

Beveiliging voor de Zorg

•

Zorg voor Beveiliging

18 juni 2009

Samenvatting

De NEN 7510-familie is een verzameling van normen op het gebied van informatiebeveiliging voor instellingen in de gezondheidszorg. Dit document beoogt hulp te bieden bij een hands-on aanpak voor het voldoen aan dit normenstelsel. Centraal doel is grip krijgen en houden op informatie en processen, en dan met name de beveiliging daarvan.

Dit rapport is tot stand gekomen met inbreng van:

- M. van Eemeren, ON2IT b.v., Waardenburg, marcelvaneemeren@on2it.eu;
- dr. N. S. Hekster, IBM Nederland b.v., Amsterdam, n.s.hekster@nl.ibm.com;
- O. Nillesen Msc, Lloyd's Register Quality Assurance (LQRA), Rotterdam, onno.nillesen@lr.org;
- dr. J. Popping, J.P. Adviesbureau, jpadviesbureau@cs.com;
- drs. J. Scheerder, ON2IT b.v., Waardenburg, js@on2it.net.

Inhoudsopgave

1	Veilige zorg = veilige informatie	4
1.1	Vele en grote risico's	4
1.2	Informatiebeveiliging	4
1.3	Informatiebeveiliging is specialistenwerk	5
2	Uit de praktijk gegrepen	6
3	Informatievoorziening in de zorg	7
3.1	NEN 7510	7
3.2	NEN 7511: Toetsbare voorschriften	7
3.3	Implementatie van NEN 7511	8
3.4	NEN 7512: Vertrouwensbasis voor gegevensuitwisseling	8
4	Voldoen aan NEN-normen	10
4.1	P D C A	10
4.2	Organisatie en bedrijfsprocessen	10
4.2.1	Organisatie rollen	10
4.2.2	Bedrijfsprocessen	11
4.3	Technische invulling	14
4.3.1	Strategisch beleid en planning	14
4.3.2	Operationeel beleid en effectuering	15
4.3.3	Verslaglegging en meting	17
4.3.4	Evaluatie en analyse	17
4.4	Op weg naar NEN-compliance	17
4.5	Technische oplossingen	20
4.5.1	Plan	20
4.5.2	Do	20
4.5.3	Check	22
4.5.4	Act	23
5	Certificatie/Compliance NEN 7510	24
5.1	Aanpak	24
5.2	Risicomanagement	24
5.3	Traject	25
5.4	Resultaat	27
6	Samenvatting en conclusie	28
	Index	28

1 Veilige zorg = veilige informatie

Zorg is mensenwerk, maar bij het medisch handelen en de zorgverlening speelt de kwaliteit van informatie en daarmee ICT infrastructuur, een sleutelrol. Recente rapporten van de Inspectie voor de Gezondheidszorg over een onderzoek bij 20 ziekenhuizen, berichten van het Ministerie van VWS, t/m 1735 vermijdbare sterfgevallen (1) tonen opnieuw aan, dat er zowel op zorg- als informatiegebied, nog veel te verbeteren valt.

De afhankelijkheid van adequate ICT voorzieningen is groot en groeiende door de invoering elektronische dossiers, zorgnetwerken, telewerken etc. De kwaliteit van informatie (beschikbaarheid, integriteit, vertrouwelijkheid) vergt steeds meer bescherming tegen chronische en acute risicosituaties. Daartoe stelt de overheid eisen aan goed beheerde zorgsystemen (GBZ) en bestaan er normen voor informatiebeveiliging in de zorg (NEN7510), waaraan voldaan moet worden.

1.1 Vele en grote risico's

Uw ICT systeem is helaas niet immuun voor interne en externe gevaren. Het wordt doorlopend op de proef gesteld door de invoering van specifieke, nieuwe zorg- en andere toepassingen, integratie met bestaande applicaties, ketenautomatisering (meerdere zorgprocessen, soms instellingsoverschrijdend), faciliteiten voor tele- en thuiswerken, etc.

Daarbij komen toenemende externe bedreigingen, vaak aangeduid met virussen, wormen, trojaanse paarden, hackers, malware, gepersonaliseerde spam- en phishing-berichten en andere vormen van cybercrime.

Een andere bron wordt gevormd door semi-zakelijke- of privé - toepassingen zoals webmail (hotmail), video (bijv. YouTube), VOIP (Skype, MSN), "googelen", instant messaging en andere vormen van social networking, waarbij vaak persoonlijke gegevens worden prijsgegeven. Ook cliënten- en patiënteninformatie wordt soms onbedoeld publiek gemaakt, hetgeen kan leiden tot identiteitsdiefstal.

Besmetting van buiten en menselijke onachtzaamheid kunnen de beschikbaarheid en kwaliteit van bedrijfsgegevens ernstig aantasten, terwijl veilige informatie in de zorg van levensbelang is.

1.2 Informatiebeveiliging

Veilige zorg vereist veilige informatie en daarmee drukt informatiebeveiliging zwaar op het ICT budget. Uit een onderzoek zoals beschreven in de Automatisering Gids van januari 2009 (2) is gebleken dat 1 op de 6 respondenten geen informatiebeveiligingsbeleid heeft, dat incidenten regelmatig voorkomen en dat kosten zelden bekend zijn, maar aanzienlijk.

Een grote variëteit aan specifieke en technische beschermingsmaatregelen kan worden ingezet: firewalls, antivirus, wachtwoorden, spamfilters, etc. Deze tools zijn lang niet altijd dekkend, onderling samenhangend en up to date. Beveiliging start bij beleid, directieverantwoordelijkheid en actief bewust zijn van mogelijk onveilig handelen.

Zowel de techniek als het organiseren van beveiliging vereisen continue aandacht. Ook het Amerikaanse Ponemon Institute (3) wijst in haar rapport "The ignored risk of employees' use of internet applications" van oktober 2008 op deze problematiek.

Ondanks de aandacht voor informatiebeveiliging gaat het toch vaak mis: Eerder lagen in Nederland patiëntengegevens op straat en recent valt te lezen dat 3 ziekenhuizen in Duitsland met de Downadup worm besmet zijn geraakt, ondanks dat de ziekenhuiscomputers van de laatste Windows updates waren voorzien (4).

1.3 Informatiebeveiliging is specialistenwerk

Analoog aan het zorg- en medische specialisme, is ook informatiebeveiliging specialistenwerk. Voorkomen is ook hier beter dan genezen en een overeenkomst is ook het belang van een integrale, toepassingsgerichte aanpak op het point of care, in dit geval primair gericht op de afdeling informatievoorziening (ICT, Informatisering, I&A) en met als uitkomst een samenstel (i.p.v. separate) van -elkaar aanvullende- maatregelen.

2 Uit de praktijk gegrepen

Beveiliging is voor velen een weinig tastbaar begrip. Daarom volgen hier enkele uit het leven gegrepen praktijksituaties.

Nieuwe verpleger op de afdeling

Er komt een nieuwe verpleger op de afdeling. Hoe wordt de nodige toegang tijdig gerealiseerd? Kan de nieuwe verpleger de dossiergegevens van een acuut te behandelen cliënt meteen inzien?

Een medewerker neemt afscheid

Een medewerker treedt, tijdelijk of permanent, uit zijn functie. Dan dient hij ook geen toegang meer te hebben tot vertrouwelijke of kritische gegevens, lokaties en apparatuur. Hoe kan het herroepen van toegangsprivileges gewaarborgd worden? Kan de ex-werknemer na afloop van het dienstverband de faciliteiten meteen niet meer gebruiken?

Toegangsgegevens raken verloren

Een specialist raakt zijn portefeuille kwijt, met daarin een elektronische pas om 's nachts de deuren van een ziekenhuis te openen. Er zit ook een notitie in waarop zijn gebruikersnaam en aanmeldprocedure voor allerlei gegevenssystemen in het ziekenhuis staan. Hoe kan verzekerd worden dat, na ontdekking van het verlies, derden geen oneigenlijke toegang hiermee kunnen krijgen? Hoe kan gecontroleerd worden of dit niet al gebeurd is?

Meerdere instellingen

Een medewerker is verbonden aan meerdere instellingen en heeft instellingsoverschrijdende, transmurale toegang nodig. Hoe kan dat geregeld worden zonder het beveiligingsbeleid van de afzonderlijke instituten geweld aan te doen?

Compleet clientendossier

In het kader van de hulpverlening aan verslaafden wordt methadon verstrekt aan ambulante cliënten. Het is denkbaar dat die proberen meerdere verstrekkingen van het dagrantsoen te verkrijgen door snel te 'shoppen' bij meerdere wijkposten, zodat goede coördinatie noodzaak is. Hoe kan dat voorkomen worden?

Externe contacten

In de ambulante gezondheidszorg en hulpverlening aan verslaafden komt het voor dat cliënten in aanraking komen met derde partijen, zoals bijvoorbeeld politie en justitie. Toch moeten ook daarmee gegevens uitgewisseld worden. Dit gebeurt typisch door de gegevens onversleuteld via e-mail over het publieke Internet te versturen. Een spanningsveld ontstaat tussen de verplichting tot waarborging van vertrouwelijkheid en integriteit van deze gegevens enerzijds en de verplichting om adequaat hulp te verlenen anderzijds.

Pogingen tot ongeoorloofde toegang?

Op de balie van een drukke afdeling staan computers. Zo'n computer kan toegankelijk zijn voor willekeurige passanten.

