Informatiebeveiliging en privacy in de zorg

Wat moeten bestuurders weten?

Een overzicht.

ip-zorg
Informatieveiligheid
en privacy in de zorg

Juni 2023
Stichting IP-Zorg

Inhoud

1 Toelichting

Dit document geeft een beeld van ontwikkelingen waar de zorgsector mee te maken heeft op het gebied van informatiebeveiliging en privacy. Het betreft maatschappelijke en technologische ontwikkelingen, ontwikkelingen op gebied van wet- en regelgeving en toegenomen risico's. Er wordt tevens kort ingegaan op het handelingsperspectief dat hier een antwoord op zou kunnen zijn. De geschetste ontwikkelingen laten zien dat informatievoorziening steeds meer een strategisch risico wordt dat aandacht dient te krijgen van het bestuur van de organisatie, naast de aandacht die het heeft (moet hebben) van informatiebeveiligings- en privacy-specialisten in de organisatie. Daarom heeft dit document als ondertitel *Wat moeten bestuurders weten?* Wij hopen dat dit document zijn weg vindt naar die bestuurders. Mogelijk dat zij het direct onder ogen krijgen, mogelijk dat zij het krijgen aangereikt via hun informatiebeveiligings- of privacyfunctionarissen. Het voorgestelde handelingsperspectief richt zich op deze informatiebeveiligings- en privacy-specialisten in de organisatie, maar ook op hun bestuurders. De focus ligt hierbij op de eigen organisatie, de omgeving en op samenwerkingsorganisaties of ketenpartners.

Eerst wordt kort ingegaan op de context. Vervolgens komen algemene en specifieke ontwikkelingen, wet- en regelgeving en de inhoudelijke thema's met betrekking tot informatieveiligheid en privacy aan de orde.

Wij reiken in dit overzichtsdocument specifieke onderwerpen aan en hebben ervoor gekozen om weinig bronnen en verwijzingen te gebruiken. Aan de hand van de specifieke informatie kan de lezer voldoende relevante informatie vinden, op het internet dan wel via de eigen specialisten.

1.1 Ontstaan Stichting IP-Zorg

Voor veel professionals in de zorg is het voldoende borgen van informatieveiligheid en privacy een belangrijk vraagstuk. Terwijl wet- en regelgeving op dit gebied toenemen, manifesteren toezichthouders als de Inspectie Gezondheidszorg en Jeugd en de Autoriteit Persoonsgegevens zich steeds nadrukkelijker. Maar ook opdrachtgevers, ketenpartners, financiers en cliënten worden veeleisender op dit gebied. Zorginstellingen zien zich voor grote uitdagingen geplaatst als het gaat om informatieveiligheid en privacy, terwijl aan de andere kant beschikbare middelen vaak beperkt zijn of conform andere prioriteiten worden toegewezen. Stichting IP-Zorg is in 2019 ontstaan vanuit de gedachte dat samenwerking binnen de zorg op dit gebied belangrijk is zodat niet onnodig het wiel hoeft te worden uitgevonden. Stichting IP-Zorg is een netwerkorganisatie die zich ten doel stelt verbinding tot stand te brengen tussen personen en organisaties die binnen de zorg- en welzijnssector actief zijn op het gebied van informatieveiligheid en privacy. Ook biedt IP-Zorg zorginstellingen en andere betrokkenen de gelegenheid om op de hoogte te blijven van actuele ontwikkelingen.

1.2 Aangesloten organisaties en medewerkers in de zorg

Iedereen die werkzaam is in de zorg- en welzijnssector kan zich aansluiten bij Stichting IP-Zorg. Men kan bijdragen door deel te nemen aan activiteiten, zoals webinars en bijeenkomsten. Maar ook door op andere wijze actief kennis en kunde in te brengen. Zorginstellingen worden bij Stichting IP-Zorg ook "Aangesloten Organisaties" genoemd. Aan deelname zijn geen kosten verbonden.

Ongeveer 250 medewerkers van zorgorganisaties en zorg-gerelateerde belangenorganisaties hebben zich aangesloten. De nieuwsbrief wordt gemaild naar ongeveer 400 belangstellenden (stand per januari 2023).

1.3 Partners

Stichting IP-Zorg kent diverse bedrijven als kennispartners. Kennispartners hebben aantoonbare ervaring in de zorg- en welzijnssector en kennis over de diensten of producten die zij aanbieden. Kennispartners hebben een goede staat van dienst en staan als zodanig bekend. Kennispartners worden betrokken bij onderzoeken, bijeenkomsten, ontwikkelen van eisen, modellen of richtlijnen. Leidraad daarbij is inbreng van expertise en kwaliteit, boven een commercieel doel.

Daarnaast werkt Stichting IP-Zorg samen met CIP-Overheid, het landelijke expertisecentrum op gebied van informatiebeveiliging en privacy dat zich richt op overheidsorganisaties. Stichting IP-Zorg maakt bijvoorbeeld gebruik van het kennis- en discussieplatform cip.pleio van CIP-Overheid. Op deze *community site* is allerhande materiaal beschikbaar, worden discussies gevoerd, en kunnen mensen elkaar vinden aan de hand van de kennis die ze willen delen of om informatie van anderen te verkrijgen. Iedereen die werkzaam is in de zorg en aangesloten bij Stichting IP-Zorg of bij een kennispartner werkzaam is, kan toegang krijgen tot het platform en lid worden van onze IP-Zorg-community.

Ook onderhoudt IP-Zorg goede contacten met Z-CERT. Zij hebben bijgedragen aan webinars waarin cyberweerbaarheid en ransomware centraal stonden. Z-CERT is in 2017 als onafhankelijke stichting opgericht op initiatief van de NVZ, NFU, de Nederlandse GGZ en VWS. In januari 2020 is Z-CERT aangewezen als Computer Emergency Response Team voor de gehele zorgsector. Bij Z-CERT werken cybersecurity-specialisten die zorginstellingen helpen bij het versterken van de digitale veiligheid. Z-CERT bedient momenteel meer dan 300 zorginstellingen.

Tenslotte vindt er ook afstemming plaats met ECP Platform voor de InformatieSamenleving, een platform waar overheid, wetenschap, bedrijven, onderwijs en maatschappelijke organisaties samenwerken en kennis uitwisselen over vormgeving van de digitale samenleving. Vanuit ECP worden voor de zorg relevante initiatieven ondersteund, zoals Digivaardig in de zorg, Informatieveilig gedrag in de zorg en Veilig Internetten.

1.4 Webinars

Na de startbijeenkomst in 2019 zijn er zeven webinars georganiseerd.

