

# Zorginstellingen staan voor INFORMATIEBEVEILIGING IS MÉÉR DAN TECHNIEK ALLEEN

**Ter ondersteuning van het zorgproces worden steeds vaker IT-middelen ingezet. Dat heeft gevolgen voor de manier waarop er met informatie wordt omgegaan. Om die informatie op alle niveaus te kunnen beschermen, is het van belang dat beveiligingsmaatregelen verder reiken dan technologische ingrepen alleen. Daarbij dienen de organisatorische en procedurele aspecten van informatiebeveiliging zeker zo veel aandacht te krijgen.** CORNÉ DE KEIZER

## NEN 7510

De kwaliteitscriteria waaraan informatiebeveiligingsmaatregelen in de zorg moeten voldoen, zijn beschreven in de NEN 7510. Deze norm, beheerd door het Nederlands Normalisatie-instituut (NEN), vereist tevens dat deze maatregelen op controleerbare wijze zijn ingericht voordat kan worden gesproken over adequate informatiebeveiliging.

(Bron: [www.nen7510.org](http://www.nen7510.org))

**E**en groot deel van de dagelijkse taken van een zorgprofessional bestaat uit het nemen van beslissingen. Welke specifieke medicijnen krijgt een patiënt? Krijgt hij wel of geen extra bloedonderzoek? Beslissingen naar aanleiding van dit soort vragen worden genomen op basis van de beschikbare informatie. De kwaliteit van patiëntinformatie is daarom letterlijk van levensbelang.

In de zorg wordt al jaren gebruikgemaakt van IT om de zorgprocessen te ondersteunen en van informatie te voorzien. Daar waar IT-middelen in het verleden slechts een ondersteunende rol vervulden, kunnen we tegenwoordig constateren dat de afhankelijkheid van IT almaar groter wordt. Dit zien we onder meer terug in het steeds concreter wordende elektronisch patiëntendossier (EPD).

Met de toename van IT-toepassingen worden systemen steeds vaker gekoppeld en aangesloten op het netwerk. Röntgenfoto's, MRI-systemen, bloed- en andere onderzoeksuitslagen: al deze gegevens dienen op ieder gewenst moment beschikbaar te zijn om bijvoorbeeld een diagnose te kunnen stellen of een behandelplan te maken.

Als gevolg van de door de branche gevraagde koppelingen wordt binnen de aanwezige IT-systemen, maar

ook door medische apparatuur als MRI-scanners, in toenemende mate gebruikgemaakt van open systemen en open standaarden. Moderne medische apparatuur werkt veelal met open standaarden als TCP/IP. Daar waar systemen nog proprietary (oftewel fabrikantspecifiek) zijn, is het met een specifieke interface vaak toch mogelijk een koppeling te maken met een open systeem. Denk bijvoorbeeld aan het 'gesloten' Radiology Information System (RIS), dat via specifieke gatewaysoftware gekoppeld wordt aan het open Picture Archiving and Communications System (PACS).

De ontwikkelingen op dit gebied gaan snel. Behalve de aan de zorg gelieerde partijen willen ook grote softwarebedrijven als Microsoft een plaats veroveren in de zorgbranche. Zo biedt de softwaregigant uit Redmond inmiddels een speciale productfamilie voor de zorg aan, waaronder een compleet ziekenhuisinformatiesysteem (ZIS), inclusief een RIS en een PACS.

Daarnaast wordt de wens om systemen van de diverse zorgpartijen te koppelen steeds groter. Momenteel wordt daar op kleine schaal gebruik van gemaakt. Denk bijvoorbeeld aan huisartsen die informatie in het EPD van een regionaal ziekenhuis kunnen inzien. Maar dit is slechts het begin.

Ook systemen van bijvoorbeeld zorgverzekeraars of andere zorgpartners kunnen worden gekoppeld.