Op een late zaterdagavond zijn er opeens opmerkelijk veel mislukte inlogpogingen op een baliecomputer. Wordt dit ontdekt? Is het daarna snel duidelijk of het om een medewerker gaat wiens werk in de knel komt omdat het inloggen om een of andere reden faalt, of dat het gaat om een poging om oneigenlijk gebruik van dit systeem te maken?

Er komt een nieuwe applicatie

Een nieuwe applicatie wordt beschikbaar gesteld voor een specialisme. Hoe kan de ingebruikname hiervan zo gerealiseerd worden dat er geen gevaar is voor de bestaande infrastructuur?

3 Informatievoorziening in de zorg

Flexibiliteit van informatievoorziening en beveiliging van informatie staan vaak op gespannen voet te staan. Door beveiligingsmaatregelen goed afgewogen te implementeren kan de noodzakelijke flexibiliteit echter vaak wel behouden worden.

Kenmerkend in de zorgsector is de complexiteit door de veelheid aan partijen: zorgaanbieders, cliënten, zorgverzekeraars, overheidsinstanties en andere belanghebbenden spelen allen een rol in het verzamelen, opslaan, verwerken en transporteren van informatie.

Het gezamenlijk gebruik van informatie door meerdere verschillende partijen vraagt om standaarden voor informatieopslag, berichtopmaak, communicatieprotocollen, definities en codering van medische termen en, niet in de laatste plaats, informatiebeveiliging.

Ook internationaal is men zich steeds meer bewust van het belang van beschikbaarheid, integriteit en vertrouwelijkheid van zorginformatie, mede door de grensoverschrijdende uitwisseling ervan. Naast het borgen van deze kwaliteitscriteria vereist dit dat de informatiebeveiligingsmaatregelen op controleerbare wijze, zowel wat bedrijfsprocesniveau als onderliggende infrastructuur betreft, zijn ingericht, voordat er sprake is van adequate informatiebeveiliging.

In Nederland staat de relevante norm bekend als NEN 7510 en daarmee samenhangend NEN 7511 en NEN 7512. De Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) haakt ook in op een aantal aspecten betrekking hebbende op informatie, onder meer de bewaartermijnen ervan. Deze wet heeft dus consequenties voor dataopslagsystemen en de programmatuur om data te archiveren en te ontsluiten.

3.1 NEN 7510

De NEN 7510 is gebaseerd op de in april 2005 gepubliceerde revisie van de Code voor Informatiebeveiliging. De Code voor Informatiebeveiliging is internationaal geaccepteerd als ISO/IEC 17799. Onder informatiebeveiliging in de zorg wordt verstaan:

het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om verantwoorde zorg te kunnen bieden.

NEN 7510 geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die een organisatie in de gezondheidszorg dient te treffen ter beveiliging van de informatievoorziening. De organisaties waarop de norm zich richt variëren van individuele hulpverlener tot grote zorginstellingen en andere organisaties die bij de informatievoorziening in de gezondheidszorg zijn betrokken. De te treffen maat-

regelen verschillen per type organisatie. Bij deze norm horen implementatiehandboeken voor verschillende organisatietypen. Samen met de implementatiehandboeken geeft de norm een leidraad voor het organisatorisch en technisch inrichten van informatiebeveiliging. Zo biedt zij een basis voor vertrouwen in de zorgvuldige informatievoorziening bij en tussen de verschillende organisaties in de zorg. De indeling is gebaseerd op ISO/IEC 17799.

Het is de plicht van de zorgverlener er voor te zorgen dat geen inlichtingen over de patiënt aan derden ter beschikking komen. Tenzij de patiënt hier uitdrukkelijk toestemming voor heeft gegeven. Alleen personen die direct bij het onderzoek en de behandeling betrokken zijn, mogen over de patiëntgegevens beschikken.

— WGBO

3.2 NEN 7511: Toetsbare voorschriften

Na de publicatie van NEN 7510 in april 2004 heeft het ministerie van VWS (de directie Innovatie, Be-

roepen en Ethiek) aan NEN gevraagd het onderwerp 'Informatiebeveiliging in de zorg' daadkrachtig ter hand te nemen. Het ministerie wil er op toezien dat de toenemende (elektronische) gegevensuitwisseling goed en veilig functioneert. Zij is van plan om een verplicht karakter te geven aan de implementatie van de informatiebeveiliging in iedere zorginstelling. In november 2005 zijn NEN 7511-1, -2 en -3 gepubliceerd als uitwerking van de algemene norm NEN 7510.

Onder de verantwoordelijkheid van de normcommissie 'Informatiebeveiliging in de Zorg' van NEN zijn drie toetsbare voorschriften opgesteld voor de hele zorgsector. Door naleving van de norm, in combinatie met een toetsbaar voorschrift, wordt voldaan aan passende beveiliging rondom het gebruik van het Burger Service Nummer (BSN). Volgens de regels die NEN gebruikt zijn alle belanghebbende partijen bij dit proces betrokken.

De normcommissie heeft zorgorganisaties, die min of meer van dezelfde beveiligingsrichtlijnen gebruikmaken, ingedeeld in drie clusters. De informatievoorziening van een huisarts verschilt van die van een academisch ziekenhuis evenals de manier waarop zij hun beveiligingsproblemen oplossen. Voor de drie clusters zullen de te treffen maatregelen voor het waarborgen van informatiebeveiliging hierdoor ook significant van elkaar verschillen. De aanpak zou echter voor allen in beginsel hetzelfde kunnen zijn: richt de organisatie met beleid in en kijk daarbij goed naar de risico's die samenhangen met cliënten, omgeving en eigen organisatie. De clusterindeling is als volgt:

- Complexe organisaties zoals algemene ziekenhuizen, universitaire medische centra, gezondheidscentra, GGD- en GGZ-instellingen;
- Samenwerkende organisaties zoals thuiszorginstellingen, verpleeghuizen, bloedbanken, ambulancediensten en revalidatiecentra;

- Solopraktijken zoals apothekers, alleen praktiserende en in samenwerkingsverband praktiserende huisartsen, fysiotherapeuten, psychiaters, psychologen en tandartsen.

3.3 Implementatie van NEN 7511

Informatiebeveiliging is een gedeelde verantwoordelijkheid van alle betrokkenen in de zorg. De norm voor informatiebeveiliging zal daarom voor alle betrokken partijen toepasbaar moeten zijn, ongeacht de aard en omvang van het bedrijfsproces. Verschillende toepassingen van de norm worden zichtbaar gedurende de implementatie ervan. Naast de normen NEN 7510, 7511 en 7512 is een handboek opgeleverd om de invoering van de normen in zorginstellingen krachtig te ondersteunen. De normen in combinatie met het handboek bieden een houvast aan organisaties en personen om informatiebeveiliging in de praktijk te brengen.

In het handboek, dat beschikbaar is op het Internet¹, zijn uitleg, voorbeelddocumenten en sjablonen te vinden met betrekking tot de eisen die in NEN 7511 zijn geconcretiseerd. Het handboek moet de normen complementeren met concrete aanvullingen rondom informatiebeveiliging.

Specialisten van drie internetbeveiligingsbedrijven zijn er deze week in geslaagd om 1,2 miljoen patiëntgegevens van twee Nederlandse ziekenhuizen te openen. De 'hackers' deden dat op verzoek van publiciste Karin Spaik en hadden toestemming van de ziekenhuizen. Spaik waarschuwt voor schendingen van het medisch beroepsgeheim en pleit voor een betere beveiliging.

— *Volkskrant, 2 september 2005*

3.4 NEN 7512: Vertrouwensbasis voor gegevensuitwisseling

Deze norm is in twee opzichten een aanvulling op de richtlijnen die NEN 7510 aan organisaties in de zorg geeft voor hun informatiebeveiliging. In de eerste plaats richt deze norm zich op de zekerheid die partijen elkaar moeten bieden als voorwaarde

¹ Het handboek is te downloaden op <http://www.nen7510.org>.

voor vertrouwde gegevensuitwisseling. Ten tweede levert deze norm een nadere invulling voor een aantal van de richtlijnen van NEN 7510. Dat betreft dan vooral de aanzet tot risicoclassificatie en de uitwerking van de eisen over identificatie en authenticatie die behoren bij een bepaalde risicoklasse.

Het toepassingsgebied van deze norm is de elektronische communicatie in de zorg, tussen zorgverleners en zorginstellingen onderling en met cliënten, met zorgverzekeraars en andere partijen die bij de zorg zijn betrokken.

NEN 7512 geeft een schematische benadering voor het classificeren van communicatieprocessen naar het risico dat zij voor de gezondheidszorg met zich meebrengen. Aansluitend bij die classificatie worden voor uitwisseling van gegevens minimum-eisen gesteld met betrekking tot de bron van de gegevens, het transportkanaal en de ontvanger van de gegevens. Bron en ontvanger kunnen personen zijn, maar ook organisaties of hun informatiesystemen. Als overkoepelend begrip wordt hiervoor in deze norm de term 'entiteiten' gebruikt.

Hoewel kwalificaties van de betrokken partijen vitaal zijn voor het te stellen vertrouwen gaat deze norm er niet op in. Kwalificaties horen echter bij een identiteit, en het met voldoende zekerheid vaststellen van de authenticiteit van een partij alvorens deze vertrouwen te schenken is dan ook een eerste vereiste. In deze norm wordt aangegeven welke zekerheid over de identiteit van de te vertrouwen partij voor de onderscheiden risicoklassen voldoende wordt geacht.

