September | 15

De top 20 veiligheidsmaatregelen voor leveranciers van software voor WZC's

Peter Berghmans

In dit document wordt een overzicht gegeven van de 20 belangrijkste maatregelen die een leverancier dient te nemen om conform met de voorwaarden voor informatieveiligheid software kan integreren in een omgeving waar de Circle of Trust van toepassing is.

1. Inleiding

Wanneer een woonzorgcentra deel uitmaakt van de vertrouwensketting, Circle of Trust, dient het te voldoen aan een aantal veiligheidsvoorwaarden. Deze voorwaarden zijn zowel technisch als organisatorisch van aard. Leveranciers die de woonzorgcentra helpen bij de verwerking van de gegevens, dienen eveneens de nodige waarborgen te bieden.

Deze nota bevat een aantal waarborgen die een leverancier van software én ondersteunende onderhouds- en support taken dient te voorzien in de verdere realisatie van haar aanbod voor woonzorgcentra. de veiligheidsvoorwaarden zijn onderverdeeld in 3 onderdelen:

1. Informatieveiligheid tijdens het ontwerp van de software
2. Informatieveiligheid na het in productie stellen van de software
3. Organisatorische maatregelen voor informatieveiligheid

2. Informatieveiligheid tijdens het ontwerp van software

Wanneer software wordt ontworpen voor Woonzorgcentra waarbij persoonsgegevens van bewoners worden verwerkt, gelden onderstaande principes.

Principe	Toelichting	Hints
1. Informatie wordt in de software beschermd (at rest) in overeenstemming met de gevoeligheid van de gegevens	Bij het ontwerp van de software gaat de ontwikkelaar na welke gegevens in de toepassing worden verwerkt. Afhankelijk van het gegevenstype wordt de data voorzien van de nodige beveiliging m.b.t. toegang, logging, encryptie edm.	De classificatieindex zelf is opgenomen in bijlage 1 van deze nota.
2. Wanneer gegevens worden in transit zijn, wordt deze beveiligd volgens de opgestelde beveiligingsmatrix	Wanneer informatie wordt uitgewisseld tussen verschillende systeemcomponenten of systemen, al dan niet onder beheer van dezelfde leverancier, gelden specifieke eisen inzake authenticatie, encryptie van de data en het transportkanaal. De beveiligingsmatrix geeft aan wanneer welke maatregel van toepassing is.	De beveiligingsmatrix is opgenomen in bijlage 2
3. De software wordt voorzien van een privacy logging	- De logging wordt voorzien in overeenstemming van de classificatieindex (zie hoger) - De toegang tot deze logging is geregeld volgens het need-to-know principe - De integriteit van de logging is beschermd - De loggings voldoen aan de wettelijke bewaartermijn - De leverancier licht toe hoe de logging door het woonzorgcentrum kan worden gecontroleerd.	Privacy logging verschilt van systeemlogging (technische logging). Het geeft aan wie welke persoonsgegevens verwerkt en welke verwerking plaatsvond.
4. Behandeling van het eHealth certificaat	De omgang met het eHealth certificaat voldoet aan de voorschriften van eHealth zelf.	De regels voor de behandeling van het certificaat zijn gepubliceerd door eHealth en worden in bijlage 3 verder behandeld.