## Risico's

De ontwikkeling van internet-technologie maakt dat de grenzen tussen intern (binnen de instelling) en extern (huisartsen, zorgpartners, internet) vervagen. Maar met het veranderen van de situatie veranderen de risico's eveneens. Dit heeft vergaande gevolgen voor de betrouwbaarheid van de binnen de IT-systemen verwerkte patiëntgegevens. Denk daarbij aan configuratiefouten of een onzorgvuldig afgeschermd dataopslagsysteem dat onbedoeld online wordt gezet.

Voorbeeld: een ziekenhuis maakt gebruik van een ZIS waarin op een bepaald moment een beveiligingslek wordt ontdekt. In korte tijd wordt door de fabrikant een securitypatch ontwikkeld, waarmee het beveiligingslek ongedaan wordt gemaakt. Echter, wegens omstandigheden is het ziekenhuis niet in staat deze patch te draaien. Daardoor is het systeem gedurende enkele maanden kwetsbaar voor gerichte aanvallen. Zo kan het volledige ZIS worden overgenomen door een kwaadwillende. Een gevolg kan zijn dat het systeem vastloopt, waardoor de zorgverlening stilvalt. Maar het kan ook zo zijn dat een gedeelte van de gegevens wordt gewist, waardoor het bijvoorbeeld niet langer mogelijk is een correcte diagnose te stellen. Daarnaast bestaat de mogelijkheid dat gevoelige patiëntinformatie op straat komt te liggen. De vraag

*Zorginstellingen hebben de verantwoordelijkheid de aanwezige risico's te kennen en ernaar te handelen*

# nieuwe uitdaging

is niet hoe groot deze kans is, maar of een zorginstelling dit soort risico's überhaupt wil lopen. Hoewel het antwoord over het algemeen 'nee' zal zijn, suggereren de huidige ontwikkelingen het tegenovergestelde. Het is daarom belangrijk dat een zorginstelling de risico's kent en onder ogen durft te zien.

Het koppelen van systemen en medische apparatuur via het netwerk en het gebruik van open systemen en standaarden brengt extra risico's op het gebied van betrouwbaarheid met zich mee (zie kader). Deze risico's zijn altijd te herleiden tot een of meer van de drie kerngebieden van informatiebeveiliging. Deze kerngebieden zijn:

- **Beschikbaarheid.** Informatie dient op het juiste moment beschikbaar te zijn. Bij de voorbereiding of uitvoering van een operatie is het van groot belang dat de behandelend artsen toegang hebben tot de patiëntgegevens. De al dan niet elektronische informatiesystemen dienen dan ook altijd in de lucht te zijn. Dat brengt de nodige maatregelen met zich mee.

- **Integriteit.** Integriteit van informatie wil zeggen dat de informatie correct en compleet is. De medewerker die data in het systeem invoert, is hiervoor grotendeels verantwoordelijk. Denk hierbij aan bloedwaarden, gewicht van een patiënt, bepaalde afwijkingen, etc. Dit zijn gegevens die van belang kunnen zijn bij het stellen van een juiste diagnose. Onbewust onjuiste of incomplete invoer (bijvoorbeeld het vergeten te vermelden van een penicillineallergie) kan grote gevolgen hebben en in sommige gevallen zelfs levensbedreigende situaties veroorzaken.

- **Vertrouwelijkheid.** Het spreekt voor zich dat onbevoegden patiëntinformatie niet mogen inzien. In Nederland is hier voldoende wetgeving voor en ook zorginstellingen besteden er veel aandacht aan. Toch zijn sommigen bijzonder geïnteresseerd in de medische gegevens van bepaalde personen. Denk bijvoorbeeld aan iemand van de roddelpers die graag wil weten of een bekende presentator een psychiater is verleden heeft, of wil uitzoe-

ken of dat ene soapsterretje nu wel of niet zwanger is.