Een te vertrouwen partij zal zijn identiteit en eventueel kwalificaties moeten aantonen en de vertrouwende partij moet die kunnen controleren. Door deze authenticatie wordt de vereiste zekerheid bereikt. Bij elk van de risicoklassen beschrijft de NEN-norm de minimaal vereiste wijze van authenticatie en de bijbehorende bewijsstukken. Voor de acceptatie van bewijsstukken is vertrouwen nodig in de uitgevende instantie en in de mate waarin het bewijsstuk bestand is tegen vervalsing en onrechtmatig gebruik.

In deze norm wordt zoveel mogelijk aangesloten bij methoden en voorzieningen die ook buiten de zorg worden toegepast. Waar de hoogste zekerheidseisen gelden wordt verwezen naar de normen die gelden voor een 'Public Key Infrastructure'. Bij lagere eisen wordt aangegeven welke andere methoden en middelen dan in aanmerking komen.

4 Voldoen aan NEN-normen

Aan NEN 7510 voldoen betekent dat zowel op organisatorisch als op technisch vlak een aantal zaken gerealiseerd is. Voor de organisatie geldt dat er een aantal specifieke processen en rollen en processen aanwezig moet zijn. Het gaat hier om *logische* rollen, die op allerlei wijzen fysiek gecombineerd kunnen worden. Zo kan een Hoofd ICT de rollen van zowel CIO als CTO vervullen, of een informatiemanager tevens de rol van CSO vervullen. Vitaal hierbij is wel dat verantwoordelijkheden voldoende gescheiden zijn: het mag niet zo zijn dat een beleidswijziging voorgesteld, ingevuld, beleidsmatig geverifieerd, uitgevoerd, en uitvoeringsmatig getoetst wordt door één enkele persoon.

4.1 PDCA



Daar beveiliging wezenlijk een zelf-reflectief permanent proces van observeren, meten, reflecteren en bijsturen is, mag het weinig verbazing wekken dat in het vervolg regelmatig verwezen wordt naar het 'Plan, Do, Check, Act' patroon: de klassieke 'PD-CA-loop'.

4.2 Organisatie en bedrijfsprocessen

Om beveiligingskaders te definiëren en het beveiligingsproces te verankeren in de organisatie, met heldere verantwoordelijkheden op een

expliciete manier daarin vevat, is vanuit NEN-perspectief een aantal rollen onderscheiden.

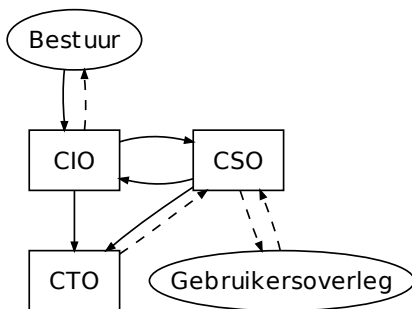
4.2.1 Organisatirollen

Bestuur Het bestuur van de organisatie is verantwoordelijk voor het beleid van de organisatie. Het stuurt verantwoordelijken voor inhoudelijke deelgebieden aan, en ontvangt feedback van hen om de uitvoering te kunnen toetsen.

CIO De 'Chief Information Officer', een rol die typisch door een informatiemanager vervuld wordt, is primaire verantwoordelijk in de organisatie voor het strategische informatiebeleid. Hij vertaalt beleidskeuzes van het bestuur maakt naar operatio-

neel beleid, en rapporteert terug aan het bestuur. Het opstellen van een expliciet beveiligingsplan hoort tot zijn taak. Dit plan is geformuleerd in nauwe relatie tot een expliciete classificatie in gegevensdomeinen van de verschillende soorten bedrijfsgegevens en gegevenssystemen.

werkbeheer of Systeem- en Netwerkbbeheer, heeft primaire verantwoordelijkheid in de organisatie op het operationele vlak van de informatietechnologie. Hij opereert binnen de door de CIO gesteld kader, en rapporteert voortgang en operationele kerngegevens terug. Wijzigingen laat de CTO altijd eerst (ook) accorderen door de CSO.



CSO De 'Chief Security Officer' heeft een adviserende rol in strategische context en een veto in operationele context. Hij bewaakt het beveiligingsproces actief, en stemt de door de CTO aangedragen wijzigingen af op het geldende beveiligingsplan.

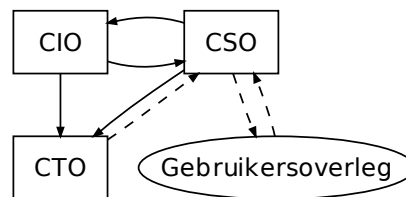
Gebruikersoverleg Dit overlegorgaan maakt signalen van (representanten) van eindgebruikers zichtbaar, zodat betrokkenheid van eindgebruikers kan leiden tot verbetering en vergroting van draagvlak.

CTO De 'Chief Technical Officer', typisch terug te vinden in functies als (Hoofd) Systeembeheer, Net-

*"That which doesn't kill you also leaves scars."
— Simson L. Garfinkel*

4.2.2 Bedrijfsprocessen

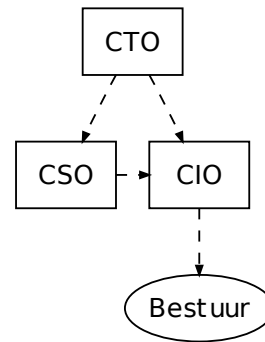
Metten Het lopende informatieproces levert een stroom van meetgegevens op die relevant zijn voor de beveiliging. Eindgebruikers raadplegen en modificeren gegevens, systemen wisselen gegevens uit.



Deze gebeurtenissen zichtbaar maken is de eerste stap die nodig is om de legitimiteit ervan toetsbaar te maken. Naast legitimiteitswaarborging – of, vice versa, detectie van beveiligingsincidenten – is ook

kennis van het normale functioneren van de informatiesystemen relevant. Beschikbaarheid van kritische systemen bewaken is ook deel van het beveiligingsproces. Dit omvat monitoring van belasting van systeemcomponenten en prestatiepeil ervan. Het is aan de CTO om kerngegevens van het operationele proces te meten.

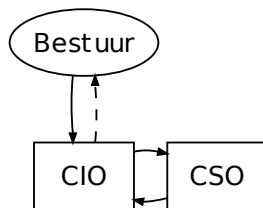
Verslaglegging Alle betrokkenen doen expliciet verslag van besprekingen en beslissingen.



De CTO legt daarnaast operationele details vast en de CIO stelt periodieke rapportages op, en stelt expliciet beleid op voor CTO en CSO.

Plannen en Beleid Maken Zonder expliciet beleid, waarin doelstellingen en kaders helder geformuleerd zijn, is toetsing onmogelijk.

Het bestuur stelt de doelen en randvoorwaarden voor inzet van informatietechnologie; de CIO legt op basis hiervan een informatie-infrastructuur vast. Dit definieert de informatiestromen en de ermee gepaard gaande informatieprocessen en -verantwoordelijkheden (c.q. bevoegdheden) in brede zin. Een specifiek deel hiervan is het beveiligingsbeleid: het beveiligingsplan. Dit laatste staat voor de CSO centraal, en wordt door deze gebruikt als toetssteen van het overige beleid dat de CIO opstelt.



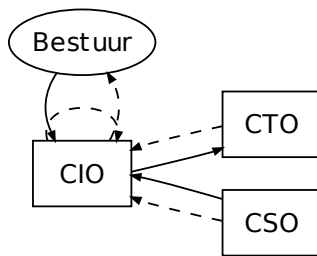
Analyse Een taak van de CIO is het analyseren van de waargenomen kerngegevens. Deze extrapoleert bijvoorbeeld historische trends, die eventueel tot aanpassingen in het strategische beleid en wijzigingen in de operationele praktijk leiden. Abnormale gebeurtenissen (anomalieën) meldt de

CIO aan de CSO. Incidenten zijn een belangrijk hulpmiddel om de kwaliteit te verbeteren en daarmee een signaal dat niet verwaarloosd kan en mag worden.

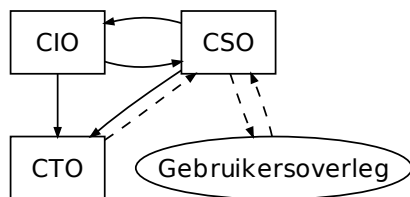
Evaluatie De bevindingen zoals vastgelegd in de verslaglegging worden structureel geëvalueerd.

Maak ook deze evaluaties deel van de verslaglegging.

Hierbij is het aan de CSO om te signaleren waar discrepantie tussen beveiligingsplan en waargenomen realiteit bestaat. Waar dit het geval is, is het wegnemen hiervan geen vrijblijvende taak. Dit kan leiden tot aanpassing van het beveiligingsplan en/of van de technische inrichting van de informatievoorzieningen.



Effectuering Elke verandering aan een informatiesysteem heeft mogelijk gevolgen voor de toegankelijkheid van gegevens, en voor beschikbaarheid en functioneren ervan.



Daarom moeten wijzigingen eerst getoetst worden aan het beveiligingsplan. Een functionele toevoeging, hoe handig ook, die bepaalde gegevens onbedoeld te breed toegankelijk maakt kan daarmee niet zonder meer uitgevoerd worden.