5. Installatie van geprivilegieerde toegangen	Bij de installatie van de software kijkt de leverancier er op toe dat wachtwoorden - voor geprivilegieerde toegang steeds verschillend is per woonzorgcentrum. - die gebruikt worden bij het uitwisselingsproces tussen verschillende systeemcomponenten, verschillend is tussen verschillende klanten - wachtwoorden die horen bij services bij voorkeur worden behandeld als managed service accounts	Managed service accounts: https://technet.microsoft.com/nl-be/library/hh831451
6. Voorwaarden bij de opslag van wachtwoorden van gebruikers	- De leverancier voorziet in een veilige procedure voor het uitreiken en de herinitialisatie van gebruikerswachtwoorden. - De leverancier voorziet in veilige wachtwoordcontainers zoals het principe van salted password hashing	Hashing: https://crackstation.net/hashing-security.htm
7. Voorwaarden bij gegevensopslag in een multi tenant omgeving	Gegevens van verschillende woonzorgcentra worden opgeslagen in een eigen databank of in een eigen schema op een gemeenschappelijke databank. Er is geen enkele andere overdracht van gegevens tussen de tenants, tenzij via het eHealth platform.	Wanneer iedere tenant gebruik maakt van een eigen schema, voorziet en documenteert de leverancier duidelijke afscheidingsregels
8. Principes voor veilige ontwikkeling van software	- De leverancier hanteert waakt erover dat veilige ontwikkelprincipes worden gevolgd (vb vermijden van OWASP kwetsbaarheden) - De leverancier zorgt voor een veilige OTAP straat.	OTAP=Ontwikkel, Test, Acceptatie en Productie
9. Principes voor de installatie van software in een veilige netwerkomgeving	De installatie van de software in productie wordt geïnstalleerd op een beveiligd netwerk. Persoonsgegevens mogen niet rechtstreeks worden ontsloten op het internet, maar worden afgeschermd via een WAF. Databanken zijn niet rechtstreeks opvraagbaar.	WAF = Web Application Firewall Het netwerk van het WZC wordt op regelmatige tijdstippen gecontroleerd op zwakheden (verantwoordelijkheid WZC). Voor het netwerk van de cloud omgeving gelden dezelfde principes.
10. Kwetsbaarheids-analyse	Elke via het publieke internet toegankelijke component dient een periodieke kwetsbaarheidsanalyse te ondergaan voor het in productie nemen van de software. De resultaten hiervan zijn ter beschikking van het WZC voor installatie en worden op geregelde tijdsstippen herhaald (vb Qualys, Nessus)	Zonder de kwetsbaarheidanalyse is het veiligheidsniveau van de toepassing ongekend.
11. Penetratietest	Wanneer de software wordt aangeboden in een cloud omgeving, is deze voorzien van een logische scheiding tussen verschillende woonzorgcentra. In het kader van Circle of Trust dient voorafgaand aan de in productiestelling via een penetratietest te worden aangetoond dat de scheiding tussen de omgevingen kan worden gegarandeerd - Tijdens deze penetratietest wordt tevens de authenticatie nagegaan van de eindgebruiker ten aanzien van de cloudomgeving waartoe deze toegang heeft (en bijgevolg de kans dat deze gebruiker via authenticatie andere omgevingen kan benaderen).	Wanneer dergelijk verkeer mogelijk zou zijn, dan doorbreekt men het principe van de Circle of Trust.

	- Tijdens deze penetratietest wordt nagegaan welke de kans is dat met een ander eHealth certificaat kan worden aangemeld op Vitalink/Belrai	
12. Structuur van de gegevens	De leverancier documenteert de Data Lifecycle Management van de gegevens die de software verwerkt. Hierbij wordt in kaart gebracht op welke manier datacreatie (via gebruikers of andere input kanalen), dataflow, dataopslag en destructie van gegevens wordt gerealiseerd. Ook data export op vraag van de klant komt aan bod.	

3. Informatieveiligheid voor software in productie

Principe	Toelichting	Hints
13. Regelmatige kwetsbaarheids- en penetratietesten	Wanneer software publiekelijk op internet beschikbaar is, wordt deze op regelmatige tijdstippen en minstens jaarlijks onderworpen aan een kwetsbaarheid en/of penetratietest.	De classificatieindex zelf is opgenomen in bijlage 1 van deze nota.
14. Afspraken over onderliggende systeemcomponenten en onderhoud	Het WZC en de leverancier maken afspraken over het systeemonderhoud, backup, continuïteitsplannen en malware beveiliging	
15. Incidentbeheer voor informatieveiligheid	- Wanneer de leverancier de ICT omgeving van het bewonersdossier operationeel ondersteunt, is een incidentbeheer nodig dat zowel proactief (voorkomen van incidenten, bijvoorbeeld door opvolgen van loggings inzake veiligheid) als retroactief (een uitgewerkt incidentafhandelingsplan) noodzakelijk, inclusief alle bepalingen rond de betrokkenheid van het WZC bij het afhandelen van incidenten. - Het incidentbeheer wordt opgevolgd door de Security Operator	Het WZC blijft verantwoordelijk voor de nadelige gevolgen van een incident (vb lekken van de gegevens van bewoners). Het WZC dient aan te tonen op een correcte manier dergelijke incidenten te kunnen identificeren en afhandelen, maar kan dit niet als er geen garanties van de leverancier bestaan.
16. Toegang tot de gegevens van het WZC	- De leverancier is ten allen tijde in staat om na te gaan wie op welk tijdstip toegang heeft gehad tot de gegevens van het WZC en kan op vraag een nominatieve lijst ter beschikking geven wie potentieel toegang zou kunnen hebben tot deze gegevens. Deze regels zijn zowel van toepassing op personeelsleden van de leverancier als op subcontracters en onderaannemers - De leverancier zorgt voor strikte en gedocumenteerde toegangsregels en technische maatregelen voor de toegang tot gegevens van woonzorgcentra.	De toegang tot gegevens die de gezondheid betreffen is nominatief (KB 2001). Het niet kunnen antwoorden op de gestelde vragen is een breuk in de Circle of Trust.

