contact op met drs. Patrick van Eekeren MCM, tel: (033) 4 220 220, e-mail: patrick.van.eekeren@mxi.nl of kijk op onze website www.mxi.nl.

M&I/Partners/

adviseurs voor management en informatie

Bijlage

Onderdelen die de Scan NEN7510 beoordeelt

Nr.	NVZ start-norm	Handboek NEN 7510	NEN 7510/7511 referentie	Onderdeel
1	√	√	5.1	Een informatiebeveiligingsbeleid is/wordt beschikbaar, geaccordeerd, nageleefd
2	√		6.1.1/ 6.1.2	Een informatiebeveiligingsproces is/wordt beschreven, ingericht en geborgd
3	√	√	6.1.3	Informatiebeveiliging is/wordt in de organisatie belegd (taken, bevoegdheden en verantwoordelijkheden)
4	√		6	Een risicoanalyse is/wordt uitgevoerd
5	√		6	Een informatiebeveiligingsplan is/komt beschikbaar en prioriteiten zijn/worden gesteld
6	√		6	De zeer hoog/hoog risicopunten worden in 2009 aangepakt
7	√	√	8.2.2	Het personeel is/wordt bewust van informatiebeveiliging (awareness)
8	√		9.1.2	De fysieke toegang tot de systemen is/wordt beveiligd
9	√		9.1/9.2	De computerruimten voldoen/gaan voldoen aan de norm
10	√	√	10.4.1	Een virusscanner is/wordt geïnstalleerd op servers en werkplekken
11	√		10.5.1	Backup- en restoreprocedures zijn/worden beschikbaar
12	√		10.6.1	Het netwerk beschikt over/verkrijgt hoge beschikbaarheid en voldoende snelheid
13	√		10.6.1	Het firewallbeheer is/wordt geregeld inclusief onderhoud
14		√	10.8.2	Overeenkomsten voor gegevensuitwisseling zijn/worden gesloten
15	√		10.8.8	Online beschikbare gegevens zijn/worden beveiligd en de verantwoordelijkheden zijn/worden belegd (indien van toepassing)
16	√	√	11.2.6/ 11.3	Autorisatie en wachtwoorden zijn/komen op orde
17	√		12.1.1/ 12.4.3/ 12.5.4	De technische achterdeuren in de informatiesystemen, het netwerk of andere systemen zijn/worden aantoonbaar gesloten
18		√	13.1.3	Continuïteitsbeheer is/wordt ontwikkeld/geïmplementeerd
19		√	14.1.2	Met intellectueel eigendom is/wordt rekening gehouden
20		√	14.1.3	Bedrijfsdocumenten zijn/worden beveiligd
21		√	14.1.4	Persoonsgegevens zijn/worden beschermd
22		√	14.2.1	Het beveiligingsbeleid wordt (op termijn) nageleefd
23		√	15.2.1	Een procedure voor het melden van beveiligingsincidenten is/wordt geïmplementeerd en de organisatie weet/komt te weten dat beveiligingsincidenten moeten worden gemeld