Waar sprake is van een strategische wijziging spreken CIO en CSO de wijziging door. Hierbij bepaalt de CSO de impact, en toetst de wijziging aan het beveiligingsplan. Bij uitvoering van een wijziging legt de CTO de voorgestelde wijziging, zoals die daadwerkelijk geïmplementeerd wordt, ter toetsing voor aan de CSO. Tevens wordt de voorgestelde wijziging besproken in het gebruikersoverleg, voor zowel praktische feedback alsook om het nodige draagvlak te creëren.

4.3 Technische invulling

De volgende stappen voor het van de in sectie 4.2.2 genoemde processen worden genomen om de NEN-normen in te vullen. Taken worden waar mogelijk vertaald naar technische infrastructuur door middel van de in sectie 4.5 genoemde hulpmiddelen.

"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."

— Gene Spafford

4.3.1 Strategisch beleid en planning

- i) **Heldere keuzes maken**; waar spanning optreedt tussen functionaliteit en beveiliging kan het niet zo zijn dat de wettelijke en overige bedrijfskritische vereisten van beveiliging vanzelfsprekend wijken. Integendeel, als uitgangspunt is 'als het niet op verantwoorde wijze kan, dan kan het dus niet' een gezond beginsel.

- ii) **Gegevens en gegevensstromen classificeren** op basis van een risico-analyse die prioriteiten wat beschikbaarheid, integriteit en vertrouwelijkheid van gegevens in kaart brengt. Deze classificatie is niet neutraal, maar impliceert een onderlinge ordening. Het is belangrijk in deze ordening de verschillende vereisten van beschikbaarheid, integriteit en vertrouwelijkheid ieder op naar waarde te schatten.

- iii) De vaak impliciete **vertrouwensrelaties expliciet maken**, volgens welke personen, netwerken en systemen toegestaan wordt om in aanraking te komen met bepaalde informatie:

- (a) **Zorgvuldig en selectief vertrouwen stellen** in de integriteit van **computersystemen** op het netwerk. Een computersysteem kan alleen vertrouwd worden als het om te beginnen aan minimale soliditeitseisen voldoet, en onder exclusief beheer van een daar-

toe gemandateerde beheersinstantie staat. Bovendien moet het ook systematisch en in het verlengde van het structurele beheer gecontroleerd en bewaakt worden, en uitsluitend voor geautoriseerde gebruikers na authenticatie toegankelijk zijn.

- (b) **Zorgvuldig en selectief vertrouwen stellen** in de integriteit van **deelnetwerken**. Hierbij geldt dat een deelnetwerk alleen dan (een bepaalde mate van) vertrouwen kan genieten als het uitgesloten is dat een in principe niet-vertrouwd systeem erop actief kan zijn.
- (c) **Alleen geautoriseerde personen** toegang geven met niet-publieke gegevens of gegevensstromen.
- (d) **Alleen gekwalificeerde systemen** toegang geven tot niet-publieke gegevens of gegevensstromen.
- (e) **Alleen gekwalificeerde netwerken** in aanraking brengen met niet-publieke gegevens of gegevensstromen.

Elke niet expliciet vertrouwde persoon, systeem of netwerk mag dus alleen in aanraking komen met gegevens die sowieso al publiek waren. Dit omvat expliciet gastgebruikers, publiekelijk toegankelijke systemen en gast-netwerken, en netwerken waarbinnen computersystemen functioneren waar gebruik van gemaakt kan worden zonder dat autorisatie na authenticatie conform de reguliere gebruikersadministratie plaats heeft gevonden.

Het internet heeft geen bijzondere status; het is één van de netwerken waarop in principe niet-betrouwbare personen en computersystemen actief kunnen zijn en dat dus geen vertrouwde status heeft.

"In the last week I handed my credit card to a waiter who disappeared with it for five minutes. I faxed my credit card information to a business in New Jersey, and the fax probably lay exposed to everyone in that office for hours and perhaps to the cleaning crew that night. I called a hotel and gave my card data to a reservation clerk and continued my recklessness by ordering some merchandise from a clothing catalogue, again by reading my credit card information to some unseen operator. Compared with the risk of handing my credit card to a stranger, which I do nearly every day, sending it over the Internet is pretty secure."

— Peter H. Lewis

4.3.2 Operationeel beleid en effectuering

- i) Logische **indeling in deelnetwerken** maken, primair in relatie tot de gegevensclassificatie gedefiniëerd, en verder gerelateerd aan functionele gegevens- en gebruiksdomeinen. Deelnetwerken zijn onderling absoluut gescheiden, zodat expliciete toegangsregels tussen netwerken onderling geformuleerd kunnen worden – en ook daadwerkelijk worden. Netwerkverkeer tussen de deelnetwerken onderling wordt gelogd en deze informatie wordt structureel en frequent geanalyseerd. Dit kan gerealiseerd worden door netwerkverkeer via 'perimeter security' firewalls te laten gaan. Zulke firewalls bieden uitgebreide screening en scanning van het netwerkverkeer, inclusief controle op malicieuze gegevensstromen (virussen, wormen en andere malware). Ze garanderen strikte handhaving van de gedefiniëerde toegangsregels, en loggen evenementen voor verslaglegging en analyse.
- ii) **Authenticatie, Autorisatie integraal opnemen** in netwerk-, systeem- en applicatie-infrastructuur, en het kaliber van authenticatie proportioneel te maken met de beveiligingsclassificatie. Hoe hoger de eisen voor een gegevensdomein, des te strenger de normen van authenticatie.

- iii) Uitsluitend onder de **bescherming door versleuteling met sterke cryptografie** transport over mogelijk onveilige kanalen, of dat nu via fysieke media dan wel via netwerken loopt, van gegevens waar ook maar enige integriteits- of vertrouwelijkheidseis voor geldt plaats te laten vinden.
- iv) **Gegevenslekkage tegengaan** door elke vorm van onversleutelde lokale gegevensopslag (op welk medium dan ook) onmogelijk te maken, en door op netwerkniveau restricties aan te brengen voor elke mogelijke gegevenslekkage. Dit omvat met name, maar niet alleen, 'file sharing' en 'peer to peer', web- en ftp-uploads, mail attachments, en bestandsuitwisseling zoals mogelijk in veel 'instant messaging' technieken.
- v) De **integriteit van netwerken permanent bewaken**, daarbij malicieuze activiteit zo snel mogelijk detecterend en blokkerend. IPS²- of NAC³-technologie bieden hierin assistentie. NAC kan tevens optreden tegen gedragingen die indruisen tegen het geldende beleid voor netwerkgebruik.
- vi) Gebruikte **computer- en netwerksystemen aan te passen** waar nodig. Voor de verschillende Windows-platforms in het bijzonder geldt hier dat minimumvereisten van soliditeit in architectuur en uitvoering, zo deze al haalbaar zijn, zeker niet 'uit de doos' gerealiseerd zijn. Op met name deze platforms is sprake van intensieve initiële inspanningen ('hardening'), noodzaak tot een stapeling van ingrijpende aanvullende bewakingstechnologie, en aanvullende permanente extra bewaking op systeemniveau. Door inzet van NAC-technologie inclusief authenticatie en integriteitscontrole ('pre-admission'), en permanente bewaking van computersystemen ('post-admission') als voorwaarde voor toelating op het netwerk, kan een minimale basis afgedwongen worden.
- vii) **Toegang af te schermen** naar alle niet-publieke gegevensdomeinen:
- vanaf vooraf gesanctioneerde en gecontroleerde systemen;
 - middels cryptografische verbindingen die integriteit en vertrouwelijkheid garanderen;
 - met sterke, 'multi-factored' authenticatie⁴ die tenminste bestaat uit:
 - een pre-shared key c.q. een uitgewisseld certificaat;
 - een vertrouwelijke 'passphrase';
 - een éénmalige passphrase of code, zoals door een 'token' geboden wordt;
 - uitsluitend in de vorm van 'application hosting' – gegevens en gegevensmanipulatie zijn exclusief beschikbaar in een gecontroleerde, beheerde omgeving. Deze kan alleen integraal, b.v. middels 'remote desktop' of in de vorm van een hierop toegesneden web-portal, benaderd worden. Het is hierbij zaak om zo'n omgeving professioneel in te richten met het oog op het uitsluiten van mogelijke lekkage. Met name de beschikbaarheid van lokaal aangesloten print- en opslag-systemen in de 'remote' omgeving en 'clipboard sharing' uitschakelen is van belang.

²'Intrusion Prevention System', voor diepgaande inspectie van, en waar nodig ingrijpen in, netwerkstromen.

³'Network Access Control', gebruikt om 'compliance' af te dwingen voorafgaand aan – en samengaand met – toelating van computersystemen op een netwerk.

⁴Authenticatie op basis van verschillende bronnen, bijvoorbeeld iets dat je *hebt* (bijvoorbeeld een UZI-pas), iets dat je *weet* (een PIN-code, bijvoorbeeld) en/of iets dat je *bent* (zoals een vingerafdruk).

4.3.3 Verslaglegging en meting

- i) **Accounting** expliciet deel uit te laten maken van elk facet van de netwerk-, systeem- en applicatie-infrastructuur. Systematische accounting vergt o.m. de aanleg van enige infrastructuur en (automatische) visualisatie- en analysemiddelen voor het loggen van netwerk-, systeem- en applicatie-evenementen.