- Secure by Design; Een toekomstvaste Netwerk Infrastructuur als technische randvoorwaarde voor functionele toepassingen (2020)
- Microsoft Teams; veilig communiceren met zorgverleners, cliënten en achterban (2020)
- Informatieveilig gedrag in de zorg; een wetenschappelijke aanpak vertaald naar de praktijk (2020)
- Aantoonbaar voldoen aan NEN 7510 en AVG met behulp van tooling (2021)
- NEN7510: Certificeren en zelf de regie houden (2021)
- Ransomware; hoe kun je het voorkomen en wat moet je doen wanneer het je overkomt (2021)
- Cyberweerbaarheid in de zorg; digitale veiligheid, hoe organiseer je het en waar moet je als zorginstelling rekening mee houden (2022)
- Gegevensuitwisseling binnen het sociaal domein (2022)

1.5 Onderzoek leveranciersmanagement

Stichting IP-Zorg heeft een enquête uitgevoerd onder zorginstellingen om inzicht te verkrijgen in de wijze waarop voor zorgsystemen invulling wordt gegeven aan leveranciersmanagement, de mate waarin informatiebeveiliging en privacybescherming hierin worden meegenomen en de rol die de verschillende leveranciers hierin zelf vervullen.

Het verkregen inzicht kan allereerst worden gebruikt om waar mogelijk vanuit het kennisnetwerk van IP-Zorg te komen tot een benchmark, te komen tot een gezamenlijke afstemming met leveranciers, waar noodzakelijk het inkoopproces te verbeteren en te professionaliseren, de dienstverlening (beter) te monitoren en de eigen organisatie en die van de leverancier aan te sturen en waar mogelijk effectiever te maken.

Alhoewel de respons op de enquête beperkt was, kan hieruit wel worden afgeleid dat zorginstellingen afhankelijk zijn van een beperkt aantal leveranciers in de markt en zorginstellingen niet gemakkelijk hiervan veranderen. Men gebruikt vaak al jaren hetzelfde systeem en heeft in de meeste gevallen ook niet het voornemen te wijzigen. Informatieveiligheid en privacy zijn vaak geen onderwerpen geweest die bij de selectie en implementatie een rol hebben gespeeld, en ook in de gebruiksfase wordt er lang niet altijd op gemonitord. Vaak ontbreekt de kennis en tijd om hier adequaat invulling aan te geven.

1.6 Bijeenkomst met partners

Eind september 2022 is een bijeenkomst geweest met vertegenwoordigers van kennis- en samenwerkingspartners. Tijdens deze sessie is onder leiding van een onafhankelijk voorzitter met elkaar van gedachten gewisseld over ontwikkelingen in de zorg, grote uitdagingen waar zorginstellingen mee te kampen hebben, en wat dit wel of niet betekent voor informatiebeveiliging en privacy. Tijdens deze sessie is de behoefte aan de orde gekomen om tot een gezamenlijk document te komen, waarbij niet alleen de uitdagingen worden geschetst maar ook het daaraan gekoppelde mogelijke handelingsperspectief. Dit document geeft hier invulling aan.

2 Ontwikkelingen

Voor zorginstellingen wordt de afhankelijkheid van ICT steeds groter. Dit heeft te maken met een toenemende vraag naar zorg, toenemende complexiteit van zorgverlening die meer afstemming vraagt met andere ketenpartners en toenemende krapte op de arbeidsmarkt. Al deze ontwikkelingen worden veelal op enige wijze mogelijk door verdergaande digitalisering, of worden juist ingegeven doordat verdergaande digitalisering aan de orde is.

De komende jaren zal digitalisering door inzet van zorgdomotica, internet of things, e-health, maar ook door (verplichte) elektronische gegevensuitwisselingen met ketenpartijen verder toenemen. Ook het recent afgesloten Nationaal Zorg Akkoord gaat hiervan uit. Dit leidt tot meer geautomatiseerde verwerking van (persoons-)gegevens en zal nieuwe afwegingen met zich meebrengen ten aanzien van o.a. compliance en risico's. Ook komen belangen van cliënten, medewerkers en andere betrokkenen steeds meer centraal te staan (denk aan de rechten van betrokkenen in het kader van de

AVG). De Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) stelde al verplicht dat zorginstellingen per 1 juli 2020 elektronische toegang voor cliënten of hun vertegenwoordigers moesten inrichten. De volgende stap is de Persoonlijke Gezondheidsomgeving (PGO) die de cliënt zelf beheert en waar steeds meer zorginformatie-systemen van zorginstellingen op zullen aansluiten om gegevens beschikbaar te maken binnen de gekozen PGO.

De rol van leveranciers wordt hierbij steeds belangrijker. Leveranciers moeten, na een initiële kwalificatie, worden gecertificeerd. De verwachting is dat dit zal leiden tot schaalvergroting, waardoor enkele grote leveranciers de markt zullen domineren. De afhankelijkheid van leveranciers kan voor zorginstellingen nadelen opleveren, temeer daar zorginstellingen vanwege hoge implementatiekosten niet snel meer zullen of niet meer kunnen veranderen van (zorginformatie-)systeem.

Een ontwikkeling bij veel zorginstellingen is de overgang van on-premise applicaties (op eigen infrastructuur) naar applicaties die bij de leverancier draaien in de vorm van een SaaS-dienst (vaak onterecht en onjuist 'in de cloud' genoemd). Hiermee worden zorginstellingen ontzorgd, echter men blijft wel verantwoordelijk.

Terwijl zorginstellingen voor grote uitdagingen staan die het gevolg zijn van de hiervoor geschetste ontwikkelingen, is een extra complicerende factor dat instellingen ook te maken hebben met grote budgettaire uitdagingen. De vraag naar zorg neemt toe, terwijl het totale zorgbudget niet in dezelfde mate toeneemt of wordt beperkt. De daarbij stijgende kosten voor bijvoorbeeld salarissen, energie en vastgoed, zorgen ervoor dat voor informatiebeveiliging en privacybeschermende maatregelen eerder minder geld beschikbaar zal zijn dan meer. Dit gaat bovendien gepaard met een grote krapte op de arbeidsmarkt die niet alleen geldt voor zorgpersoneel, maar ook voor de specifieke expertise die nodig is voor een goed functionerende en betrouwbare informatievoorziening. Ook dit zal bij leveranciers aanzetten tot schaalvergroting.

3 Wet- en regelgeving

Voor de zorgsector bestaat zorgspecifieke wet- en regelgeving; het gaat hier om allereerst de Wet geneeskundige behandelingsovereenkomst (WGBO), Wet langdurige zorg (Wlz), Wet maatschappelijke ondersteuning (Wmo) en Jeugdwet, Wet verplichte geestelijke gezondheidszorg (Wvggz), Wet zorg en dwang (Wzd) en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). Daarnaast heeft de AVG veel impact gehad vanwege de verplichting om de verwerking van persoonsgegevens veel beter in kaart te brengen, inclusief de privacyrisico's. Maar ook vanwege de extra aandacht voor rechten van cliënten, medewerkers en andere betrokkenen ten aanzien van de verwerking van persoonsgegevens.