Een zorginstelling dient dus van tevoren te bepalen wat het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid van een informatiesysteem moet zijn. De informatie die de roddeljournalist in bovenstaand voorbeeld nodig heeft, ligt vast in het EPD. Het is de roddeljournalist in dit geval natuurlijk niet te doen om het hacken van een pc. Hij is op zoek naar iets dat waardevoller is voor hem: medische informatie van een bekende Nederlander. Op het moment dat informatie bijvoorbeeld via een eenvoudig telefoontje te achterhalen is, wordt de volledige technische beveiliging omzeild.

Het achterhalen van informatie door middel van manipulatie en misleiding van mensen – ook wel social engineering genoemd – komt steeds vaker voor. Doordat er meer en meer technische barrières worden opgeworpen, wordt het voor kwaadwillenden steeds moeilijker via computersystemen de benodigde informatie te achterhalen. In dat geval is social engineering een relatief eenvoudige methode om toch de juiste informatie te verkrijgen: er zijn namelijk geen technische hoogstandjes voor nodig. Het is daarom van groot belang informatiebeveiliging in een breder perspectief te plaatsen dan alleen het nemen van technische maatregelen.

Zorginstellingen hebben de verantwoordelijkheid de aanwezige risico's

*Meestal is er veel aandacht voor techniek, terwijl het organisatorische aspect en het gedragsaspect onderbelicht blijven*

te kennen en ernaar te handelen. Risico's dienen dan ook teruggebracht te worden tot een aanvaardbaar niveau. Daarom moet een zorginstelling op basis van risicoanalyses passende maatregelen treffen.

## Maatregelen

Het nemen van maatregelen reikt verder dan het installeren van een aantal beveiligingsproducten. Het is

## PATCHES EN UPDATES

**M**oderne medische apparatuur is veelal gebaseerd op open systemen en open standaarden. Verzamelde data uit medische apparatuur worden direct in deze systemen opgeslagen. Daarbij maakt men gebruik van besturingsystemen als Windows en Linux. Daarnaast worden deze systemen ook nog eens gekoppeld aan een netwerk.

De belangen van fabrikanten zijn in dit geval driedelig. In eerste instantie moet het correct functioneren van de apparatuur gegarandeerd worden (beschikbaarheid). Vervolgens dient alle verzamelde informatie correct te worden verwerkt (integriteit) en alleen beschikbaar te zijn voor geautoriseerde personen (vertrouwelijkheid).

Het probleem ligt bij de achterliggende systemen. Doordat men gebruikmaakt van open systemen en standaarden dient de apparatuur (zeer) regelmatig voorzien te worden van de laatste securitypatches en updates. Fabrikanten zijn echter terughoudend in het installeren van deze updates omdat een update het correcte functioneren van de apparatuur kan beïnvloeden. Dat houdt in dat er een bepaalde tijdspanne aanwezig is tussen het moment van het verschijnen van de update en het moment dat de fabrikant een update daadwerkelijk vrijgeeft. Juist in deze tussenliggende periode is de aanwezige informatie zeer kwetsbaar voor mogelijke aanvallen. Dit betekent een extra risico voor de zorginstelling en vooral voor de patiëntveiligheid.

zelfs meer dan alleen het uitvoeren van een heel project. Maatregelen dienen als processen te worden geïmplementeerd binnen de organisatie. Dat is niet

eenvoudig, maar wel een must voor het succes van de informatiebeveiliging – en daarmee van de kwaliteit van de zorgverlening en de patiëntveiligheid. Juist bij het inrichten van die processen zal blijken dat informatiebeveiliging meer is dan IT alleen. Het juiste niveau van informatiebeveiliging kan pas worden bereikt als in alle werkprocessen op de juiste manier met informatie wordt omgegaan. Dat kan alleen door een

## Verdedigingslaag Kenmerk beveiliging

## Beleid, procedures en bewustwording

De basis van informatiebeveiliging wordt gevormd door beleid en procedures. Dit beleid en de bijbehorende procedures zijn opgesteld op basis van een gedegen norm. In de zorg is dat de NEN 7510. Hiermee is de basis gelegd voor de overige verdedigingslagen. Het juiste niveau van vertrouwelijkheid, integriteit en beschikbaarheid van de omgeving wordt aan de hand van zowel de norm als de binnen de instelling aanwezige risico's benoemd. Op basis hiervan zijn maatregelen beschreven en geïmplementeerd binnen de organisatie.