4. De organisatie van informatieveiligheid bij de leverancier

Principe	Toelichting	Hints
17. Het uitwerken	- Wanneer de software operationeel wordt ondersteund	Krachtens artikel 16 blijft het

van een veiligheidsbeleid en -plan	door de leverancier, dient deze te beschikken over een veiligheidsbeleid en -plan. Alle veiligheidsprocedures dienen te worden geformaliseerd en de maturiteit moet worden kenbaar gemaakt volgens de principes van ISO 27000. Het veiligheidsbeleid en -plan wordt opgevolgd door een Security Operator. - Voor de leverancier in de cloud levert de leverancier de resultaten op van de cloud evaluatie tool van SMALS en documenteert deze.	WZC verantwoordelijk voor de veiligheid. Het ontbreken van een veiligheidsbeleid gestoeld op ISO 27000 geeft het WZC onvoldoende garanties
18. Verwerkers-overeenkomst, ICT contract en afsprakennota infoveiligheid	Er dient een verwerkersovereenkomst te worden opgesteld tussen de leverancier en het WZC (een voorbeeld is uitgewerkt in het e-WZC project), een ICT contract en een afsprakennota voor informatieveiligheid. Modellen van deze nota's zijn beschikbaar (zie hoger)	Dit is een bepaling van de privacywet (artikel 16), evenals een voorwaarde voor Vitalink
19. Omgang met medewerkers van de leverancier	De leverancier zorgt ervoor dat personeelsleden worden ingelicht over de geldende principes van informatieveiligheid en privacy en controleert de toepassing van de regels voorafgaand en tijdens het dienstverband. De toegangen van personeelsleden worden ontnomen wanneer een personeelslid vertrekt.	
20. Omgang met subcontractors	- De leverancier zorgt ervoor dat subcontractors worden ingelicht over de geldende principes van informatieveiligheid en privacy en controleert de toepassing van de regels voorafgaand en tijdens het contract. - De leverancier dwingt alle onderhavige maatregelen af bij de leverancier - De leverancier informeert het woonzorgcentrum over de identiteit van de subcontractors en diens toegang tot informatie.	

Bijlage 1: Classificatie van informatie

Wanneer informatie wordt verwerkt in een toepassing, dan dient de informatie te worden beschermd in overeenstemming met het classificatieniveau ervan. We hebben het in dit geval over een primaire verwerking, met name de verwerking in de software waarin de gegevens initieel door de gebruiker worden ingegeven. Typisch het bewonersdossier.
Een overzicht van de classificatieniveaus kan je vinden in deze bijlage. De niveaus helpen om het juiste beveiligingsniveau te kiezen. Hieronder worden een aantal voorbeelden gegeven voor de toepassing ervan:
Vb 1: Administratieve gegevens van een bewoner zijn volgens het classificatieniveau 'persoonsgegevens'. Deze gegevens zijn in een applicatie steeds voorzien van logging op aanmaak, wijziging, verwijdering van de gegevens. Bovendien zijn deze gegevens enkel toegankelijk het aanmelden van een gebruiker met zijn of haar persoonlijk wachtwoord.
Vb 2: Kwaliteitsgegevens van een woonzorgcentrum zijn 'vitale gegevens' en zijn tevens 'unieke bron'. Overeenstemmend met deze classificatie zijn de gegevens in een applicatie dienen de gegevens te worden ingegeven na unieke identificatie van de gebruiker. Eenmaal gevalideerd worden de gegevens voorzien van een hash, zodat het wijzigen van de gegevens na validatie steeds opspoorbaar is. Aangezien de gegevens uniek zijn, is de backup van de gegevens gegarandeerd.
Vb 3: Medicatiegegevens van een bewoner vallen onder het 'beroepsgeheim', ze zijn bovendien 'vitaal' en 'proceskritisch'. Deze gegevens zijn in een applicatie steeds voorzien van logging op aanmaak, consulteren, wijzigen, verwijderen van de gegevens. Bovendien zijn deze gegevens enkel toegankelijk het aanmelden van een gebruiker met zijn of haar persoonlijk wachtwoord. De gebruiker valt bovendien onder het beroepsgeheim. Eenmaal een medicatieschema is gevalideerd worden de gegevens voorzien van een hash, zodat het wijzigen van de gegevens na validatie steeds opspoorbaar is. De software bevat een exportfunctie waardoor gegevens snel toegankelijk zijn wanneer gegevens niet beschikbaar zijn.
Vb 4: Het consent van een bewoner is een gegeven die beschikbaar is in de authentieke bron. Bijgevolg mag het gegeven niet lokaal worden bewaard maar dient het te worden opgevraagd bij de authentieke bron. Dit gebeurt telkens bij initiatie van een verwerkingsflow (een handeling).
Vb 5: Het formularium van een apotheek krijgt het label 'referentie'. Dit betekent dat wijzigingen aan deze gegevens strikt worden gecontroleerd door de verificatie van de gebruiker en logging. Bovendien wordt een versiegeschiedenis bijgehouden van de wijzigingen.
Vb 6: Een transfertdocument valt onder het 'beroepsgeheim', is vitaal en proceskritisch. Ze worden op dezelfde manier behandeld als de medicatiegegevens.