Onderstaand wordt ingegaan op nieuwe wet- en regelgeving die consequenties heeft voor zorginstellingen:

3.1 Wet elektronische gegevensuitwisseling in de zorg

De Wet elektronische gegevensuitwisseling in de zorg (Wegiz) beoogt te borgen dat binnen de zorgsector te allen tijde de juiste informatie op de juiste plek op het juiste moment beschikbaar is. De Wegiz doet dit door in een aantal stappen elektronische gegevensuitwisseling tussen zorgaanbieders verplicht te stellen in plaats van gebruik van papier, fax, etc. Deze wet raakt cliënten en zorgaanbieders, maar ook de leveranciers van applicaties, zowel als infrastructuur in de zorg. De gegevensuitwisseling zal plaatsvinden op basis van standaarden en leveranciers zullen waar nodig hun systemen hiervoor moeten aanpassen. Uiteindelijk zullen leveranciers zich hiervoor ook moeten laten certificeren, hetgeen nieuwe of extra eisen zal stellen aan leveranciers. De Wegiz zal na de inwerkingtreding (naar verwachting uiterlijk 2024) stapsgewijs worden doorgevoerd op basis van afzonderlijke algemene maatregelen van bestuur gedurende de periode 2024 tot 2028. De gekozen volgorde sluit op dit moment aan op de VIPP-programma's, te beginnen met E-Overdracht, medicatie, BGZ, Beeldopnamen.

3.2 Wet digitale overheid

De Wet digital overheid (Wdo) borgt dat burgers op veilige en betrouwbare wijze kunnen inloggen bij de (semi-)overheid. De wet is van toepassing op alle publieke dienstverleners waar ook zorginstellingen onder vallen. Naar verwachting zal in eerste instantie alleen DigiD als passend inlogmiddel wettelijk worden erkend; dit betekent dat cliënten op het cliëntenportaal van een

zorginstelling moeten kunnen inloggen met DigiD (betrouwbaarheidsniveau substantieel/hoog). Het gebruik van DigiD stelt hoge eisen aan de inrichting van informatiebeveiliging. Om DigiD te mogen gebruiken, dient een organisatie bovendien jaarlijks een DigiD-assessment door een onafhankelijk auditor te laten uitvoeren wanneer de DigiD-aansluiting in eigen beheer is (voor de on-premise applicaties). Het is van belang om de voorbereidingen hierop zo snel mogelijk te starten dan wel de keuze te maken het beheer volledig uit te besteden.

De Wdo zal naar verwachting halverwege 2023 in werking treden, waarna organisaties nog gelegenheid zullen krijgen om aan te sluiten op DigiD.

3.3 Wet aanpak meervoudige problematiek sociaal domein

De Wet aanpak meervoudige problematiek sociaal domein (Wams) beoogt een oplossing te bieden voor de noodzakelijke gegevensuitwisseling in het geval van problematiek, die meerdere gebieden binnen het sociaal domein raakt. Dit betreft bijvoorbeeld gezinssituaties met meerdere problemen, waar ook meerdere (soorten) zorgverlening bij zijn betrokken. Op dit moment ontbreekt vaak de wettelijke grondslag die noodzakelijk is om gegevens te mogen uitwisselen tussen de betrokken zorgverleners en andere betrokkenen, zoals bijvoorbeeld gemeenten. Aangezien gemeenten in deze situaties vaak de regie voeren, kan geen beroep worden gedaan op toestemming als grondslag. Dit beperkt de zorg- en hulpverlening op dit moment aanzienlijk., wanneer vereiste gegevensuitwisseling hierdoor niet tot stand kan komen. De Wams creëert een expliciete grondslag voor gegevensuitwisseling tussen betrokken zorginstellingen en gemeenten en is tevens de basis voor een meldpunt voor betrokkenen. De verwachting is dat deze wet niet in werking treedt voor 1 januari 2024.

3.4 Herziening NEN 7510

De NEN 7510, de Nederlandse norm voor informatiebeveiliging in de zorg, is in 2017 voor het laatst herzien. In september 2022 heeft NEN de komende herziening opgestart. Deze vloeit voort uit het feit dat ISO 27001 en ISO 27002 recentelijk zijn herzien en het herzieningsproces voor ISO 27799 loopt. NEN 7510 is gebaseerd op deze normen. Er wordt ingespeeld op nieuwe ontwikkelingen met betrekking tot informatiebeveiliging: extra aandacht voor inrichting van cyberweerbaarheid, het toenemende gebruik van SaaS-diensten, borging van business continuïteit, toepassing van (wettelijke) bewaartermijnen en waar mogelijk maskeren van (gevoelige) persoonsgegevens. Praktisch gezien is er een nieuwe structuur en hoofdstukindeling. De verwachting is dat de herziene versie in 2024 zal worden gepubliceerd.

Organisaties die al gecertificeerd zijn, of voor publicatie van de nieuwe versie (2024) gaan certificeren, krijgen drie jaar na publicatie van de nieuwe versie om over te gaan. Dit betekent met name het omzetten van de gekozen beheersmaatregelen naar de nieuwe structuur en waar nodig het toepassen van de daarbij behorende implementatierichtlijnen. Hiervoor is een tabel beschikbaar.

Ook in de eisen van NEN 7510-1 zullen wijzigingen aangebracht worden. Er moet een transitieaudit plaatsvinden, die kan samenvallen met de hercertificeringsaudit.

Organisaties die ervoor kiezen om niet extern te certificeren, of die vanaf 2024 opgaan voor certificering, kunnen zich eigenlijk al vanaf nu richten op de nieuwe eisen en implementatierichtlijnen. Hiervoor kan gebruikt gemaakt worden van ISO 27001:2022 en ISO 27002:2022.

3.5 Wet kwaliteitsregistraties zorg

Het wetsvoorstel Wet kwaliteitsregistraties zorg (Wkz) legt de basis voor het verplicht en rechtmatig, zonder toestemming van de cliënt, aanleveren van (bijzondere) persoonsgegevens door zorgaanbieders ten behoeve van kwaliteitsregistraties in de zorg. Zorginstituut Nederland krijgt de taak kwaliteitsregistraties, waarvan is vastgesteld dat die het meten en verbeteren van de kwaliteit van zorg en daarmee het algemeen belang dienen, op te nemen in een (nieuw) register voor kwaliteitsregistraties. Tot slot voorziet dit wetsvoorstel in de wettelijke plicht voor zorgaanbieders om, in het geval dat een kwaliteitsregistratie is opgenomen in het register voor kwaliteitsregistraties van het Zorginstituut, de gevraagde informatie aan (de gegevensverwerker van) de betreffende kwaliteitsregistratie aan te leveren. Het wetsvoorstel is op 16 december 2022 ingediend bij de Tweede Kamer.

3.6 Europese Network and Information Systems-richtlijn (NIS2)

Sinds 2020 is vanuit de Europese Unie gewerkt aan de *Network and Information Security (NIS2) directive*. Deze richtlijn is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. De Europese lidstaten hebben tot eind 2024 de tijd om de NIS2-richtlijn op te nemen in nationale wetgeving. In Nederland wordt de richtlijn vertaald naar de Wet Beveiliging Netwerk- en Informatiesystemen (WBNI). De richtlijn schrijft verplichtingen voor, waaraan zowel publieke als private organisaties binnen bepaalde sectoren, waaronder gezondheidszorg, moeten voldoen. Eisen worden gesteld aan risicobeheer, continuïteit, incidentmanagement, netwerkbeveiliging, toegangscontrole en encryptie. Eventuele sancties kunnen betrekking hebben op boetes en schorsing van bestuurders.