De praktijk leert dat deze laag veelal minimale aandacht krijgt en dat er vaak wordt gekozen voor maatregelen op basis van onderbuikgevoel en zonder gedegen onderbouwing.

Het is van groot belang dat medewerkers van een zorginstelling weten wat het informatiebeveiligingsbeleid inhoudt, welke procedures hiervoor gelden en wat de noodzaak ervan is. Uiteraard dient men zich er ook naar te gedragen. Grote winst kan worden behaald in het aanleren van veilige procedures. Bewustwordingssessies voor medewerkers blijken in de praktijk een minimaal effect te hebben. Door energie te steken in het aanpassen van de procedures en deze strikt door te voeren binnen een afdeling, kan het gewenste effect worden bereikt, namelijk het afdwingen van het veilig omgaan met patiëntgegevens.

## Fysieke beveiliging

Fysieke beveiliging is een van de basisbenodigheden voor een complete beveiliging. De aanwezigheid van beveiligingsmedewerkers is hier een voorbeeld van. Maar denk bijvoorbeeld ook aan het in kaart brengen van de ruimten die alleen toegankelijk zouden mogen zijn voor geautoriseerd personeel. Daarnaast moet voor de technische ruimten gezorgd worden voor overspanningsbeveiliging en airconditioning.

Voor papieren gegevens wordt gebruikgemaakt van afgesloten kasten, archieven of een kluis. Maar ook een papiervernietiger is een typisch voorbeeld van een fysieke beveiligingsmaatregel.

## Logische beveiliging

De logische beveiliging van de omgeving is onderverdeeld in een vijftal lagen:

- **Perimeter** De koppeling naar het internet en naar eventuele andere netwerken wordt beveiligd door een enterprise-firewallomgeving, aangevuld met Intrusion Detection & Prevention. Op de perimeter wordt proactief beheer uitgevoerd zodat de bescherming te allen tijde optimaal is.

- **Intern netwerk** De interne omgeving is gesegmenteerd zodat de verschillende communicatiestromen beveiligd worden. Niet alle gebruikers kunnen zomaar bij alle informatie en systemen.

- **Host** De besturingssystemen worden met grote regelmaat up-to-date gehouden door middel van de laatste securitypatches. Proactief beheer en het doorlopend monitoren van systemen zijn voorbeelden van toegepaste beveiligingsmaatregelen.

- **Applicatie** Applicaties dienen afdoende beveiligd te zijn. Authenticatie dient bijvoorbeeld op een veilige manier plaats te vinden. Gebruikers loggen voor specifieke toepassingen in met behulp van een secure token of smartcard. Zo kunnen alleen geautoriseerde gebruikers toegang krijgen tot de ter beschikking gestelde applicaties en de bijbehorende data. Verkeer tussen de applicatie en de gebruikerswerkplek is versleuteld, bijvoorbeeld via SSL. Daarnaast dienen applicaties regelmatig te worden gepatcht en getoetst op mogelijke kwetsbaarheden door middel van bijvoorbeeld ethical hacks.

- **Encryptie** De uiteindelijke data van de omgeving worden op een veilige manier verwerkt en opgeslagen. Encryptie van vertrouwelijke data tijdens transport (e-mail) en opslag vervult hierbij een sleutelrol.

combinatie van beleid, procedures, techniek en, niet in de laatste plaats, bewustzijn bij de medewerkers.

Informatiebeveiliging wordt meestal ingevuld aan de hand van een Defense in Depth-strategie (zie afbeelding 1). Deze strategie is gebaseerd op de aloude stelregel 'de keten is zo sterk als de zwakste schakel'. De beveiliging van een organisatie en haar informatie bestaat uit een keten van maatregelen die elkaar aanvullen en versterken. De toepassing van de Defense in Depth-strategie biedt de zekerheid die een kwalitatief hoogwaardige beveiligingsomgeving nodig heeft.

