

Grip en controle over patiëntgegevens

VOORKOMEN IS BETER DAN GENEZEN

In de nabije toekomst krijgt een patiënt direct en volledig online toegang tot zijn eigen dossier. Dit brengt grote veranderingen met zich mee voor de IT-voorzieningen in de zorgsector. Men moet aantoonbaar grip op en controle hebben over de beschikbaarheid en bescherming van behandel- en patiëntinformatie. De specifieke beveiligingsnormen NEN7510 en NEN7513 bieden hiervoor een goede leidraad. CORNÉ DE KEIZER

Er is maatschappelijk veel gaande over de rechten en zeggenschap van een patiënt met betrekking tot het medisch dossier. Los van de vraag of het altijd in het belang van de patiënt is, zijn de gevolgen van deze ontwikkelingen voor de IT-omgeving van ziekenhuizen groot. Men moet aantoonbaar grip op en controle hebben over het beschikbaar stellen van behandel- en patiëntinformatie. En de optimale bescherming van digitale privacygevoelige patiëntinformatie kunnen waarborgen. De Inspectie voor de Gezondheidszorg (IGZ) zal toetsen of (beveiliging van de) ICT correct wordt nageleefd. Hiervoor zijn onder andere de specifieke beveiligingsnormen NEN 7510 en NEN 7513 van toepassing.

De betrouwbaarheid van ziekenhuisinformatiesystemen en de IT-voorziening is in het belang van de patiënt en dient daarom aantoonbaar te zijn. 'In control' zijn is daarom voor ieder ziekenhuis een basisbehoefte. Hoewel in control raken van een IT-omgeving een veelomvattend onderwerp is, zijn vanuit de IT-optiek een drietal randvoorwaarden zeer actueel:

- ❖ ZIS in control;
- ❖ Infrastructuur in control;
- ❖ IT-beheer in control.

ZIS in control

Een ziekenhuisinformatiesysteem (ZIS, zoals Chipsoft, iSoft en McKesson) is voor een ziekenhuis hét centrale punt waar medische gegevens worden verwerkt en bewaard. Vanuit de in-controlgedachte rijst een aantal basisvragen bij het aantonen van wat er is gebeurd:

- ❖ Is een bepaald behandeldossier geraadpleegd of gewijzigd door medewerkers die beroepsmatig helemaal niets met de patiënt te maken hebben?
- ❖ Wie heeft dat dan gedaan?
- ❖ Wanneer heeft die persoon dat gedaan?
Dit leidt automatisch tot vervolgvragen, zoals:
 - ❖ Hoe komt dergelijke informatie op eenvoudige wijze naar boven uit een systeem?
 - ❖ Hoe kan er zekerheid worden verkregen dat de informatie correct is?
 - ❖ Uit hoeveel verschillende systemen moet informatie eigenlijk worden opgehaald?
 - ❖ Hoe kan er zekerheid worden verkregen dat deze informatie juridische waarde heeft?

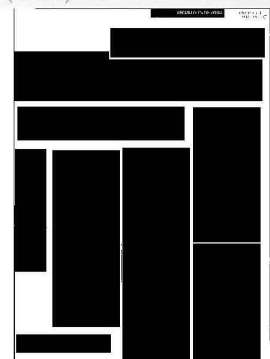
Binnen de branche is veel aandacht voor dit vraagstuk. Medio 2010 heeft het Nederlands Normalisatie-instituut (NEN) hier zelfs een nieuwe norm voor geïntroduceerd: NEN 7513. NEN omschrijft deze nieuwe norm als volgt: "De norm voorziet in eisen voor stelselmatische registratie van acties op elektronische patiëntdossiers."

Binnen de norm worden concrete richtlijnen gegeven over datgene wat gelogd moet worden. Daarnaast zijn er richtlijnen voor de integriteit en onweerlegbaarheid van de logging. Dit laatste heeft veel gevolgen op het gebied van security. Een logfile op een Linux- of Windows-server kan namelijk niet zomaar als onweerlegbaar worden beschouwd. Het heeft bovendien een (zeer) beperkte juridische waarde. Daarnaast is het doorzoeken van een logfile geen sinecure. Het is ook ondoenlijk om een patiënt inzage te geven in de 'platte' logs. Daarom zijn voor het beveiligen en beschikbaar stellen van de logs serieuze maatregelen nodig.