3.7 Verzamelwetten gegevensbescherming en - gegevensverwerking

Ten tijde van het schrijven van dit document zijn verschillende 'Verzamelwetten' in de fase van wetsvoorstel en consultatie:

- Verzamelwet gegevensbescherming: Wijziging van de Uitvoeringswet Algemene verordening gegevensbescherming en enkele andere wetten in verband met het stroomlijnen en actualiseren van het gegevensbeschermingsrecht.

- Verzamelwet gegevensverwerking VWS I: Wijziging van een aantal wetten op het terrein van het Ministerie van Volksgezondheid, Welzijn en Sport om de grondslagen voor gegevensverwerkingen te verstevigen.
- Verzamelwet gegevensverwerking VWS II: Wijziging van een aantal wetten op het terrein van het Ministerie van Volksgezondheid, Welzijn en Sport om de grondslag voor gegevensverwerkingen te verstevigen.

Het in detail duiden van de voorgenomen wijzigingen in detail voert te ver voor dit document.

Op grond van eerstgenoemde Verzamelwet zijn bijvoorbeeld wijzigingen in de UAVG voorgesteld omtrent toestemming en het intrekken daarvan door betrokkenen tussen 12 en 16 jaar oud en wijzigingen rondom overdracht van dossiers gedurende de behandeling en wanneer de behandeling is beëindigd.
In de Verzamelwet VWS I worden wijzigingen voorgesteld in bijvoorbeeld de Jeugdwet, Wet kwaliteit, klachten en geschillen zorg, Wet maatschappelijke ondersteuning 2015, Wet op de beroepen in de individuele gezondheidszorg, de gezondheidswet, de Wet verplichte geestelijke gezondheidszorg, de Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten, de Wet langdurige zorg, geneesmiddelenwet, en de Wet donorgegevens kunstmatige bevruchting. De belangrijkste wijziging voor al deze gevallen betreft de grondslag voor inzage; *"De met het toezicht belaste ambtenaren zijn, voor zover dat voor de vervulling van hun taak redelijkerwijs noodzakelijk is, bevoegd tot inzage van de dossiers van betrokkenen, het maken van kopieën daarvan en indien dat niet ter plaatse kan geschieden, de dossiers voor dat doel voor korte tijd mee te nemen tegen een door hen af te geven schriftelijk bewijs, of het vorderen van inlichtingen ter zake."*

In de Verzamelwet VWS II worden wijzigingen voorgesteld in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, de Wet langdurige zorg, de Wet kwaliteit, klachten en geschillen zorg, de Wet maatschappelijke ondersteuning 2015, de Wet op het RIVM, de Wet publieke gezondheid, de Wet verplichte geestelijke gezondheidszorg en de Zorgverzekeringswet. Dit betreft wijzigingen als heir beiden van grondslag voor het verwerken van het BSN van betrokkenen, toezicht en handhaving, een grondslag voor het CIZ om persoonsgegevens te verwerken en deze op verzoek – anoniem - aan de Minister te verstrekken als informatie ten behoeve van het te voeren beleid, een grondslag voor inzage in dossiers van cliënten van wie de vrijheid is ontnomen en een grondslag voor binnentredingsbevoegdheid, een grondslag voor een zorgkantoor om aan het gemeentelijk college informatie te verstrekken over ingangs- en einddatum van langdurige zorg de bewaartermijn voor persoonsgegevens door het CAK en het uitwisselen van persoonsgegevens tussen officieren van justitie, Wlz-uitvoerders, college van B&W, zorgverzekeraars, het CIZ, de Dienst Justitiële Inrichtingen en het Ministerie van Justitie en Veiligheid.

Het moge duidelijk zijn op grond van de verschillende Verzamelwetten voor de zorg veel wijzigingen in het verschiet liggen. Eenieder zal de op de eigen organisatie betreffende wetgeving in de gaten moeten houden.

4 Toenemende elektronische gegevensuitwisseling

4.1 Ontwikkelingen

Waar de Wet elektronische gegevensuitwisseling in de zorg (Wegiz) het wettelijk kader vormt voor de elektronische gegevensuitwisseling in de zorg, zal de NEN 7545 "Gegevensuitwisseling in de zorg – verpleegkundige overdracht" als normenkader de eisen bevatten voor de elektronische verwerking en uitwisseling van verpleegkundige informatie tussen zorginstellingen. Informatiestromen beperken zich immers niet alleen tot de eigen organisaties; er is sprake van ketens. Het normenkader richt zich op alle activiteiten voor het uitwisselen en verwerken van verpleegkundige informatie in gehele keten van de zorg. De norm is van toepassing op zowel de intra- als extramurale zorg, op cure en care.

Een andere belangrijke ontwikkeling die van belang is voor elektronische gegevensuitwisseling is NUTS, de naam van het samenwerkingsverband dat tot doel heeft om digitale gegevensuitwisseling tussen zorgorganisaties te faciliteren. Op basis van ontwikkelde open source software wordt het

hiermee voor zorgorganisaties mogelijk om specifieke gegevens van een client te delen met andere zorgorganisaties.

Van belang is de toenemende elektronische gegevensuitwisseling meer te bezien vanuit een risicoperspectief. Hierbij gaat het om het bepalen van de impact van verstoring van de elektronische gegevensuitwisseling. Wat zijn de gevolgen van verschillende scenario's die beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid raken? Het inschatten van de dreigingen en risico's, en op basis hiervan bepalen van de benodigde maatregelen en het opstellen van actieplannen. Relevant hierbij zijn:

- Eigen systemen en interfaces
- Externe interfaces
- Gemeenschappelijke ICT-producten (dus dezelfde technologie, ICT-/OT-systeem)
- Gemeenschappelijke diensten (datacenters of ICT-dienstverleners)

4.2 Wat betekent dit voor de praktijk

- Hanteer voor de inrichting van de externe gegevensuitwisseling de Handreiking Ketenaanpak van CIP-Overheid.
- Voer als organisatie een ketenrisicoanalyse uit; gebruik hiervoor de Handreiking Ketenrisicoanalyses van CIP-Overheid. Het gaat hier zowel om security- als privacyaspecten (DPIA).
- Stem met de ketenpartijen af welke onderdelen een gemeenschappelijk karakter hebben en een gezamenlijke risicoanalyse noodzakelijk maken.

