

Automatisering binnen de zorgsector, een nieuwe uitdaging, nieuwe kansen maar ook nieuwe risico's

Nederland digitaliseert en ook in de gezondheidszorg is digitalisering de sleutel naar verdere toekomstige ontwikkeling. Zeker in de gezondheidszorg speelt informatievoorziening een vitale rol. Efficiency & Workflow, Kostenbeheersing en Quality of Care hangen af van een adequate, efficiënte en complete maar vooral geïntegreerde informatie voorziening. De diversiteit en hoeveelheid van informatiesystemen, waar informatie van o.a. de patiënt wordt vastgelegd, maakt de zorg, wat informatiestromen betreft, tot een van de meest complexe sectoren in onze maatschappij.

Per 1 januari 2006 zullen in de zorgsector de Elektronische Medicatie Dossiers regio voor regio worden ingevoerd. Later zullen de Elektronische Patiënten Dossiers dezelfde digitale weg bewandelen.

Het digitaliseren en via de elektronische weg verspreiden van patiëntgegevens brengt nieuwe risico's en kwetsbaarheden met zich mee. Gegevens kunnen via ICT-netwerken aan derde worden verstrekt of openbaar worden gemaakt. Door adequate beveiligingsmaatregelen te treffen en zorg te dragen voor een goed ingerichte van uw ICT-omgeving kunnen deze risico's tot een minimum worden beperkt.

Het speerpunt bij de invoering van EMD's en EPD's zou ten allen tijden het waarborgen van de vertrouwelijkheid van medische en andere patiëntgegevens moeten zijn. De gevoeligheid van patiëntinformatie mag niet onderschikt worden aan de door de overheid opgelegde, noodzakelijke maar ook ingrijpende innovatie van de ICT in de zorgsector. Het beveiligen van persoonlijke informatie moet dan ook als harde eis gesteld worden bij het invoeren van EMD's en EPD's.

Het invoeren van EMD's en EPD's zal op den duur zeker een bijdrage leveren als het gaat om doelgerichte en efficiënte zorgverlening. Voordat de voordelen van het digitaliseren van gegevens merkbaar zullen dienen echter allereerst de randvoorwaarden goed ingericht te worden. Alleen door risico's in kaart te brengen en af te dekken kan een goede uitgangssituatie gecreëerd worden.

Secure Connection BV kan uw zorginstelling ondersteunen bij het inrichten van uw ICT-beveiliging en/of uw ICT-omgeving in het algemeen. Naast advisering kun wij uw organisatie ook operationeel ondersteunen bij het inrichten en het beheren van uw ICT-omgeving. Wilt u weten wat Secure Connection BV voor uw specifieke situaties en voor uw wensen en eisen kan betekenen? Neem dan vrijblijvend contact op met één van onze consultants.

Een op maat gesneden RemoteWerkplek beveiligingsadvies

Zoals al in onze nieuwsbrief van april dit jaar werd genoemd wordt mobiel werken steeds populairder en belangrijker. Organisaties die een architectuur willen gaan neerzetten die deze informatie-uitwisseling mogelijk maakt of al hebben uitgerold, worden geconfronteerd met de vraag welke risico's ze hiermee lopen en of de security eisen (B, I, V) vanuit de organisatie nog gewaarborgd zijn.

Met het kennisobject (remoteWerkplek) van Secure Connection kan een kwetsbaarheidsanalyse m.b.t. telewerken worden uitgevoerd. De interviewer heeft de mogelijkheid om een advies te vragen over een bestaand of een nieuw telewerkconcept.

Op basis van een bestaand telewerkconcept stelt het programma een beveiligingsadvies samen die aansluit bij de eisen van de organisatie. Hierbij wordt rekening gehouden met de volgende factoren:

De mate van gevoeligheid van de gegevens die worden verwerkt

De mate waarin het telewerkconcept zoals dit bij de organisatie zal worden uitgerold kwetsbaar is voor aantasting van het vereiste niveau van beschikbaarheid, integriteit en vertrouwelijkheid

Met betrekking tot de eerste factor wordt gevraagd naar de mate van vertrouwelijkheid van de gegevens die door de telewerkers worden verwerkt. In de analyse wordt rekening gehouden met de hoogste klasse van vertrouwelijkheid van de gegevens die worden verwerkt. Met betrekking tot de tweede factor wordt gevraagd naar een groot aantal kenmerken van het telewerkconcept, zoals:

De gekozen technologie (PPTP/L2TP/IPSEC/SSL VPN, inbelfaciliteit)

Architectuur van de werkplek: remote control (o.b.v. "thin client")/ remote node

Locatie waar de remote werkplek wordt ingezet

De faciliteiten die de telewerker wordt geboden

De aard van de PC waarop het telewerken plaatsvindt

De aard van de werkzaamheden die door de telewerker wordt uitgevoerd

Op basis van de security eisen vanuit de organisatie en de eisen en wensen m.b.t. de architectuur kan een kwetsbaarheidsanalyse worden uitgevoerd. Afhankelijk van de gekozen oplossing adviseert het programma naast organisatorische maatregelen, ook voor de betrokken componenten (OS, FW, encryptie, authenticatie, VPN client, ICA, RDP, etc) technische maatregelen die de eisen met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid kunnen afdekken.

Secure Connection geeft op verzoek een demonstratie van dit en desgewenst andere kennisobjecten of tools. Als u hier meer over wilt weten kunt contact opnemen met één van onze consultants.

Actueel

6 september 2005

"Extra beveiliging patiëntgegevens"

DEN HAAG Minister Hoogervorst neemt maatregelen om digitale informatie over patiënten te beschermen. Ziekenhuizen moeten mogelijk aan dezelfde wettelijke eisen voldoen als banken moeten voor het beveiligen van hun klantgegevens.

Begin volgend jaar begint in een aantal regio's een nieuw registratiesysteem van patiëntgegevens. De minister zegt dat het systeem pas wordt ingevoerd als de veiligheid goed is geregeld.

Vorige week bleek dat hackers eenvoudig de gegevens van een miljoen patiënten konden inzien en veranderen. De hackers hadden toestemming van de ziekenhuizen om te kijken hoe makkelijk dat kon.

Bron: www.nos.nl