Maar moet de zorgsector dan het wiel uitvinden? Het antwoord hierop is natuurlijk 'nee'. Andere branches, waaronder de financiële sector, hebben al jaren te maken met het in-controlvraagstuk. Door gebruik te maken van deze ervaringen, maar ook van de toegepaste technologie, kan de zorgsector een vliegende start maken met het in control krijgen van de elektronische dossiers.

SIEM

NEN 7513 biedt een mooie richtlijn om invulling te geven aan de vraag 'wat moet ik doen?'. Maar NEN geeft helaas geen voorschriften hoe dat te realiseren is. Een goede en bewezen oplossing is Security Information & Event Management (SIEM). SIEM is een waar-



devol en praktisch hulpmiddel bij het realiseren van volledige controle over de IT-omgeving.

SIEM is een centrale plaats in de IT-omgeving waar alle loginformatie van apparatuur, besturingssystemen en systemen zoals het ZIS wordt verzameld. De auditlogs worden door het SIEM-systeem voorzien van een digitale handtekening en een tijdstempel. Hierdoor heeft de auditlog juridische waarde, omdat er aantoonbaar niet mee geknoeid kan zijn.

Op basis van de verzamelde auditlogs genereert SIEM automatisch rapportages over de verschillende systemen. Hierdoor worden afwijkingen ten opzichte van de norm en bijzondere trends gesignaleerd. Bij detectie van een beveiligingsincident geeft SIEM direct een alarmbericht, zodat dit incident direct kan worden opgevolgd. En het gaat nog verder als de auditlogs van verschillende systemen met elkaar worden gecorreleerd. Voorbeeld: in een normale situatie logt een gebruiker eerst in op het netwerk en pas daarna in het ZIS. Stel dat een gebruiker op een bepaald moment in het ZIS inlogt, maar deze gebruiker is niet ingelogd op het netwerk. Op dat moment is het aannemelijk dat iemand anders onder de naam van de betreffende gebruiker het ZIS wil gebruiken. Bij de juiste correlatie genereert SIEM hierop een alert, zodat direct actie kan worden ondernomen.

Ook is het mogelijk ad hoc rapportages op te vragen. Dit kan bijvoorbeeld inzichtelijk maken welke activiteiten (lezen, wijzigen van gegevens, et cetera) plaats hebben gevonden betreffende een bepaald systeem, gebruiker of patiënt. Vanzelfsprekend zijn deze laatste gebonden aan privacywetgeving.

De informatie die de SIEM-omgeving genereert, is zeer bruikbaar bij het realiseren van kwaliteitsverbeteringen. Met behulp van rapportages worden afwijkingen geconstateerd in het gewenste gedrag. Afhankelijk van de mate waarin dit voorkomt kan een en ander worden behandeld als incident (eenmalig) of als probleem. De SIEM-omgeving draagt bij aan structurele verbetering van zowel kwaliteit als informatiebeveiliging binnen de IT-omgeving en -organisatie.

Een SIEM implementeren alleen is echter niet de oplossing voor dit vraagstuk. Stel dat een gebruiker het scherm niet blokkeert en dat iemand anders vervolgens de gegevens van een patiënt wijzigt. Dan heeft de betreffende

gebruiker bij geconstateerd misbruik heel wat uit te leggen. Het op een correcte manier omgaan met IT-middelen binnen het zorgproces is voorwaarde. Dergelijke oplossingen moeten altijd onderdeel zijn van een groter geheel en een totaalplan voor de (kwaliteits) verbetering van informatievoorziening en informatiebeveiliging.

Infrastructuur in control

Apparatuur en informatiesystemen zijn meer en meer gekoppeld via het netwerk. Om in control te zijn, moet de omgeving stabiel, flexibel en schaalbaar zijn. De IT-infrastructuur moet gereed zijn voor het faciliteren van nieuwe informatiesystemen, nieuwe apparatuur en nieuwe ontwikkelingen. Nieuwe zaken moeten in feite gemakkelijk in te pluggen zijn in de infrastructuur.

Een goed hulpmiddel hiervoor is het opstellen van een IT-architectuur. Het netwerk wordt verdeeld in logische zones, en informatiesystemen en apparatuur worden aan de hand van hun classificatie in de passende zone geplaatst. Voor iedere zone gelden eigen beveiligingsrichtlijnen en specifieke maatregelen.