5 Cyberweerbaarheid

5.1 Ontwikkelingen

In het in 2022 door Z-CERT gepubliceerde Cybersecurity Dreigingsbeeld Zorg 2021[1], en het in 2023 gepubliceerde Cybersecurity Dreigingsbeeld Zorg 2022, wordt ransomware als grootste dreiging genoemd. Een ransomware-aanval zal niet alleen de vertrouwelijkheid van (gevoelige) persoonsgegevens schaden, maar leidt direct tot onbeschikbaarheid. Dit kan in het geval van de zorg ook de persoonlijke veiligheid of gezondheid van mensen raken. Denk aan een client die overlijdt als gevolg van niet toegediende medicatie of een ambulance die moet uitwijken vanwege een hack. De

[1] https://www.z-cert.nl/wp-content/uploads/2022/02/Z-CERT_RapportDreigingsbeeld_2021.pdf

grotere afhankelijkheid van ICT maakt ook de risico's groter. Een ransomware-aanval heeft bovendien financiële gevolgen voor de organisatie.

Zorginstellingen in Nederland worden steeds vaker doelwit, waarbij aanvallen meer doelgericht en beter voorbereid plaatsvinden. Omdat deze aanvallen lucratief zijn, investeren criminelen hier ook steeds meer in.

Zorginstellingen kennen veelal een divers IT-landschap met dreigingen op veel verschillende gebieden; de toenemende elektronische gegevensuitwisseling tussen zorginstellingen stelt organisaties voor nog meer uitdagingen. Belangrijk is dat allereerst goede afspraken worden gemaakt tussen partijen om informatiebeveiligingsproblemen of incidenten binnen ketens het hoofd te kunnen bieden.

Effectieve cyberweerbaarheid gaat niet alleen over bewaken van eigen systemen om voorbereid te zijn op aanvallen (middels tijdige signalering van zwakheden in configuraties of programmatuur of overtredingen op gebied van compliance), maar ook over bewaking van stelsels en ketens. Het gaat om kwetsbaarheden die bij één organisatie kunnen beginnen en zich van daaruit naar andere organisaties kunnen verspreiden. Dit is met name een punt van aandacht voor sectoren, zoals de zorgsector, waarin organisaties een keten moeten vormen om zorgprocessen zo effectief en efficiënt mogelijk te laten verlopen.

Zorginstellingen kunnen zich niet veroorloven bij de invulling van cyberweerbaarheid alleen te focussen op de eigen organisatie, maar moeten zich meer richten op de keten waarvan ze deel uitmaken.

Cybersecurity begint met het ***identificeren*** *van wat er aan informatiesystemen en gegevensdragers aanwezig is, wie hier toegang toe hebben, aan welke bedreigingen deze zijn blootgesteld enzovoorts. Vervolgens neem je maatregelen om deze systemen te* ***beschermen*** *tegen het optreden en impact van de bedreigingen. Door middel van* ***detecteren*** *controleer je of deze bescherming nog steeds functioneert, wanneer een afwijking (bijvoorbeeld een te ruimte autorisatie) is aangetroffen moet je hierop kunnen* ***reageren****. Door middel van* ***herstel*** *breng je de beveiliging weer terug in de gewenste staat of voer je verbeteringen door.*

Belangrijk zijn:

- Begin met risico-inschatting
- Kies voor een geïntegreerde aanpak/oplossing waar zaken als ISMS, vulnerability management, kwaliteit van code, IDS/IPS, SIEM, etc. onderdeel van zijn en waarmee compliance aan gangbare standaards (bijvoorbeeld het NIST cybersecurity framework of CIS-controls kan worden aangetoond
- Kies voor een flexibele oplossing die optimaal aansluit bij de eigen context (infrastructuur, processen, keteninformatievoorziening)

- Borg dat ook aangesloten ketenpartijen aan de eisen voldoen en dit ook kan worden getoetst.
- Vul periodieke security- en kwetsbaarhedenscans aan met continue monitoring. Periodieke scans zijn een momentopname en geven geen volledig actueel beeld van de status van maatregelen bij aangesloten ketenpartijen.

Zie voor basismaatregelen op het gebied van cybersecurity ook de informatie van het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid.[2]

5.2 Kwetsbaarheden Analyse Tool

Het Ministerie van VWS heeft de zogenaamde Kwetsbaarheden Analyse Tool (KAT) ontwikkeld. Deze sluit aan bij de hiervoor geschetste aanpak. KAT is een open source oplossing waarin precies wordt bijgehouden welke kwetsbaarheid wanneer is geconstateerd. Zo kan snel worden herleid sinds wanneer een technische kwetsbaarheid speelt.

KAT heeft als doel het monitoren, registreren en analyseren van de status van informatiesystemen. KAT scant hiervoor netwerken, analyseert kwetsbaarheden en maakt daarvan goed leesbare rapportages. Het integreert de meest gebruikte netwerktools en scansoftware in een modulair framework, heeft toegang tot externe databases en combineert de informatie uit al deze bronnen overzichtelijk in de rapportages

Logboeken registreren alle gevonden activiteiten en acties. Deze gegevens worden forensisch accuraat (bewijsbaar) opgeslagen in een database. Gebruikers kunnen zelf business rules toevoegen. Veel business rules volgen echter uit standaarden. Alles wordt vastgelegd in een model, zodat de auditor de opzet, bestaan en werking live kan volgen en er op termijn complete dossiers uit kan halen. Met zo'n dossier kan worden aangetoond dat bevindingen tijdig en adequaat zijn opgevolgd.

KAT biedt mogelijkheden om voor welke onderzoeksperiode dan ook rapportages te genereren, conform internationale standaarden. KAT biedt de mogelijkheid om continue te monitoren. Hiermee kan direct worden vastgesteld of bevindingen zijn verholpen, hetgeen ook in de rapportage kan worden meegenomen. Op basis van een knowledge base worden resultaten gekoppeld aan de juiste context. Welk systeem betreft het? Welke processen worden hierdoor geraakt? Heeft de bevinding betrekking op techniek, compliance of iets anders? Is dit een eerder herkend risico? Op basis hiervan krijgt de bevinding een waarde en wordt het direct met de juiste prioriteit bij de juiste persoon gelegd.

[2] https://www.ncsc.nl/onderwerpen/basismaatregelen

Ontwikkeling en inrichting van KAT is geen eenvoudig proces. Maar wanneer KAT goed is ingericht, wordt in de operationele fase heel veel tijd bespaard. Immers, het leren kennen van resultaten in logboeken, van pentesttools of het koppelen van technische bevindingen aan risico's vraagt steeds opnieuw weer veel werk. Wanneer zaken goed zijn ingericht en het meeste voorwerk is gedaan, worden zaken herhaalbaar.

