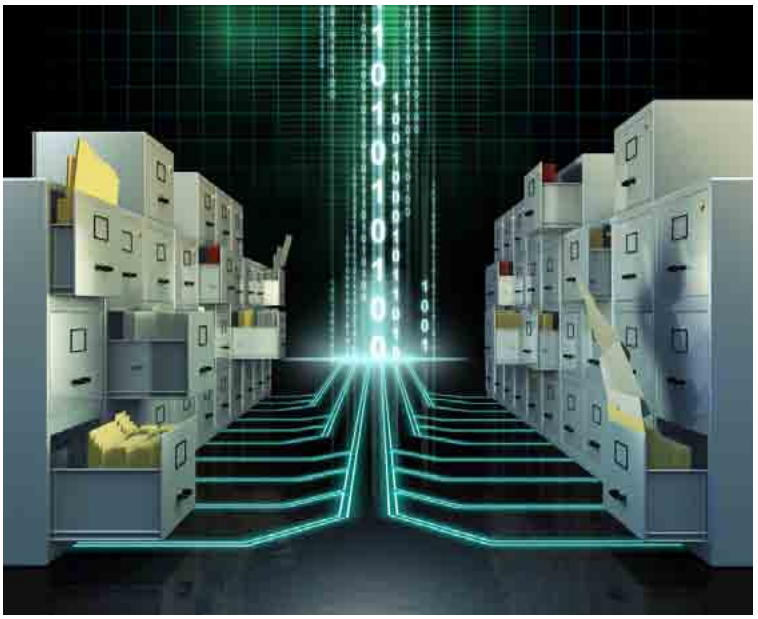
Wat is het Panacee voor informatiebeveiliging?

Waarom verloopt het beveiligen van informatie in de zorg vaak moeizaam? Ligt dat aan het digitale Elektronische Cliënten (oftewel Patiënten) Dossier dat bijvoorbeeld niet de mogelijkheid biedt om (privacy) classificaties te geven aan gegevens. Of zijn medewerkers binnen de instelling zich in mindere mate bewust van de gevoeligheid van cliënten- c.q patiëntengegevens? Zorginstellingen hebben informatiebeveiliging vaak niet als prioriteit op de agenda staan, totdat het te laat is! Ook hier geldt 'voorkomen is beter dan genezen' en een panacee is nodig. Interessant is daarom te weten welke middelen absoluut in het panacee voor moeten komen.



Het heeft weinig zin strikte regels in te voeren voor de opbouw van veilige wachtwoorden als gebruikers deze uit gemak op hun scherm plakken of opschrijven op hun werkblad of gegevens op USB-sticks opslaan . Ook heeft het weinig effect cliëntgegevens met de hoogste veiligheidsclassificatie weg te schrijven in de ECD-database (=Elektronisch Cliënt Dossier) als medisch- en zorg personeel ordners op hun werkplek laten liggen. Of als kasten met medische gegevens op de gang worden gezet omdat er nergens anders plaats is. Het is dus meer dan alleen het op orde hebben van de IT-omgeving . Informatiebeveiliging raakt (helaas) alle aspecten van de bedrijfsvoering en heeft in hoge mate te maken met bewustwording.

Pas op voor de 'papieren tijger'

Informatieveiligheid heeft in de praktijk te maken met drie aspecten die met elkaar in verband staan namelijk maatregelen, organisatie en bewustwording (awareness). Alleen als deze drie aspecten in balans zijn, kan een blijvende en onderhoudbare informatieveiligheid worden gecreëerd.

Het integraal verhogen van de informatieveiligheid is te vergelijken met de introductie van een nieuw bedrijfsproces en raakt daardoor de gehele organisatie. Het is een volwaardig project waar namen en verantwoordelijkheden aan gekoppeld moeten worden en waar tijd en ruimte voor vrij gemaakt moet worden. Informatieveiligheid gaat ook over het maken van keuzes, die niet altijd populair zijn onder gebruikers. Informatiebeveiligers dienen daarom mandaat te krijgen van de directie om deze keuzes te maken, anders wordt informatiebeveiliging al snel een papieren tijger. Daarnaast is informatiebeveiliging geen vrijblijvendheid: de overheid heeft de normering hiervoor (NEN7510) van kracht verklaard voor de gehele sector.

Maar awareness kan niet overnacht gecreëerd worden. Het is een proces van jaren waarin medewerkers die omgaan met gevoelige informatie bewust dienen te worden gemaakt van de risico's van een slechte informatieveiligheid. En daar ligt in de praktijk het probleem.