Het basisprincipe van de Defense in Depth-aanpak is dat informatie een drietal verschijningsvormen kent:

- **Elektronische informatie.** Dit is alle elektronisch verwerkte en/of opgeslagen data binnen de zorginstelling. Denk hierbij aan e-mails, het EPD, bestanden op servers, bestanden op USB-sticks, etc.

- **Fysieke informatie.** Hieronder vallen alle dossiers, documenten, brieven, uitgeprinte e-mails, memo's, tekeningen, schema's, etc. Fysieke informatie is bijvoorbeeld ook een röntgenfoto of een afdruk van een echoscopie. Maar ook gegevens die op een whiteboard

blijven staan na een patiëntbespreking, of een aantekeningenvel dat in de prullenbak wordt gegooid.

- **Niet-tastbare informatie.** Dit is een van de lastigst te beheren vormen van informatie. Binnen een organisatie is veel kennis aanwezig bij de medewerkers. Deze in het hoofd aanwezige kennis is niet tastbaar maar vormt een belangrijk onderdeel van de organisatie. Al deze informatie kent een bepaalde mate van vertrouwelijkheid. Het is aan de medewerker daar verantwoordelijk mee om te gaan.

Om deze drie vormen van informatie te beschermen zijn meerdere verdedigingslagen nodig. Iedere laag heeft zijn eigen specifieke kenmerken. In tabel hiernaast worden de verdedigingslagen beknopt toegelicht.

**Drie pijlers**

Van de gerealiseerde processen dienen opzet, bestaan en werking aangetoond te kunnen worden. Hiervoor hanteert de NEN 7510 de Plan-Do-Check-Act-cyclus. Binnen veel organisaties zijn de onderdelen Plan en Do zonder meer uitvoerbaar – in de vorm van de initiële implementatie van een maatregel. De Check- en Act-activiteiten worden daarna óf vergeten óf krijgen minder prioriteit door de drukte van alledag.

Het mooie van de NEN 7510 is dat ook hier een aanpak wordt gepropageerd die verder gaat dan de IT alleen. Van de elf aandachtsgebieden binnen de norm zijn er slechts een aantal gericht op IT-maatregelen. De overige hoofdstukken gaan over beleid, personeel, wetgeving en de wijze waarop procedures zijn geïmplementeerd binnen de instelling.

Bij een succesvol informatiebeveiligingsbeleid zijn een drietal pijlers te onderscheiden, die alle drie een gelijk belang hebben (zie afbeelding 2). In de praktijk is vaak een scheefgroei te zien tussen de drie pijlers. Meestal is er veel aandacht voor techniek, terwijl het organisatorische aspect en het gedragsaspect onderbelicht blijven.

Organisatorische maatregelen zijn vaak terug te voeren op beleid en procedures. Hier is binnen de NEN 7510 veel aandacht voor. Procedures op de werkvloer gericht op

informatiebeveiliging worden vaak vergeten in een zorginstelling. Op zich is dat vreemd. Als het om expliciet medische handelingen gaat zijn er procedures te over, maar als het om informatiebeveiliging gaat, schiet men nogal eens tekort. Toch zijn beide zaken onlosmakelijk met elkaar verbonden. In het volgende voorbeeld komt dit duidelijk naar voren. Het inbrengen van een infuus bij een patiënt is een zogenaamde voorbehouden handeling. Dit mag niet zomaar door een willekeurige

Deze procedure heeft een belangrijke reden: op het moment dat iemand die niet bevoegd en bekwaam is een dergelijke medische handeling uitvoert, kan dit grote gevolgen hebben en in sommige gevallen zelfs levensbedreigend zijn. Het niet correct of incompleet bijhouden van gegevens in een EPD kan echter eveneens desastreuze gevolgen hebben. Toch wordt van medisch personeel niet verwacht een aantoonbaar kennisniveau te hebben op het gebied van de voor hen relevante IT-middelen. Een