1 Informatie kan worden onderverdeeld worden in onderstaande klassen

Vertrouwelijkheid — Dit label verwijst naar de exclusiviteit van de verwerker van de gegevens. Volgende onderverdelingen worden voorzien binnen deze dimensie:

- **Persoonsgegevens**: Indien deze informatie wordt verspreid, dan is de persoonlijke levenssfeer van een persoon aangetast.
- **Beroepsgeheim**: Het inkijken van deze gegevens of het verspreiden ervan is strafbaar zoals bedoeld in artikel

458sw. Toegang tot de gegevens kan enkel als de actor tot de circle of trust behoort.
- **Niet bepaald**: geen buitengewoon risico. Er wordt gerekend op de het goede huisvader principe van de verwerker.

Betrouwbaarheid — Dit label behandelt de integriteit, juistheid, volledigheid, authenticiteit en bewijskracht van informatie. Volgende onderverdelingen worden voorzien binnen deze dimensie:
- **Vitaal:** Indien deze gegevens worden gemanipuleerd of gewijzigd, heeft dit zware gevolgen voor de behandeling van de bewoner, medewerker of de organisatie
- **Referentie:** Indien gemanipuleerd of gewijzigd, dan heeft dit een gevolg op het aanbod van producten en diensten en de gegevensstructuur
- **Niet bepaald**: geen buitengewoon risico. Er wordt gerekend op de het goede huisvader principe van de verwerker.

Beschikbaarheid — Dit label behandelt de continuïteit, tijdigheid, toegankelijkheid en ophaalbaarheid van informatie. Volgende onderverdelingen worden voorzien binnen deze dimensie:
- **Unieke bron:** Indien verloren gegaan of verduisterd, kan dit gevolgen hebben voor de wettelijke of zorgkundige aantoonbaarheid van een behandeling of zorgproces
- **Proceskritisch:** Indien niet toegankelijk, heeft dit zware gevolgen voor het zorgproces of een kritisch bedrijfsproces.
- **Niet bepaald**: geen buitengewoon risico. Er wordt gerekend op de het goede huisvader principe van de verwerker.

2 Overeenkomstig de hogergenoemde informatieklassen, worden passende maatregelen genomen

Persoonsgegeven
- Toegang is beperkt tot een strikt nominatieve lijst
- Toegang is nominatief
- De toegang is afgeschermd met een persoonlijk wachtwoordbeleid
- Logging op aanmaak, wijziging, verwijdering van de gegevens
- Gegevens worden geëncrypteerd bij transmurale uitwisseling

Beroepsgeheim
- Toegang is beperkt tot een strikt nominatieve lijst
- De toegang is nominatief
- De toegang is afgeschermd met een persoonlijk wachtwoordbeleid
- Toegang is beperkt voor zij met een aantoonbare therapeutische relatie met de bewoner
- Logging op aanmaak, consulteren, wijzigen, verwijderen van gegevens
- Gegevens worden geëncrypteerd bij intra- en transmurale uitwisseling