Dit omvat 'logging' door netwerkapparatuur, serversystemen, netwerkdiensten, gebruikerssystemen en applicaties. Veelal worden evenementen al geregistreerd in logbestanden; daarnaast biedt 'syslog' technologie een hulpmiddel om evenementen structureel te laten loggen en registreren, en biedt 'snmp' technologie netwerkgebaseerde alertering.

4.3.4 Evaluatie en analyse

- i) Systematisch **risico-analyse** uit te voeren en ter permanente her-evaluatie van de gekozen gegevens- en netwerksegmentatie, met als technologische hulpmiddelen de opname van 'netwerksensors' in elk netwerksegment als luisterende oren voor een IDS⁵ en eveneens automatisch actieve 'vulnerability scans' uit te laten voeren middels specialistische software op de eigen netwerken, zowel erbinnen als tussen de netwerken onderling.
- ii) Periodieke beleid en uitvoering, integraal, te **herevaluëren** op basis van opgedane ervaringen en waarnemingen, waarin ook rekening gehouden wordt met continue veranderingen in technologie en wet- en regelgeving.

4.4 Op weg naar NEN-compliance

NEN-compliance vergt een aantal voorbereidende stappen. Hiermee wordt een fundament gelegd voor een operationele praktijk waarin de eerder genoemde doelen en processen verankerd kunnen worden. We noemen de volgende voorbereidende taken:

i) Domeinen en Grenzen

Classificeer gegevens en gegevensstromen, en stel gegevensdomeinen op. Stel vast in welke mate beveiligingseisen gelden voor de verschillende gegevensdomeinen.

Deel het netwerk fysiek en logisch op in deelnetwerken. Allerlei maatregelen worden mogelijk door deze compartimentering/segmentering.

- a) Als er sprake is van Internet-connectiviteit, dan speelt het Internet

de rol van een ongeautoriseerd netwerk.

- b) Dit geldt ook elk ander deelnetwerk dat niet onder volledige controle staat en waarop niet-vertrouwde systemen actief kunnen zijn.
- c) Beveiligingsmaatregelen zijn proportioneel aan de mate waarin eisen van vertrouwelijkheid, dataintegriteit en beschikbaarheid gelden. Hoe kritieker een bepaalde gegevensklasse is, des te zwaarder zijn de eraan gerelateerde beveiligingsmaatregelen.
- d) Maatregelen om ongeautoriseerd netwerkgebruik tegen te gaan. Een inventarisatie zal moeten plaatsvinden van de in de diverse (deel)netwerken

⁵Intrusion Detection System; voor permanente monitoring van activiteiten op een netwerk.

aanwezige netwerkaansluitingen. Open netwerkaansluitingen in onbeveiligde ruimtes dienen afgesloten te worden, en eventueel aanwezige 'port security' features van netwerkapparatuur kunnen geactiveerd worden om op elke netwerkpoort af te dwingen dat alleen de bekende, legitieme systemen er gebruik van maken.

e) 'Remote' toegang tot gegevens in sensitieve gegevensdomeinen moet voorbehouden zijn aan gegarandeerd integere computersystemen. Gegevenslekage moet uitgesloten zijn:

- Onbeheerde of niet volledig beheerde systemen geen toegang verlenen.
- Elke vorm van lokale data-opslag uitschakelen: er kunnen geen CD's gebrand worden en USB sticks aangesloten worden. Eventuele interne opslag is niet benaderbaar.
- Toegang op afstand ('remote access') tot gegevens alleen als welomschreven dienst bieden, op zodanige wijze dat een specifiek met dit oogmerk opgezette omgeving, uitsluitend voor vooraf bepaalde applicaties, opgezet is. Eindgebruikers krijgen alleen in die omgeving en via deze welgekozen applicaties toegang tot de gegevens. Faciliteiten voor het delen van het klembord ('clipboard'), printers, en het aankoppelen van lokale opslag op de 'remote' server en 'remote' opslag op de lokale machine moeten uitgeschakeld zijn.
- 'Thin client' werkomgevingen bieden een relatief eenvoudige

en effectieve manier om functionaliteit te realiseren terwijl toch een basisniveau van beveiliging gegarandeerd kan worden. Een mogelijke invulling hiervan is werkplekken direct van het netwerk te laten opstarten, geheel zonder lokale installatie/configuratie en gegevensopslag.

ii) Perimeter Security

De gegevensstromen aan de grens van elk deelnetwerk moeten bewaakt worden:

- a) Een strikt *secure by default* uitgangspunt, waarin alleen kan wat expliciet toegestaan wordt, is de eerste stap in het controleren van gegevensstromen.
- b) Eindgebruikers dienen betrokken te worden bij het beveiligingsbeleid. Gebruikers dienen zich expliciet aan letter en geest van het geformuleerde beveiligingsbeleid te committeren.
- c) De wenselijke gegevensstromen moeten *nauwkeurig* in kaart gebracht worden, zodat het mogelijk wordt om legitieme gegevensuitwisseling te onderscheiden van onwenselijke toegang.
- d) Toetsing of de wenselijke en waargenomen gegevensstromen ook daadwerkelijk wel toelaatbaar zijn dient op structurele basis plaats te vinden.

iii) Interoperabiliteit met standaarden

Gegevensuitwisseling en samenwerking tussen gegevenssystemen hoort te geschieden op basis van *standaarden*. Gesloten, niet-inspecteerbare, leveranciersspecifieke systemen staan daarmee op gespannen voet. Hierdoor wordt het niet alleen mogelijk om het gewenste functioneren daad-

werkelijk te garanderen, maar wordt ook controleerbare transparantie van het gehele proces mogelijk. Daar in de volksmond het woord 'standaardisatie' nog wel eens gebruikt wordt om precies het tegendeel aan te duiden is het zaak om standaardisatie (het baseren van functionaliteit op een bepaalde standaard) niet te verwarren met productselectie (de keuze voor een bepaalde leverancier en product). Vanwege de transparantie en gegarandeerde interoperabiliteit in heterogene omgevingen brengt standaardisatie een belangrijk secundair voordeel met zich mee: deelsystemen kunnen vrijelijk vervangen worden door andere, zolang deze de relevante standaarden respecteren. Standaardisatie betekent dus een radicale breuk met 'vendor lock-in', zodat een grote keuzevrijheid – en flexibiliteit – ontstaat.

De inzet van 'Open Source' verhoogt de transparantie, en kan daarmee een gunstige uitwerking hebben voor daadwerkelijke standaardisatie.

iv) Authenticatie en autorisatie spelen een sleutelrol. Authenticatie, of identificatie, gaat om het bepalen van de identiteit. Het authenticatieprobleem is: hoe kan een computersysteem vaststellen dat u daadwerkelijk bent wie u zegt te zijn? Het autorisatieprobleem is: hoe kan vastgesteld worden dat het legitiem is (of niet) dat een gebruiker iets uit een medicijnkast haalt? Voor beide geldt dat er een gradatie van betrouwbaarheid is om authenticiteits- en autoriteitskwesities te bepalen. Voor NEN-

compliance is het wezenlijk dat de sterkte van de gebruikte authenticatie en autorisatie proportioneel is met de beveiligingsnormen. Een dossierkast waar een stagiair ongeoorloofd dossiers uit kan halen is ernstig, maar minder erg dan dat de volledige voorraad van anaesthetische middelen verdwijnt; voor authenticatie en autorisatie voor de dossierkast op de gang dus minder strenge eisen.

- a) Sterke, meervoudige authenticatie is nodig voor belangrijke gegevensdomeinen.
- b) De gebruikersadministratie dient voldoende flexibel te zijn om de gehele levenscyclus van gebruikers grondig te kunnen controleren. Versnippering van de gebruikersadministratie is onwenselijk; voorkom hiermee secundaire schaduw-systemen en (partiele) replicatie- of synchronisatieschema's.
- c) Communicatiekanalen waar (ook) authenticatie in plaatsvindt moeten middels sterke cryptografie beschermd zijn, zodat authenticatie nooit over een onveilig kanaal geschiedt. Dit omvat niet alleen 'plain' netwerkverkeer, maar ook andere onveilige communicatie, zoals per briefpost, fax, telefoon of SMS.
- d) NAC-technologie biedt zowel pre- als post-admissiecontrole in netwerken, met authenticatie als integraal onderdeel.

4.5 Technische oplossingen

Een aantal instrumenten – technische hulpmiddelen – is beschikbaar om de taken en processen die boven omschreven zijn uit te voeren. Aandachtspunten bevinden zich op elk van de 'PDCA'-assen:

1. Plan
2. Do
3. Check
4. Act

We bespreken deze gebieden thematisch, en stippen daarbij de beschikbare technische hulpmiddelen aan.



Het is nuttig enige woorden te wijden aan voorzorgsmaatregelen in brede zin.

⁶...ouden menei, "alles stroomt en niets blijft", Herakleitos van Efeze – [http://nl.wikipedia.org/wiki/Panta_rhei_\(Herakleitos\)](http://nl.wikipedia.org/wiki/Panta_rhei_(Herakleitos)); zeker het technologische veld is in permanente flux is. Even nadat een systeem helemaal volgens de regels van de kunst van het moment opgetuigd is, zijn er alweer nieuwe kritieke updates te installeren, bijvoorbeeld. Permanente verandering is de enige constante.