KAT is door VWS ontwikkeld en toegepast om aangesloten coronatest-aanbieders continu te toetsen op kwetsbaarheden. Uitslagen van scans kunnen ook aan elkaar worden verbonden. Dit maakt de tool ook bij uitstek geschikt om securitymonitoring uit te voeren op gegevensuitwisselingen in ketenverband, waarbij meerdere partijen informatie met elkaar delen, veelal gebruik maken van dezelfde voorzieningen en waarmee dus een onderlinge afhankelijkheid ontstaat. KAT biedt hiervoor de mogelijkheid om continu te monitoren om vast te stellen dat partijen ook de aansluitvoorwaarden naleven. [3]

5.3 Versterken van de beveiligingsketen

Als het gaat om elektronische gegevensuitwisseling, kan worden vastgesteld dat dit voor de zorgsector vaak in regionaal verband tot stand komt. Het gaat dan bijvoorbeeld om de afstemming tussen instellingen in de langdurige zorg, ziekenhuizen, apotheken en eerstelijns zorgverleners in de regio. Wanneer in een keten wordt samengewerkt door verschillende organisaties, dan volstaat het niet wanneer een organisatie in de keten alleen voor zichzelf risico's inschat. De organisaties in een keten zijn afhankelijk van elkaars inspanningen om risico's tot een acceptabel niveau terug te dringen. Dreigingsinformatie is doorgaans complex en door het delen ervan en het gezamenlijk analyseren en beoordelen, kan een compleet dreigingsbeeld voor de keten worden ontwikkeld. Bijzondere aandacht kan hierbij worden besteed aan gateways (HIS en KIS?), deelplatformen (Cross-enterprise Document Sharing, XDS), cloud- en SaaS-security, threat intelligence, risicomanagement, etc.

Een en ander roept de vraag op of ook de regionale samenwerkingsverbanden een rol kunnen en willen spelen bij het versterken van de beveiligingsketen, inclusief de relatie tussen de eerste- en tweedelijns zorgaanbieder.

[3] Zie hierover de website van KAT – Kwetsbaarheden Analyse Tool op https://openkat.nl/

5.4 Wat betekent dit voor de praktijk

Het bovenstaande leidt tot de volgende aanbevolen acties:

- Onderzoek of regionale samenwerkingsverbanden in de zorg (bijvoorbeeld RSO's) willen of kunnen ondersteunen en faciliteren bij het bundelen van de regionale kennis en kunde om zo gezamenlijk beter bestand te zijn tegen cyberdreigingen en risico's die gebaat zijn bij onderlinge afstemming en versterking, als het gaat om de regionale ketenzorg.
- Onderzoek aansluiting bij Z-CERT. Een zorginstelling kan zich bij Z-CERT melden om deelnemer te worden, ook zonder dat er afspraken zijn met de koepelorganisatie. Collectieve aansluiting is gerealiseerd voor NFU, NVZ en de Nederlandse GGZ. Momenteel is Z-CERT in gesprek met ActiZ en VGN om de mogelijkheden te verkennen voor een gezamenlijke aansluiting bij Z-CERT. En tevens worden de mogelijkheden onderzocht om via een regionale/ alternatieve constructie de 1e lijn te gaan bedienen, te beginnen met huisartsen en openbare apothekers.
- Ga na welke dienstverleners op gebied van security monitoring samen met Z-CERT de regionale organisaties kunnen ondersteunen. Diverse IT-Security partijen delen via het zogenaamde Zorg Detectie Netwerk (ZDN) al zorgspecifieke dreigingsinformatie met hun klanten uit de zorgsector.
- Toets of en hoe de dienstverlening kan worden aangevuld met andere onderdelen van informatiebeveiliging en privacy (bijvoorbeeld CISO/FG as a service, beheer ISMS, CSERT, ondersteuning leveranciersmanagement).

6 Bewustwording en gedrag

6.1 Ontwikkelingen

Uit internationaal onderzoek, zoals bijvoorbeeld het 2022 Data Breach Investigations Report van Verizon, weten we dat de menselijke factor vaak doelwit is bij digitale aanvallen. Daarnaast maken mensen natuurlijk wel eens fouten. En als de veilige manier van werken te onhandig of te moeilijk is, blijken er vaak olifantenpaadjes beschikbaar om de veilige werkwijze te kunnen omzeilen.

Om mensen digitaal weerbaarder te maken werken veel organisaties aan bewustwording. Aandachtspunt hierbij is dat puur bewustwording vaak niet genoeg is. Mensen weten bijvoorbeeld best dat ze niet moeten appen onder het autorijden. Maar ze doen het toch. Mensen weten vaak wel dat ze geen makkelijk te raden wachtwoord moeten gebruiken. Maar ook dat… doen ze toch. In de internationale Security-Awareness-gemeenschap is de afgelopen jaren dan ook de stap gezet van focus op bewustwording naar focus op gedrag. Ook is er meer aandacht voor risicoanalyse als basis voor de keuze van onderwerpen.

Alleen kennis zal in veel gevallen dus niet direct leiden tot gedragsverandering. Toch is een basisniveau van kennis een voorwaarde om informatieveilig gedrag te stimuleren. Dit helpt medewerkers om slimmere keuzes te maken met betrekking tot informatieveiligheid en privacy. Ook kunnen zij vragen van patiënten/cliënten over dit onderwerp beantwoorden.

Kern van NEN 7510 is het in kaart brengen van risico's, het nemen van maatregelen en het vaststellen of deze maatregelen doeltreffend zijn: is de informatie nu echt veiliger? Bij bewustwording worden vaak alleen de inspanningen gemeten: x-aantal mensen heeft een training bijgewoond of e-learning voltooid, x-aantal berichten op intranet geplaatst, x-aantal posters opgehangen. Dit zegt niets over de doeltreffendheid, we weten niet of de informatie nu beter beschermd is. Meten is essentieel om te weten of acties doeltreffend zijn. Niemand wil toch kostbare tijd van zorgverleners verspillen met niet-effectieve bewustwordingsacties?

6.2 Wat betekent dit voor de praktijk

Voor een doeltreffende aanpak van de menselijke factor in informatiebeveiliging en privacy is een planmatige aanpak, gebaseerd op risicoanalyse, met gecombineerde inzet van bewustwordings- en gedragsinterventies noodzakelijk, waarbij resultaten gemeten worden.

7 Legacysystemen

7.1 Ontwikkelingen

Een legacysysteem is een (technisch) verouderd computersysteem. Met het begrip legacysysteem wordt zowel legacysoftware als legacyhardware bedoeld. Legacysystemen komen op veel plaatsen voor binnen de ICT, maar nog meer bij de operationele technologie (OT) waarvan binnen de zorg veelvuldig gebruik wordt gemaakt. Redenen waarom legacysystemen hierbij vaak nog in stand worden gehouden, zijn:

- Prijzen van apparatuur die wordt gebruikt, waren vaak hoog. Deze kennen veelal een lange afschrijvingstermijn;
- Veel systemen worden real-time gebruikt; systemen zijn helemaal geoptimaliseerd op performance en betrouwbaarheid. Wijzigingen in systemen kunnen dit sterk negatief beïnvloeden
- Bij wijzigingen ontstaan vaak compatibiliteitsproblemen
- Updaten van OT-producten is vaak veel complexer dan in het geval van ICT

Legacysystemen bedreigen echter wel de digitale veiligheid; er wordt veelal geen support meer geleverd, er zijn geen securitypatches meer voor het besturingssysteem, maar ook is het lastiger om kennis van het product binnen de organisatie up-to-date te houden. Ook kunnen legacysystemen vaak niet mee met noodzakelijke veranderingen binnen de overige infrastructuur in de organisatie. Het is niet alleen een risico voor de stabiliteit en betrouwbaarheid, maar ook een rem op noodzakelijke innovaties.