Vaak zetten zorginstellingen het thema informatiebeveiliging pas serieus op de agenda als er dwang bestaat vanuit de overheid of als zich een aantal incidenten hebben voorgedaan die de aandacht trekken van de directie. Informatiebeveiliging wordt dan (vaak) behandeld als een IT project met een begin en een einde. Niet zelden ligt het initiatief hiertoe ook binnen de IT afdeling, wat de associatie van informatieveiligheid met IT alleen maar doet toenemen.

Gebruikersgemak versus beveiliging

Er bestaat een directe relatie tussen informatieveiligheid en gebruikersgemak. Een hoger gebruikersgemak komt de veiligheid vaak niet ten goede en vice versa. Gebruikers zien weliswaar het nut in van informatieveiligheid, maar willen daar in het dagelijks gebruik zo min mogelijk hinder van ondervinden. Informatiebeveiligers dienen een balans tussen beide aspecten na te streven en daar ook door de directie in te worden gesteund. Een praktijkvoorbeeld is de tijdsinstelling van beeldscherm beveiliging. Gebruikers vinden dat hinderlijk, maar het is een effectieve maatregel om ongewenste toegang te voorkomen.

Wat zijn de standaarden?

Dé standaard voor informatiebeveiliging in de zorg in Nederland is de NEN7510-2011 met daaraan gekoppeld een aantal aanvullende normen zoals de NEN7521: toegang tot patiëntgegevens. Strikt genomen is de NEN7510 geen norm, maar meer een kader. Het begrip norm doet vermoeden dat het hier een set regels betreft die ingevoerd moeten worden, waarna de organisatie zoals dat zo mooi heet 'NEN7510-compliant' is. De vergelijking met normen als die voor afmetingen van ziekenhuisbedden dringt zich daarbij op.

In werkelijk is de NEN7510 echter niets van dat alles. Het betreft meer een leidraad om de informatieveiligheid binnen een willekeurige zorginstelling op orde te krijgen. Daarbij worden tools en materialen aangereikt die gebruikt kunnen worden om dat doel te bereiken. Een van die tools is een uitgebreide set (ca. 400) van maatregelen in 11 categorieën die kunnen helpen om een grotere informatieveiligheid te verkrijgen. Welke van die maatregelen daadwerkelijk uitgevoerd dienen te worden is echter aan de zorginstelling zélf. Enige voorwaarde is dat het proces om tot een hoger veiligheidsniveau te komen (iteratief) doorlopen dient te worden. Dit proces, het ISMS (Information Security Management System), is tevens het enige waarvoor een instelling gecertificeerd kan worden. Het vergt een gedegen voorbereiding en blijvende aandacht gedurende lange tijd.

Pragmatische aanpak

Zorginstellingen die opzien tegen een grootse aanpak bij de introductie van het ISMS doen er goed aan een weloverwogen stappenplan voor informatiebeveiliging te maken over een langere periode (bijvoorbeeld 2 à 3 jaar) en hieraan vast te houden. De betekenis van blijvend commitment van de directie kan daarbij niet overschat worden.

Een mogelijk stappenplan ziet er als volgt uit:

1. Zorg voor commitment van de directie voor de te nemen stappen en betrek de directie nadrukkelijk in het proces.
2. Bepaal een basis-set (baseline) aan maatregelen die minimaal gerealiseerd dient te worden om een basis veiligheidsniveau te verkrijgen. Neem daarbij de NEN7510 als leidraad.
3. Zet een organisatie op rondom informatiebeveiliging die met deze baseline aan de slag gaat en besteed de nodige aandacht aan rollen en verantwoordelijkheden. Verkrijg mandaat hiervoor bij de directie!
4. Start een interne campagne om awareness van de gebruikers geleidelijk te verhogen en doe dit over een langere periode.
5. Claim een informatie-gerelateerd project; de invoering van een (nieuw) ECD is in die zin optimaal. Een dergelijk project heeft een grote impact op de gehele organisatie. Het laten meeliften van het thema informatiebeveiliging heeft daarom niet alleen een praktisch effect, voldoen aan de eisen wat betreft omgang met cliëntgegevens, maar zorgt tevens voor een hogere awareness bij alle betrokkenen.

Tot slot: 'Neem de tijd en houd vol'! Organisaties dienen volhardend te zijn in het streven naar de invoering van informatiebeveiliging.