4.5.1 Plan

Uit de analyse kan de noodzaak tot ingrijpen naar voren komen. Nieuwe of herziene strategische keuzen op bestuursniveau kunnen leiden tot wijziging van de status quo. In het algemeen, maar in het bijzonder voor technologie en zeker voor beveiligingsgerelateerde technologie, geldt: 'panta rhei'⁶, er is nu eenmaal een permanente stroom van wijzigingen. Orde brengen betekent hier de regie over de wijzigingen nemen.

Afhankelijk van gebruikte managementstechniek en -stijl (ITIL, PRINCE2, ...) zijn hiervoor allerlei hulpmiddelen beschikbaar. Dit is een zodanig breed veld van algemene aard dat we niet zien als iets dat specifiek in de context van de NEN-normen besproken dient te worden.

4.5.2 Do

Diverse hulpmiddelen maken het mogelijk om grip te krijgen en te houden op omvangrijke en complexe infrastructuren, en ook wijzigingen erin gecontroleerd aan te kunnen brengen:

- i) 'Next-generation' netwerkbeveiligingsapparatuur helpt om de onderlinge raakpunten van deelnetwerken rigoreus te beveiligen, zodat ook het correcte verloop en de inhoud van het netwerkverkeer bewaakt wordt. Hiervoor kunnen **IBM ISS proventia M** appliances worden toegepast, waarin generieke firewall-technologie geïntegreerd is met o.a. diepe protocolinspectie, malware-detectie en IPS-functionaliteit.
- ii) Elk systeem dat een zelfstandige installatie en configuratie heeft moet beheerd, onderhouden en bewaakt worden. Het is daarom

verstandig het gebruik van 'fat clients' zoveel mogelijk te vermijden, en ze van kritische netwerken te weren. Elk volledig vanaf het netwerk werkend systeem ('thin client'), zonder lokaal operating system, applicaties, configuratie en gegevensopslag, is een probleem minder; elke systeem met een eigen operating system, applicaties, configuratie, en gegevens dat geïnstalleerd, bewaakt, onderhouden, en gebackupt moet worden is een probleem extra. Waar een 'fat' installatie onvermijdelijk is dient de lokale installatie zo beperkt mogelijk te zijn⁷.

'Thin client' technologie kent een lange traditie en is reeds lang volwassen. Er is keuze te over. Dit geldt ook voor web-based en andere vormen van 'remote' applicatiegebruik.

iii) Controle over de systeem- en applicatie-installatie van alle werkplekken nemen is nodig, zeker als deze in sensitieve domeinen kunnen verkeren. 'Stripping' en 'hardening' van deze installaties is nodig. Relevante systeem- en applicatie-incidenten moeten structureel gelogd worden. In ieder geval de meest kwetsbare platforms (i.e. de verschillende Windows-varianten) moeten beschermd zijn door extensieve extra bewakings- en beschermingsmaatregelen. Voor dit laatste is een actief beheerd en bewaakt anti-malware pakket van degelijke snit aanbevolen.

iv) Naarmate het beveiligingsbelang van een gegevensdomein groter is, wordt sterkere authenticatie- en autorisatietechnologie ingezet. Voor gegevensdomeinen waarvoor substantiele beveiligingsnormen gelden is authenticatie met herbruikbare wachtwoorden onvoldoende. 'One Time Password' oplossingen, typisch ondersteund door 'au-

thenticatie tokens' die niet-herbruikbare inlogcodes genereren, zijn daarom al snel nodig. Voor zeer kritische/vertrouwelijke gegevensdomeinen is meervoudige (multi-factored) authenticatie geboden. **RSA SecurID** bewijst hier goede diensten.

v) Communicatiekanalen waar (ook) authenticatie overheen loopt moeten met sterke cryptografie beveiligd zijn. Authenticatie mag nooit over een onveilig kanaal plaatsvinden, zelfs niet als het om toegang tot een in principe niet-kritische resource gaat. Authenticatiegegevens worden namelijk maar al te snel door eindgebruikers hergebruikt in andere contexten. Een lek in een onbelangrijke autorisatie kan zo een lek in een gevoelig systeem worden.

Dit criterium is niet alleen van toepassing op onversleuteld netwerkverkeer, maar ook op andere onveilige communicatie – zoals per briefpost, fax, telefoon of SMS. Wachtwoorden horen onder geen beding op schrift gesteld te worden.

Technieken als **SSL**, **VPN** en **PKI** vormen de aangewezen weg om deze vorm van beveiliging te realiseren.

vi) De gehele levenscyclus van gebruikers moet grondig gecontroleerd worden. Versnippering van gebruikersadministraties ('balkanisatie') is onwenselijk, evenals secundaire schaduw-systemen en (partiële) replicatie- of synchronisatieschema's. Standaardiseren, in de betekenis van: functionaliteit baseren op standaarden, speelt hierin een belangrijke rol. **IBM Tivoli Identity Manager** en **IBM Tivoli Access Manager** kunnen hierbij ingezet worden, en hierbij kan met name 'single sign-on' een positieve uitwerking

⁷ Bijv., een applicatie moet direct specialistische locale hardware aansturen. Minimale installatie van een PC voor alleen deze applicatie is aanbevolen. Problemen en kosten kunnen verder beperkt worden door de reguliere applicaties ook op deze PC alleen via het web dan wel een of ander 'remote desktop' techniek beschikbaar te stellen

hebben. We noemen hier met name de 'Enterprise Single Sign-On' (ESSO).

Passwords are implemented as a result of insecurity.

- vii) Alleen systemen die onderworpen zijn aan de reguliere beheersdiscipline horen op het netwerk actief te zijn. Dit kan met behulp van 'Network Access Control' (NAC), zoals b.v. **Mirage NAC**, afgedwongen worden. Voor netwerken waarop het van belang is dat alleen geautoriseerde personen eraan deelnemen geldt dat authenticatie een integraal onderdeel moet vormen van de toelatingscontroles voor het netwerk zoals **Mirage NAC** die biedt.
- viii) Maatregelen moeten genomen worden om te garanderen dat wijzigingen teruggedraaid kunnen worden met een beperkte inspanning en in beperkte tijd.
- ix) Reikwijdte, doorloop en gevolg van handelingen dienen vooraf vastgelegd te worden. Significante wijzigingen moeten duidelijk aangekondigd worden. Wijzigingen horen conform de raming/aankondiging plaats te vinden. De doorloop van wijzigingen en onvoorziene complicaties moeten worden geboekstaafd.
- x) Wijzigingen die onderling afhankelijk kunnen zijn horen niet tegelijkertijd of kort opeenvolgend uitgevoerd te worden. Als het al nodig is om meerdere wijzigingen in zeer korte tijd, of zelfs tegelijkertijd, uit te voeren, dient men zich er van te verzekeren dat het daadwerkelijk gaat om onderling onafhankelijke wijzigingen.

4.5.3 Check

Vanuit beveiligingsperspectief moet belangrijke informatie zichtbaar zijn en vastgelegd worden:

⁸Zie <http://www.nessus.org/>.

- i) Het feitelijke netwerkgebruik dient gemeten te worden, met name wat betreft het netwerkgrensoverschrijdende verkeer.
- ii) Relevante incidenten moeten structureel en zover mogelijk centraal verzameld en geregistreerd worden. Eventueel aanwezig 'logging' en 'alerting' faciliteiten kunnen daarbij van dienst zijn: 'syslog' registratie en SNMP-monitoring. **IBM ISS SiteProtector** kan een goede aanvulling zijn.
- iii) Kerngegevens moeten stelselmatig vastgelegd worden door automatische 'vulnerability scans' uit te voeren en de bevindingen te registreren. Door dit op meerdere manieren te doen verbreedt men het altijd beperkte gezichtsveld dat een enkel scangereedschap nu eenmaal eigen is. Hiervoor worden **IBM ISS Security Scanner** en de **Nessus Vulnerability Scanner**⁸ (Open Source) aanbevolen.
- iv) Activiteit op het netwerk moet actief gemonitord worden. Indien aanwezig kunnen de 'event logging' van aanwezige 'perimeter security' (firewalls), IPS- en NAC-infrastructuur gebruikt worden. Bij afwezigheid van dergelijke infrastructuur wordt aanbevolen IDS-sensor(s) in het netwerk op te nemen.
- v) Anomalieën en ongeoorloofd gedrag binnen het netwerk, evenals overige beveiligingsincidenten, zijn belangrijk om te registreren. Voor wat het netwerk betreft kan IPS, zoals bijvoorbeeld de **IBM ISS proventia G**, hiervoor uitkomst bieden.
- vi) Periodieke en systematische verslaglegging van bevindingen en van operationeel handelen is noodzakelijk, opdat trends zichtbaar worden.

4.5.4 Act

Verslaglegging van kerngegevens uit de praktijk kan leiden tot nieuw inzicht. Het is van belang om in de wirwar van gegevens samenhang te ontdekken. Dergelijke relaties zijn vaak niet aan de oppervlakte zichtbaar:

- i)* Samenhangende evenementen kunnen gecorreleerd worden. Als bijvoorbeeld een worm een Windows-systeem overneemt, hoort daar een aantal gelogde gebeurtenissen bij: het systeem heeft iets van het web gehaald, er wordt een nieuw proces op het betreffende systeem gestart, er worden wijzigingen aangebracht in de software op het systeem, het systeem benadert even later op allerlei wijzen weer andere systemen op het netwerk, haalt kort daarop nog wat din-

gen van het web, en stuurt weer even later iets in bij een website. Samenhang brengen in de gigantische brei van gelogde informatie is van wezenlijk belang om te kunnen zien wat er nu eigenlijk precies speelt.