Een voordeel van een duidelijke architectuur is het eenvoudig plaatsen en beschikbaar stellen van nieuwe informatiesystemen binnen de IT-omgeving. Door heldere voorwaarden te stellen aan nieuwe systemen, voordat deze worden aangeschaft, wordt vooraf eveneens bepaald waar het systeem in de omgeving terecht komt. Dit maakt een goede capaciteitsplanning mogelijk.

Maar een architectuur op papier alleen is niet voldoende. Om de kwaliteit van informatievoorziening te garanderen, zijn ook concrete maatregelen nodig. Zoals iedere organisatie kampt ook een ziekenhuis met de problematiek rondom het uitvoeren van essentiële beveiligingsupdates. Het is voor geen enkele organisatie echt eenvoudig om dit proces onder controle te krijgen, maar bij medische apparatuur is er vaak een extra dilemma. Om een correcte werking van apparatuur te garanderen, zijn fabrikanten zeer terughoudend met het installeren van beveiligingsupdates. Als updates toch zonder toestemming worden geïnstalleerd, kan dit invloed hebben op het correct functioneren van de apparatuur. Zonder de beveiligingsupdates wordt de apparatuur echter kwetsbaar voor malware.

Virtual patching

Een belangrijk deel van de genoemde problematiek is te ondervangen met virtueel patching. Hierbij wordt gebruik gemaakt van Intrusion Detection & Prevention (IDP)-technologie. IDP-apparatuur bewaakt het netwerkverkeer en onderzoekt dit op verdacht gedrag. De IDP wordt automatisch voorzien van gegevens over de meest recente patches in de markt en mogelijk misbruik van lekken in software.

De IDP is daarmee in staat om malware te herkennen en indien nodig te blokkeren. Op het moment dat dergelijke apparatuur tussen het netwerk en de medische apparatuur wordt geplaatst, functioneert dit in feite als een virtuele patch. Kwaadaardig verkeer wordt herkend en geblokkeerd op basis van het gedrag. Dus zelfs als medische apparatuur niet is beschermd met de laatste beveiligingsupdates, is het systeem toch beveiligd.

De IDP-omgeving kan ook weer worden gekoppeld aan de eerder genoemde SIEM-oplossing. Dit maakt het mogelijk om vanaf een centrale plaats rapportages en alarmberichten met beveiligingsincidenten te genereren. Hiermee kan afwijkend gedrag worden geconstateerd, waardoor de IT-beheerorganisatie de melding direct kan opvolgen.

IT-beheer in control

De kwaliteit van de beheerprocessen is ook in de zorgsector cruciaal. Helaas bestaat het beheren van de IT-omgeving bij veel organisaties nog steeds uit het blussen van brandjes.

Voorgaand is een aantal technische maatregelen besproken. Deze maatregelen hebben echter alleen zin als de organisatie hier klaar voor is. Een SIEM-systeem dat NEN 7510- of NEN 7513-rapportages genereert en beveiligingsincidenten detecteert, maar waar vervolgens niets mee wordt gedaan, is in feite een waardeloze investering. Alleen als de organisatie om weet te gaan met de output van dergelijke systemen en deze gebruikt als input voor verdere processen, voegt de technologie iets toe.

Een goede balans tussen werkbaarheid en proces is van groot belang. Het is daarom noodzakelijk om maatregelen te nemen op basis van geconstateerde risico's. Risicobeheersing koppelen aan IT-beheer kan hierbij helpen. Bijvoorbeeld bij het stellen van prioriteiten. Bij een incident dat wordt geclassificeerd als een hoog risico, zullen sneller maat-

regelen genomen moeten worden dan bij incidenten met een laag risico.

Optimaliseren beheerprocessen

Over IT-beheer zijn boeken vol geschreven. Er zijn veel methoden, standaarden en maatregelen te vinden. Dat onderschrijft de gedachte dat IT-beheer niet eenvoudig is, en zeker niet voor iedere organisatie eenduidig is te realiseren.