Het legacyprobleem in de zorg is niet alleen een probleem van de zorginstellingen zelf, maar ook een probleem van IT-leveranciers in de zorg. Veel geleverde software bevat legacy-componenten; echter, vernieuwing vraagt van leveranciers ook tijd en investeringen. In een relatief kleine Nederlandse zorgmarkt voor IT.

Een groot probleem hierbij is dat het probleem vaak moeilijk tastbaar te maken is. Door ervaring weet men de oude "IT" nog wel werkend te houden en dan lijkt het probleem niet te bestaan. Dan kan de verleiding om te investeren in nieuwe functionaliteiten in plaats van vervangen van bestaande, groot zijn.

7.2 Wat betekent dit voor de praktijk

- Beoordeel de specifieke risico's die samenhangen met het gebruik van de legacysystemen en maak een keuze over hoe met deze risico's om te gaan: uitfaseren, mitigerende maatregelen, risico accepteren of een combinatie hiervan;
- Voorbeelden van mitigerende maatregelen zijn het extra beschermen van legacysystemen, het isoleren van legacysystemen van internet, legacysystemen op een apart netwerksegment zetten, uiteraard met toegang via een firewall.
- Zorg ervoor dat vervanging van legacysystemen onderdeel is van een meerjarig plan voor IT-investeringen; maak het probleem behapbaar en koppel het eventueel aan kleine stappen;
- Ontwikkel een multi-leverancier strategie, opdat de organisatie niet te afhankelijk is van één leverancier; overweeg de inzet van SaaS-toepassingen (bij leveranciers met een actieve update en upgrade strategie) wanneer hierdoor uitfasering van legacysoftware kan worden versneld.

8 Security - en privacy by design

8.1 Ontwikkelingen

Innovaties kunnen op gespannen voet staan met security- en privacyoverwegingen. Soms lijkt dit een vrije val, maar het staat en valt met een goede voorbereiding, het uitvoeren van de juiste controles en het bepalen van mitigerende maatregelen. Innovatie is voor de zorg van cruciaal belang, maar alleen door het juist toepassen van security en privacy by design kan worden bereikt dat innovatie ook bestendig is voor de toekomst.

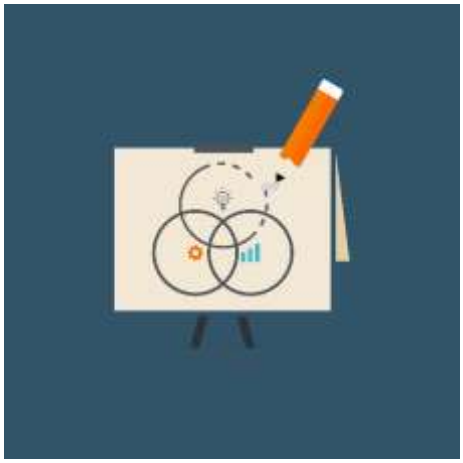
Om security en privacy by design goed toe te passen, zijn de onderstaande punten van belang:

- Betrek de doelgroep; het is van belang te weten wat zij wel of niet belangrijk vinden wanneer het gaat om de beveiliging van hun persoonsgegevens en borging van de privacy
- Gebruik bij data van cliënten/patiënten altijd een versleutelde verbinding
- Sla deze data altijd versleuteld op
- Gebruik tijdens de ontwikkeling altijd de OWASP[4] guidelines en kijk met name naar de top 10 van meest geïdentificeerde security risico's binnen de applicatieontwikkeling; borg dat leveranciers zich hieraan conformeren
- Wees transparant naar gebruikers en betrokkenen over de verwerking van hun persoonsgegevens

[4] Open Worldwide Application Security Project, zie https://owasp.org

- Zorg ervoor dat de privacyverklaring ook up-to-date is
- Zorg dat documentatie op orde is; dit betreft de gemaakte keuzes met betrekking tot security en privacy, maar ook de uitgevoerde risicoanalyse(s) en eventuele DPIA. Niet alleen de keuze is van belang, maar zeker ook de onderbouwing.

Een grote uitdaging is dat zorginstellingen gebruik maken van oplossingen die al langer in gebruik zijn en dateren van voor het in werking treden van de AVG. Alhoewel aan deze oplossingen dezelfde eisen worden gesteld, is het lastiger deze eisen alsnog in te (laten) bouwen. Typerend is dat er nog steeds zorginformatiesystemen zijn die het principe van dataminimalisatie niet ondersteunen, omdat het vereiste bewaartermijnenbeleid niet adequaat is ingericht. Dit betekent voor de zorginstellingen vaak veel handmatig werk, waardoor het in veel gevallen nauwelijks mogelijk is om aan dit beleid te voldoen. Een uitdaging die prangend wordt, wanneer bij de herziening van de NEN 7510 bewaartermijnen ook meer aandacht krijgen.



8.2 Wat betekent dit voor de praktijk

- Zorg ervoor dat binnen de organisatie security en privacy integraal onderdeel zijn van de ontwerpstrategie van nieuwe producten, processen, systemen en technieken. Dit kan onder andere door het op te nemen in formats voor bijvoorbeeld projectplannen.
- Kies voor oplossingen waarvan de leverancier kan aantonen dat privacy en security by design zijn toegepast, en dat processen waarborgen dat dit ook zo blijft.

9 Rollen en verantwoordelijkheden

9.1 Ontwikkelingen

Zorginstellingen kwalificeren volgens verschillende rollen, op verschillende momenten en functies binnen de zorgketen. Zij kunnen verwerkingsverantwoordelijke of gezamenlijk verwerkingsverantwoordelijke zijn. Zij maken gebruik van een groot aantal verwerkers die op hun beurt sub-verwerkers inschakelen. Zij geven persoonsgegevens door aan meerdere instanties. Iedere rol vraagt om een adequate vastlegging daarvan binnen de gehele keten. Het inrichten van een sluitend Register van

Verwerkingen draagt bij aan kennis over welke verwerkingen plaatsvinden binnen de instelling en welke documenten daarvoor moeten worden ingericht.

Pas wanneer de verwerkingen op de juiste wijze in beeld zijn gebracht, kunnen goede afspraken worden gemaakt over 'eigenaarschap' van gegevens en de geautoriseerde toegang daartoe.