Goede gereedschappen voor deze complexe taak zijn **IBM Tivoli Security Operations Manager** en **IBM ISS Security Fusion for SiteProtector**.

- ii)* Door verworven inzichten periodiek en op een systematische manier te rapporteren worden historische trends zichtbaar. Door systematisch bevindingen te evalueren treden signalen die aangeven dat ingrijpen geboden is aan het licht. **IBM Tivoli Security Compliance Manager** kan assisteren bij het produceren van deze rapportages.

5 Certificatie/Compliance NEN 7510

Zorgverleners hebben altijd een maatschappelijke functie en verantwoordelijkheid. Daarnaast maken zij veelal onderdeel uit van een zorgketen. Zij hebben in deze keten te maken met andere zorgverleners die een belang hebben bij juiste gegevensverwerking en goede informatiebeveiliging. Ook heeft de financiering van zorg door externen (zorgverkeeraars, AWBZ) een belang bij de kwaliteit van gegevensverwerking en informatiebeveiliging. Kortom, er is een diversiteit aan externe partijen die een zorgverlener kunnen bevragen over informatiebeveiliging en het voldoen aan de NEN 7510. De normserie fungeert als een duidelijke metafoor en certificatie door een externe onafhankelijke partij (zoals **Lloyd's Register Quality Assurance (LRQA)**) geeft het gerechtvaardigde vertrouwen dat een zorgverlener voldoet aan alle relevante eisen op het gebied van informatiebeveiliging. Het toont aan dat een zorgverlener dit onderwerp actief en continue managet en beheerst.

5.1 Aanpak

Om te voldoen aan de NEN 7510 norm is het zaak dat organisaties en certificatie- instellingen zoals **LRQA** een eenduidige afspraak maken over de wijze waarop de norm moet worden toegepast. Al eerder is aangegeven dat daarbij de keuze voor een zelf-reflectieve aanpak volgens Demings 'P-D-C-A cirkel' een cruciaal uitgangspunt is. Alleen op

deze wijze is het voor organisaties mogelijk om niet alleen nu, maar ook in de toekomst op dynamische wijze het vraagstuk informatiebeveiliging te blijven beheersen. Het onafhankelijke toezicht van een certificatie-instelling zorgt voor de borging van deze aanpak.

5.2 Risicomanagement

Steeds meer organisaties hanteren bij de aanpak van management vraagstukken een risicogerichte benadering. De toenemende aandacht voor bestuurdersaansprakelijkheid heeft deze ontwikkeling versterkt. Het is dus niet vreemd om te zien dat op diverse plaatsen de norm NEN7510 verwijst naar risico- analyse alvorens een bepaalde beheersmaatregel te nemen. Kort gezegd wordt aan organisaties gevraagd hoe waarschijnlijk het is dat een bepaalde bedreiging zich voordoet en wat daarvan de impact is. **LRQA** heeft daarom gekozen om het instrument van risico-analyse centraal te stel-

len in de aanpak van het informatiebeveiligingsvraagstuk om te voldoen aan NEN 7510. Deze aanpak vindt haar grondslag in de Internationale Code voor Informatiebeveiliging/ISO 27001⁹ die als basis heeft voor de formulering van de NEN 7510-serie.

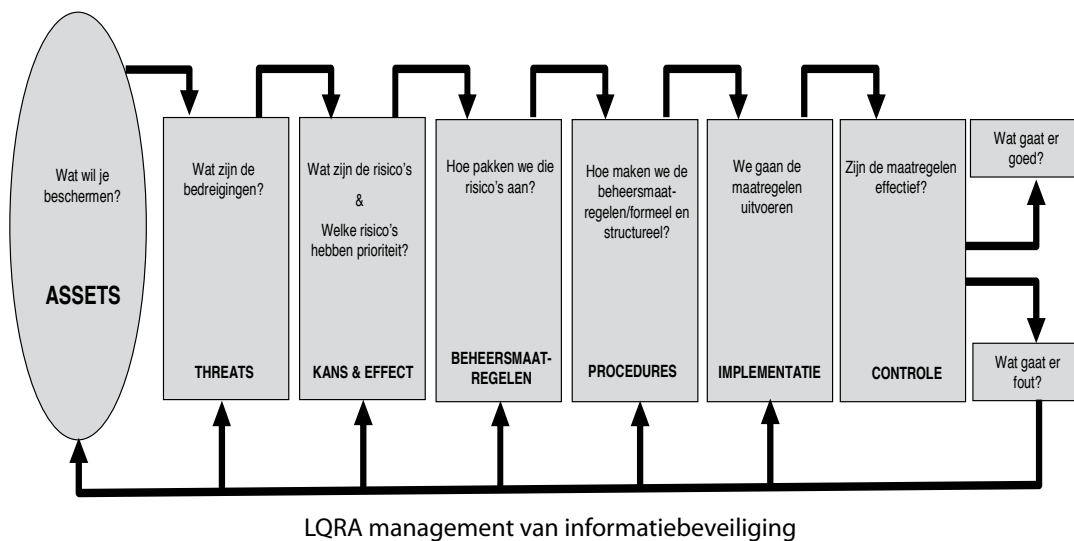
Kern van de in deze norm geformuleerde principes dat een organisatie al haar risico's op het gebied van informatiebeveiliging inventariseert aan de hand van de door haar belangrijk geachte zaken (de zogenaamde assets). Vervolgens dient zij deze risico's te analyseren (hoe groot, hoe erg) en te bepalen welke beheersmaatregelen wor-

⁹ISO/IEC 27001 Information Technology –Security Techniques – Management Systems-Requirements 2005

den geformuleerd voor de door haar relevant geachte risico's, door middel van de zogenaamde 'toepasselijkheidsverklaring'. Het is hierbij uiteraard van groot belang dat een organisatie methodisch inventariseert en analyseert en naar redelijkheid bepaalt waar de grenzen voor 'toepasselijkheid' liggen. De beheersmaatregelen, die zowel technisch als van organisatorische aard zijn, vor-

men vervolgens het vertrekpunt van de P-D-C-A cirkel. Het resulteert in een beheersmaatregelenplan (plan), dat vervolgens dient te worden uitgevoerd (do), waarvan de effectiviteit dient te worden beoordeeld (check) en waar nodig aangepast (act).

Hieronder is dit proces in een figuur weergegeven.



5.3 Traject

Voor zorgverleners die aan de NEN 7510 norm willen voldoen is het zaak dat zij niet alleen onderkennen wat de waarde is van een risicogerichte aanpak op basis van de PDCA principes, maar dat zij ook leren de instrumenten die daaraan ten grondslag liggen te beheersen.

Inventarisatie en analyse Het inventariseren van risico's blijkt voor veel organisaties niet zo'n eenvoudig proces. Dit is meestal niet gelegen in het feit dat een zorgverlener niet in staat is om vast te stellen welke risico's zich in een bepaald zorgproces voordoen, maar in het krijgen van overeenstemming over de omvang van het risico (hoe vaak

doet een bedreiging zich voor en wat is de impact). Ervaring leert dat dezelfde risico's verschillend worden ingeschat wanneer deze vanuit verschillende disciplines wordt beschouwd. Een arts zal nu eenmaal een andere visie op het risico van zoekraken van patiëntgegevens hebben dan het hoofd ICT en ook over andere kennis beschikken om zijn of haar visie te beargumenteren.

Een integrale maar vooral ook multidisciplinaire aanpak van risicomanagement waarbij vooraf spelregels en afspraken worden gemaakt zijn belangrijke uitgangspunten wanneer een organisatie start met het inventariseren en analyseren van risico's. Het is om deze reden zaak om niet alleen

voldoende verschillende disciplines te betrekken bij risico-inventarisatie, maar vooral het proces op (onafhankelijke) wijze te laten begeleiden. Het is niet ongebruikelijk om het risico-analyse en inventarisatieproces over meerdere sessies en een wat langere, projectmatige, periode uit te smeren. **LRQA** biedt verschillende trainingen aan waarbij zij zorgverleners de principes van risicomanagement bij brengt. Daarnaast coacht **LRQA** zorgverleners die het proces van risico-inventarisatie en -analyse zorgvuldig willen uitvoeren.