Het proportioneel inrichten van IT-beheer is belangrijk. Het niveau van IT-beheer moet passend zijn voor de te beheren omgeving. Dat lijkt een open deur, maar bij veel organisaties is dat niet het geval. Prioriteiten worden veelal gekozen op gevoel en op basis van 'wie het hardst roept is het eerst aan de beurt'. En niet op de werkelijke, vooraf vastgestelde, waarde van de IT-middelen. Een bedrijfskritisch systeem heeft een snellere responsetijd nodig dan een systeem wat dat niet is. Maar wie stelt vast welke systemen bedrijfskritisch zijn? De IT-afdeling? Of de eigenaar van de data op het systeem? Wie is eigenlijk eigenaar van de data op een systeem? Zijn dat de maatschappen? Of de zorgadministratie? Of (zoals er de laatste tijd veel over gepubliceerd wordt) de patiënt zelf?

Een goede impactanalyse helpt bij het vaststellen van de criteria voor ieder IT-middel. Hierbij wordt centraal vastgesteld wat het niveau van beschikbaarheid van het IT-middel moet zijn. En hoe het gesteld is met de vertrouwelijkheid en de integriteit van de data. Als van iedere classificatie ook nog wordt vastgesteld wat de bijbehorende maatregelen (wel/geen encryptie, wel/niet redundant uitvoeren, wel/geen sterke authenticatie, et cetera) moeten zijn, is een standaard geboren. Zodra via de impactanalyse wordt vastgesteld welke classificatie een informatiesysteem heeft, zijn automatisch de bijbehorende maatregelen bekend en is bekend op welke plaats in de IT-architectuur het systeem wordt geplaatst.

Maar een dergelijke basis biedt meer mogelijkheden. Het is eenvoudiger voor de IT-afdeling om SLA's af te sluiten met de organisatie. Afhankelijk van de classificatie van het systeem worden onder meer responsetijden afgesproken of back-upschema's ingericht. Zoals eerder gezegd: wel proportioneel. Standaarden als ITIL of ISO20.000 zijn prima, maar alleen een weloverwogen keuze in ITIL-componenten helpt bij het vaststellen van de standaarden binnen de organisatie.

Incidentmanagement is bijvoorbeeld een belangrijk onderdeel. NEN 7510 wijdt er zelfs een heel hoofdstuk aan. Het NEN schrijft voor dat beveiligingsrelevante activiteiten vastgelegd moeten worden. Maar ook dat bewijsmateriaal met juridische waarde moet worden verzameld. Bewijsmateriaal over datgene wat plaats heeft gevonden op een informatiesysteem (bijvoorbeeld wie een dossier heeft geraadpleegd) kan uit een SIEM-omgeving worden gehaald. Een incident kan zijn dat onterecht gebruik is gemaakt van een noodaccount. SIEM signaleert op dat moment het incident, maar levert ook direct het bewijsmateriaal. Op het moment dat dit is gekoppeld aan de classificatie van het systeem (NEN 7510 schrijft ook risicobeheersing voor), kan de incidentopvolging in het IT-beheerproces proportioneel worden uitgevoerd.

Door met behulp van de juiste middelen om te gaan met incidenten, is het mogelijk structurele verandering en verbetering door te voeren in de IT-omgeving. Dat is het verschil tussen brandjes blussen en brandpreventie. Want in de zorgsector weet men het toch als geen ander: voorkomen is beter dan genezen. ♦

CONCLUSIE

Het aantoonbaar in control zijn is een steeds belangrijker wordend vraagstuk. Met actuele technische middelen is veel te bereiken. Echter, deze technische middelen mogen geen doel op zich zijn.

Hoewel een aantal ziekenhuizen voorop loopt op het gebied van informatiebeveiliging, valt er in de branche nog veel te doen. Het aanschaffen van wat hardware en software alleen lost de problematiek niet op. Het inbedden van deze middelen in de processen en procedures is noodzakelijk voor succes.

Corné de Keizer (CISSP, CISA) is Information Security Consultant bij Motiv.

NEN-normen

- NEN 7510: norm voor informatiebeveiliging voor de zorgsector in Nederland, gebaseerd op de Code voor Informatiebeveiliging.
- NEN 7511: toetsbaar voorschrift voor solo-praktijken, samenwerkingsverbanden en grote instellingen.
- NEN 7512: gericht op de AORTA, de nationale infrastructuur voor uitwis-

seling van elektronische gegevens in de zorg.

- NEN 7513: voorziet in eisen voor stelselmatige registratie van acties op elektronische patiëntdossiers.

Andere branches hebben al jaren te maken met het in-controlvraagstuk

Technische maatregelen hebben alleen zin als de organisatie hier klaar voor is