Bij gegevensverwerkingen zijn veelal meerdere interne afdelingen betrokken maar daarnaast veelal ook externe partijen. Hierdoor kunnen complexe ketens ontstaan, waarbij in iedere schakel voldoende aandacht moet zijn voor informatiebeveiliging en bescherming van de privacy. Er kan sprake zijn van complexe afhankelijkheden en wisselende relaties tussen partijen. Het is juist dan belangrijk om goede afspraken te maken om incidenten te voorkomen en deze efficiënt op te lossen wanneer ze zich voordoen. Allereerst dienen alle betrokken partijen in beeld te zijn. Vervolgens moet worden gekeken naar zowel de eigen wettelijke verantwoordelijkheden, als de verantwoordelijkheden die onderling verdeeld moeten worden. De AVG maakt onderscheid tussen partijen in de rol van verwerkingsverantwoordelijke en die van verwerker.

Het uitgangspunt bij een ketensamenwerking moet zijn dat er duidelijke informatiekanalen en aanspreekpunten zijn. Dit gaat verder dan de relatie tussen verwerkingsverantwoordelijken onderling en tussen verwerkingsverantwoordelijke en verwerker. Het gaat ook over de vraag wie betrokkenen kunnen benaderen, hoe hun rechten worden gewaarborgd, wie de lead neemt in geval van beveiligingsincidenten, datalekken, etc., wie op dat moment relevante contactpersonen zijn, hoe wordt omgegaan met aansprakelijkheid en geheimhouding, op welke manier kan worden vastgesteld dat afspraken worden nageleefd en hoe de ketensamenwerking ook op een zorgvuldige manier weer kan worden beëindigd.

9.2 Wat betekent dit voor de praktijk

- Leg de afspraken over de hiervoor genoemde onderwerpen goed vast in een onderlinge regeling
- Stel vast op welke wijze de naleving van de afspraken kan worden geborgd
- Ga na of het regionale samenwerkingsverband hier een rol in kan spelen

10 Leveranciersmanagement

10.1 Ontwikkelingen

Door krapte op de arbeidsmarkt is het lastig om voldoende kennis en ervaring binnen de eigen organisatie te werven en te behouden. De rol van systeembeheerder bij zorginstellingen is geleidelijk aan het verdwijnen. IT is in toenemende mate een dienst die wordt ingekocht bij externe partijen. Hiermee wordt alsnog extra benodigde expertise verkregen. Dit kan een vals gevoel van veiligheid geven. Bovendien blijft de instelling zelf verantwoordelijk voor de uitvoering. De afhankelijkheid van leveranciers maakt de instelling ook kwetsbaarder.

Omdat zorginstellingen voor hun informatievoorziening steeds meer afhankelijk zijn van hun ICT-leveranciers, is een goede regie hierop van cruciaal belang. Het succes hiervan is een optelsom van professionele inkoop, goed georganiseerd contractbeheer en monitoren van afspraken (leveranciersmanagement).

Er dient derhalve te worden zorggedragen voor een goede governance-structuur waarmee controle kan worden uitgevoerd op leveranciers. Daarnaast dienen afspraken over privacy en security in elk leverancierscontract te worden vastgelegd.

Het hoge tempo van de digitale transformatie heeft bovendien als effect dat steeds meer (zorg)organisaties overstappen naar applicaties via het Software as a service-model, waarmee een organisatie (relatief) snel up-and-running kan zijn. Daarnaast is SaaS (nog) relatief goedkoop vanwege de schaalvoordelen op de licentiekosten van hard- en software bij aanvang, en daarna bij beheer en onderhoud. Voorts levert op- en afschalen van gebruikers veel minder kopzorgen en is men als gebruiker verzekerd van de laatste beveiligingsupdates en functionaliteiten, al dan niet gedreven vanuit technologische innovaties. Alhoewel (grote) SaaS-aanbieders een beveiligings- en beschikbaarheidsniveau kunnen leveren die maar door weinig organisaties kunnen worden geëvenaard met een eigen IT-infrastructuur, kent dit voordeel ook een nadeel. Bij de overstap van zorginstellingen naar SaaS-oplossingen komen er veel meer eieren in een mandje te liggen. Immers, als het fout gaat bij de SaaS-leverancier zijn er meteen meerdere zorgorganisaties getroffen. Meer dan wanneer organisaties allemaal zouden beschikken over een eigen on-premise (applicatie) infrastructuur.

De NEN 7510 schrijft voor dat zorginstellingen hun (SaaS)leveranciers met regelmaat moeten monitoren, beoordelen en auditen (Trust Nothing). Meer SaaS betekent meer leveranciers-management, en dat houdt meer werkdruk in. Verify Everything is zeer bewerkelijk. Door hier gezamenlijk in op te trekken kan de druk voor zowel zorgorganisaties als aanbieders verminderd worden. Partijen zijn daarom gebaat bij krachtenbundeling richting leveranciers.

10.2 Wat betekent dit voor de praktijk

- Ondersteun zorgorganisaties bij de ontwikkeling van een visie op inkoop van ICT- middelen.
- Pas bij inkoop de inkoop wizard van CIP-Overheid toe.
- Zorg dat eisen op gebied van informatiebeveiliging en privacy worden meegenomen in inkoopcontracten
- Ontwikkel service- en contractmanagement
- Bewerkstellig dat zorginstellingen zoveel mogelijk samen optrekken richting leveranciersmarkt; in het verleden hebben ziekenhuizen bijvoorbeeld besloten samen op te trekken richting leveranciers. Hieruit is Stichting Intrakoop voortgekomen die zich echter nog beperkt bezighoudt met ICT, informatiebeveiliging en privacy. Onderzoek of op deze gebieden de samenwerking op dit gebied allereerst vanuit de regionale organisaties kan plaatsvinden, aangevuld met een meer structurele samenwerking tussen deze organisaties.
- Onderzoek voor inkoop van ICT-diensten en informatiebeveiliging de mogelijkheden van een leveranciers prestatiemeting, waarmee de prestaties van leveranciers kunnen worden gemeten. Hiermee kan ook inzichtelijk worden gemaakt hoe tevreden collega-zorginstellingen zijn over leveranciers en hun producten.
- Kies voor oplossingen waarvan de leverancier kan aantonen dat processen rondom informatiebeveiliging op orde zijn en continu worden verbeterd. Bij voorkeur beschikt de leverancier over certificering voor de internationaal erkende ISO 27001 en/of NEN 7510.
- Kies voor oplossingen waarvan de leverancier kan aantonen dat processen rondom privacy op orde zijn en continu worden verbeterd. En bijvoorbeeld beschikt over de ISO 27701 en ISO 27018 certificaten.

11 Totstandkoming van dit document

Dit document is tot stand gekomen onder auspiciën van Stichting IP-Zorg.

- Douwe de Jong
- Nico Keijser
- Martine van de Merwe
- Peter van der Zwan

Met bijdragen van

- De kennispartners van IP-Zorg
    - Isatis Cyber Security
    - Infozorg BV.
    - Niveo
    - Pinewood
    - Trustboud GRC
- ECP | Platform voor de InformatieSamenleving
- Ivo van Heeren
- Cees van der Wens
- De deelnemers aan de workshop van 18 april 2023

Stichting IP-Zorg
Zaagmolenlaan 4
3447 GS Woerden
KvK 76097854

Illustraties: iStock en Pixabay
Vormgeving: Idee Management