Beheersmaatregelen Wanneer het fundament van het systeem voor NEN 7510 staat, de risico-analyse, is het vaak goed mogelijk om de juiste beheersmaatregelen te definiëren. De risico-analyse geeft de organisatie in feite een 'routekaart' die bepaalt welke risico's het grootst zijn en welke beheersmaatregelen daardoor prioriteit hebben. Veel organisaties zullen ook ervaren dat een grote set aan beheersmaatregelen (beveiligingsmaatregelen) nu een veel meer samenhangend geheel krijgen. Tevens ontstaat ook een budgettaire prioriteit, want er valt immers snel genoeg te zien welke bedreigingen het grootst zijn. Overigens is het zo dat beheersmaatregelen niet altijd een financiële impact hoeven te hebben. Beheersmaatregelen zijn in vier categorieën in te delen:

1. Ontwijken. Een zorgverlener kan bepaalde activiteiten ontwijken zodat een risico zich niet meer voordoet (bijvoorbeeld niet meer thuis werken)
2. Verplaatsen naar derden. Een zorgverlener kan een risico verplaatsen naar een andere risicodrager (bijvoorbeeld het uitbesteden van gegevensopslag of toegangsbeheer)
3. Accepteren. Een zorgverlener kan een risico accepteren omdat de omvang beperkt is of er onvoldoende beheersmaatregelen beschikbaar zijn (bijvoorbeeld het risico van een aanslag)

4. Verminderen. Een zorgverlener kan een risico verminderen door maatregelen te nemen waar door een bedreiging zich minder vaak voordoet of waarvan de impact wordt verminderd (het installeren van een noodstroomvoorziening waarmee stroomuitval tot een minimum wordt gereduceerd)

Procedures De beheersmaatregelen die een zorgverlener kiest om de risico's op het gebied van informatiebeveiliging te reduceren zullen niet alleen van technische aard zijn. Veel maatregelen betreffen afspraken over hoe bepaalde risicovolle activiteiten moeten worden uitgevoerd. Hierdoor ontstaat niet alleen eenduidigheid, maar wordt ook de foutkans verkleind omdat betrokkenen kunnen worden gewezen op de afspraken die zijn gemaakt. Ze bieden daarnaast houvast bij de beoordeling of het management van informatiebeveiliging goed en efficiënt werkt.

Controle Zorgverleners die willen voldoen aan de NEN 7510 en dat willen laten certificeren door een instelling als LRQA dienen niet alleen externe audits te ondergaan maar moeten ook in staat zijn met regelmaat zelfstandig te beoordelen of het gehele proces van de in dit hoofdstuk beschreven maatregelen werkt. Het hiertoe geëigende instrument is de interne audit. De interne audits moeten resulteren in een beeld over de effectiviteit van de gekozen maatregelen en daarmee een beeld over hoe de organisatie haar informatiebeveiliging beheerst.

Reflectie De resultaten van interne audits en de dynamiek van informatiebeveiliging vragen zorgverleners de geïnventariseerde risico's te evalueren, de analyses daarvan te beschouwen, de beheersmaatregelen te herdefiniëren en procedures aan te passen. Hiermee ontstaat een continu proces en een niet aflatende aandacht voor het onderwerp informatiebeveiliging

5.4 Resultaat

Een zorgverlener die, op basis van externe audits door een instelling als LRQA, aantoont dat zij alle in het traject beschreven stappen beheerst komt in aanmerking voor het certificaat tegen de normserie NEN 7510. Hiermee bewijst de instelling dat de informatiebeveiliging op orde is en dat gegevensbeheer en -uitwisseling aan haar mag worden toevertrouwd. Met een certificaat laat de instelling aan allerlei stakeholders (waaronder patiënten, belangvertegenwoordigers, collega instellingen, centrale en decentrale overheden etc.) zien dat zij voldoet aan de eisen die op nationaal niveau zijn vastgelegd. De minister van Volksgezondheid heeft daarom de verwachting uitgesproken dat zorgverleners betrokken bij het Elektronisch Patiënten Dossier aan deze norm gaan voldoen.

Ook in de toezichthoudende sfeer zal er naar verwachting een waardering zijn voor een onafhankelijke certificatie. De Inspectie voor de Gezondheidszorg (IGZ) heeft zich al herhaaldelijk positief uitgelaten over certificatie conform de NEN 7510-serie. In de gezamenlijke publicatie *'Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm'* van de IGZ en het College Bescherming Persoonsgegevens¹⁰ krijgen alle Nederlandse Ziekenhuizen de opdracht *'om in 2010 aan de hand van de resultaten van een externe audit aan te tonen dat zij voldoen aan een voldoende mate van informatiebeveiliging.'* Tevens geven het CPB en de IGZ de Nederlandse Ziekenhuizen de opdracht *'dat er voor 15 oktober een Plan van Aanpak is opgesteld waarin duidelijk wordt wat het ziekenhuis onderneemt om volledig aan de NEN 7510 norm te voldoen.'* **LRQA** verwacht dat ziekenhuizen met NEN 7510 certificatie op basis van onafhankelijke audits laten zien dat zij aan deze opdracht voldoen.

Onafhankelijkheid Dit position paper heeft tot doel hulp te bieden bij een hands-on aanpak voor het voldoen aan het normstelsel NEN 7510 en een beeld te schetsen van mogelijke beheersmaatregelen. **LRQA** is een onafhankelijke certificatieinstelling en zal de effectiviteit van deze beheersmaatregelen in alle gevallen per organisatie moeten beoordelen.

¹⁰ *Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm*: Rapportage van een onderzoek in 2007 door het College bescherming persoonsgegevens en de Inspectie voor de Gezondheidszorg naar de informatiebeveiliging in 20 ziekenhuizen.

6 Samenvatting en conclusie

Halverwege 2007 heeft de ministerraad ingestemd met een wetsvoorstel waarin de kaders voor de invoering van een landelijk elektronisch patiëntendossier (EPD) zijn vastgesteld. Het wetsvoorstel regelt onder meer de verplichting voor zorgaanbieders om aan te sluiten op het EPD en de eisen waaraan de beveiliging moet voldoen. Dit betekent dat in de toekomst alle Nederlandse zorgaanbieders getoetst zullen worden op hun informatiebeveiliging.

Enerzijds heeft dit repercussies op het beleid ten aanzien van informatie, de zorgprocessen en de manier van werken binnen een zorginstelling. Anderzijds zal ook de volledige ICT infrastructuur op haar beveiligingsaspecten moeten worden doorgelicht, en conform de NEN 7510, -7511 en -7512 normen.

Dit document maakte duidelijk welke zaken daarbij belangrijk zijn. Een van de gevolgen is dat een zorginstelling, eenmaal werkend conform NEN 751x, dat ook in de toekomst behoort te blijven doen. Permanente feedback en sturing is noodzakelijk. Naast quickscans voor de bedrijfsprocessen zijn er voor de ICT infrastructuur uitstekende oplossingen beschikbaar.

Informatiebeleid en de uitvoering daarvan vergen meer dan ooit professionele zorg, en gaan hand in hand. Het NEN normenkader voor de zorgsector is een nuttig en bovendien wettelijk verplicht hulpmiddel voor informatiebeveiliging. Op technisch gebied bestaat een keur aan geavanceerde hulpmiddelen ten behoeve van de informatiebeveiliging. Beveiliging van informatie en informatievoorzieningen vergt een dynamische en integrale aanpak.

Index

- Accounting, 16
- Application Hosting, 15
- Authenticatie, 14, 18, 20
 - Multi-Factored, 19
 - OTP
 - One Time Password, 20
 - Public Key Infrastructure, *zie* PKI
- Autorisatie, 14, 18, 20
- Balkanisatie, 20
- Bedrijfsprocessen
 - Analyse, 12, 22
 - Beveiligingsbeleid, 11
 - Effectueren, 19
 - Evaluatie, 12
 - Meten, 11, 21
 - Planning en Beleid, 11, 19
 - Verslaglegging, 11
- Beschikbaarheid, 6, 11, 12
- Beveiligingsplan, 11
- BSN
 - Burger Service Nummer, 7
- Classificatie, 13
- Compartimentering, *zie* Segmentatie
- Compliance, 17
 - Authenticatie, 17
 - Autorisatie, 17
 - Classificatie, 17
 - Inventarisatie, 18
 - Perimeter Security, 18
 - Policy, 18
 - Secure by Default*, 18
 - Proportionaliteitsbeginsel, 17
 - Toetsing, 18
- Confidentialiteit, *zie* Vertrouwelijkheid
- Cryptografie, 15
- Deelnetwerken, *zie* Segmentatie
- EPD
 - Electronisch Patiënten Dossier, 27
- ESSO
 - Enterprise Single Sign-On, 21
- Evaluatie en Herevaluatie, 16
- Fat client, 20
- Firewall, *zie* Perimeter Security
- Gegevensdomeinen, 13, 17
- Gegevenslekage, 14
- Hardening, 20
- IDS
 - Intrusion Detection System, 21
- IEC 17799, *zie* ISO 17799
- Incident, 3, 11, 20, 21
- Informatiebeveiliging, 6
- Integriteit, 6, 14
- Internet, 13, 17
- IPS
 - Intrusion Prevention System, 14, 19, 21
- ISO 17799, 6
- Logging, 16
- Multi-Factored Authenticatie, 15
- NAC
 - Network Access Control, 14, 15, 19, 21
- NEN
 - NEN 7510, 6
 - NEN 7511, 7
 - NEN 7512, 8
- Open Source, 18
- Organisatie rollen
 - CIO, 9
 - CSO, 9
 - CTO, 9
 - Gebruikersoverleg, 10
- Panta Rhei, 19
- PDCA

Plan,Do,Check,Act
Monitoring, Analysis, Planning, Execution, 9
Perimeter Security, 14
PKI
Public Key Infrastructure, 8, 20
Praktijkvoorbeelden, 5

Risiko-Analyse, 16
Intrusion Detection System, *zie* IDS
Vulnerability Assessment, 16

Segmentatie, 14, 17
Standaardisatie, 18, 20
Stripping, 20

Thin client, 17, 20
Transmurale Toegang, 5

Versleuteling, *zie* Cryptografie
Vertrouwelijkheid, 6, 13–15, 20
Vertrouwensrelatie, 13

WGBO
Wet op de Geneeskundige Behandelingsovereenkomst, 6
Windows-problematiek, 20