Vitaal	• Een strikt nominatieve lijst personen mogen de gegevens wijzigen • Herhaaldelijk wijzen op de registratieplicht en de nauwkeurigheid bij de verwerking • Wijzigen of manipuleren van de gegevens is opspoorbaar vb door een timestamp en hashing • Gegevens mogen niet worden gedupliceerd zonder goedkeuring • Volledigheid en correctheid van de gegevens wordt gecontroleerd bij gegevensoverdracht (vb via een hash principe), zowel intra als transmuraal.
Referentie	• Een strikt nominatieve lijst personen mogen de gegevens wijzigen • Wijziging van de gegevens volgt een goedkeuringsflow binnen het woonzorgcentrum en/of met externe communicatiepartners • Versiegeschiedenis wordt bijgehouden en is zichtbaar bij consultatie van de gegevens • Volledigheid en correctheid van de gegevens wordt gecontroleerd bij gegevensoverdracht (vb via een hash principe), zowel intra als transmuraal.
Unieke Bron	• Gegevens worden voorzien van een backup • De backup is voorzien van een versiegeschiedenis • Gegevens mogen pas worden vernietigd na het verstrijken van de wettelijke termijn en door een beperkt en nominatief aantal personen
Proceskritisch	• Gegevens kunnen op een zo kort mogelijke tijd worden gerecupereerd • Gegevens worden op een zo kort mogelijke tijd opnieuw beschikbaar gesteld • Zelfbeschikbaarheid van de gegevens wordt maximaal gevrijwaard.

Bijlage 2: De beveiligingsmatrix.

Eenmaal gegevens buiten de toepassing/applicatie – typisch het bewonersdossier - worden verwerkt, zijn ze in transit. Het betreft volautomatische transferts, al dan niet geïnitieerd door een gebruiker. In dit geval gelden specifieke veiligheidsmaatregelen. We maken bij de beoordeling van het veiligheidsniveau een onderscheid tussen gegevens die worden uitgewisseld tussen systemen die vallen onder een gemeenschappelijk veiligheidsbeleid en deze die worden uitgewisseld tussen systemen die niet onder een gemeenschappelijk veiligheidsbeleid vallen. Bijvoorbeeld een uitwisseling tussen systemen van een groepering van woonzorgcentra die zich in een gemeenschappelijke ICT infrastructuur (vb zelfde datacenter en zelfde ICT leverancier) bevinden vallen onder de noemer 'gemeenschappelijk veiligheidsniveau'. Een woonzorgcentrum dat informatie uitwisselt met bijvoorbeeld Pyxicare is een uitwisseling tussen systemen met een verschillend veiligheidsbeleid.
Om de te nemen veiligheidsmaatregelen vast te leggen bespreken we telkens de authenticatie (hoe zender en ontvanger worden geïdentificeerd, de beveiliging van de gegevens tijdens transport (data@move), het transportkanaal en de gegevensopslag in secundaire orde (data@rest). Met secundaire orde bedoelen we dat een dataset wordt gegenereerd vanuit het EBD en doorgestuurd wordt naar een andere toepassing. Voorbeelden zijn een server van Healthconnect, de Pyxicloud, …

	Authenticatie	data@move	Transportkanaal	Data@rest
Localhost[1]	Geen identificatie vereist	Geen dataencryptie vereist	Geen geëncrypteerd transport (via loopback interface)	Volgens classificatie
Gemeenschappelijk veiligheidsbeleid	Gebruikersnaam en wachtwoord*	Geen dataencryptie vereist tenzij data ingegeven is door arts	Encryptie van het transportkanaal over TLS	Volgens classificatie
Verschillend veiligheidsbeleid	Via eHealth certificaat of PKI****	Data is geëncrypteerd	Transportkanaal is geëncrypteerd	Volgens classificatie, met aandacht voor: Dataminimalisatie** Dataretentie***
Via Ehealth	Via eHealth certificaat	Data is geëncrypteerd	Transportkanaal is geëncrypteerd	Nvt.