*Het juiste niveau van informatiebeveiliging kan pas worden bereikt als in alle werkprocessen op de juiste manier met informatie wordt omgegaan*

verpleegkundige worden uitgevoerd; de verpleegkundige moet bevoegd en bekwaam zijn. Hiervoor dient in eerste instantie een cursus gevolgd te worden. Na afronding van de cursus mag de verpleegkundige eerst alleen onder begeleiding een infuus aanleggen. Nadat dit meerdere malen onder begeleiding en naar tevredenheid van de begeleider (aantoonbaar met handtekeningen) is gedaan, wordt de verpleegkundige bevoegd én bekwaam geacht zelfstandig een infuus in te brengen.

cursusmiddag met hooguit verplichte aanwezigheid is in veel instellingen voldoende om het systeem te mogen bedienen.

Om het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie te kunnen realiseren, zijn, zoals eerder besproken, allerlei technische maatregelen nodig. Het is van groot belang de maatregelen te kiezen die passen bij de bijbehorende informatie.

Gedrag en houding, ten slotte, zijn altijd afhankelijk van de mensen

## CONCLUSIE

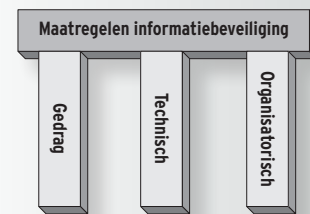
Fabrikanten van medische systemen zijn er zonder meer verantwoordelijk voor hun systemen zo veilig mogelijk te maken en de systemen te behoeden voor allerlei gevaren. De praktijk leert dat een aantal fabrikanten hier concreet invulling aan geeft. Windows-gebaseerde systemen worden bijvoorbeeld 'gehardend' en uitgerust met virusscanners. Het is echter de verantwoordelijkheid van de zorginstelling erop toe te zien wie er allemaal toegang krijgt tot het systeem. Het voorkomen van toegang door onbevoegden met een 'gevonden'

wachtwoord dient te zijn geregeld door de zorginstelling zelf.

Daarom is het nodig dat een zorginstelling de zorgprocessen en daarmee de onderliggende informatievoorziening (en dus de informatiesystemen) aantoonbaar onder controle heeft. Draagvlak én een duidelijk sturende rol vanuit het hoger management voor processen rondom het waarborgen van de informatievoorziening zijn essentieel voor het 'in control' zijn. Dat zal uiteindelijk leiden tot een verbetering van de zorgprocessen en de patiëntveiligheid binnen de zorginstelling.



Afbeelding 1. De Defense in Depth-strategie



Afbeelding 2. Pijlers van informatiebeveiliging

die met de informatie werken. Dit betekent dat de rol van het management (zowel het hoger management als het afdelingsmanagement) cruciaal is voor het succes van het integreren van informatiebeveiliging binnen de processen.

Uiteindelijk blijft het niet bij het eenmalig uitvoeren van een project. Juist een periodieke review (Check) en het definiëren van vervolgacties (Act) zijn nodig om een continue verbetering van het niveau van informatiebeveiliging te bewerkstelligen. Dit klinkt eenvoudig, maar toch blijkt het voor veel organisaties moeilijk om hier tijd en geld voor vrij te maken. Vooral als zich in de afgelopen periode geen serieuze incidenten hebben voorgedaan (of niet bekend is dat die zich hebben voorgedaan) worden de Check- en Act-stappen gemakkelijk doorgeschoven tot het moment dat een incident zich daadwerkelijk voordoet. ●

Corné de Keizer CISPP, CISA is securityconsultant bij Motiv in IJsselstijn. Daarnaast is hij lid van de Commissie Informatiebeveiliging van de NVMA Vereniging voor Zorgadministratie en Informatie.