* Bij voorkeur een systeem zoals Kerberos. Gebruikersnaam en wachtwoord zijn verschillend per woonzorgcentrum die onderdeel uitmaken van het veiligheidsbeleid. Wanneer een interactief toestel, zoals een desktop of een tablet worden gebruikt, dan gebeurt de identificatie met volgende variabelen: woonzorgcentrum, gebruikersnaam en wachtwoord op individueel gebruikersniveau
** Dataminimalisatie: Bij data duplicatie dient te worden aangetoont dat iedere gevevensset strikt tot het minimum wordt herleid. De proportionaliteit van de gegevensset dient met andere woorden te worden aangetoond.
*** Dataretentie: Gegevens mogen sin secundaire orde niet langer te worden bewaard dan de originele gegevensset[2], tenzij de nood kan worden aangetoond.

[1] Hiermee wordt bedoeld: uitwisseling tussen software op eenzelfde server

**** Indien een eigen PKI wordt gebruikt, dan dient deze te worden opgezet volgens de principes zoals bepaald in de CSA-CMM norm en meer in het bijzonder Control ID's EKM-01 – EKM-04[3].

[2] Art.8 §1 BVR van 24 juli 2009 – bewaren van persoonsgegevens http://www.juriwel.be/ws/Export/1018609.html
De voorziening of de vereniging bewaart de persoonsgegevens betreffende een gebruiker minimaal twee jaar na het beëindigen van de hulp- en dienstverlening aan de betrokken gebruiker. Ze mag die gegevens tot maximaal vijf jaar na het beëindigen van die hulp- en dienstverlening bewaren.

[3] https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

Bijlage 3: De behandeling van het e-Health certificaat.

1 De leverancier neemt de nodige veiligheidsmaatregelen in acht bij het beheer van en de toegang tot het eHealth certificaat van een woonzorgcentrum.

Maatregel 1.1 Het certificaat wordt bewaard in een veilige container, met strikte toegangsprocedures die beperkt zijn voor de gemachtigde beheerders. De leverancier houdt de lijst van gemachtigden bij en communiceert deze aan het woonzorgcentrum.

Maatregel 1.2 De toegang tot de opslagplaats van het certificaat wordt gelogd.

Maatregel 1.3 Het certificaat wordt enkel op een beveiligde wijze getransporteerd bij een overdracht van klant naar leverancier (vb via een door encryptie beveiligde zip bestand).

Maatregel 1.4 Het corresponderende wachtwoord voor de keystore wordt via een ander kanaal gecommunicaard tussen klant en leverancier (vb SMS).

Maatregel 1.5 Het corresponderende wachtwoord voor de keystore wordt op een veilige manier opgeslagen in de software: het wachtwoord is niet leesbaar.

Maatregel 1.6 Wanneer het vermoeden bestaat dat het certificaat in het bezit is van een onbevoegde of het corresponderende wachtwoord gekend is door derden, dan wordt onmiddellijk de klant verwittigd.

Maatregel 1.7 Oude certificaten worden enkel door de klant bewaard, tenzij toestemming bestaat om het bij de leverancier te archiveren.

Maatregel 1.8 Het eHealth certificaat wordt nooit zonder toestemming van de klant gedupliceerd.

Maatregel 1.9 Indien encryptie van de backup van een systeem met het eHealth certificaat wordt voorzien, wordt de encryptiesleutel op een veilige plaats bewaard en bestaat er een herstelprocedure.

2 Het eHealth certificaat wordt enkel geïnstalleerd op een systeem dat voorzien is van de nodige veiligheidsmaatregelen.

Maatregel 2.1 Volgende maatregelen zijn van kracht:

- De server met het certificaat wordt niet voor eindgebruikers doeleinden gebruikt (bijvoorbeeld het gebruik van e-mail en internet is niet toegestaan via dit systeem)
- Het aantal gemachtigde gebruikers die toegang hebben tot deze server is beperkt tot het strikte minimum.
- De server is voorzien van een sterk wachtwoordmechanisme
- De server is voorzien van schermbeveiliging
- De netwerklocatie met het eHealth certificaat is niet gedeeld via het netwerk
- Het systeem is gestript en gehardened (vb Plug & play functionaliteiten zijn uitgeschakeld)
- Een interne firewall is actief op het systeem
- Anti malware software is geïnstalleerd, actief en bijgewerkt tot de laatste versie. DeIPS functie van deze software is geactiveerd.
- De installatie van vreemde software is verboden
- De bestandslokatie van het certificaat is voorzien van logging
- Het besturingssysteem wordt bijgewerkt
- De toegang tot het systeem is persoonlijk
- Toegangslogging tot het systeem is voorzien

Maatregel 2.2 Wanneer certificaten worden bewaard in een multi tenant omgeving, dan dient dit te worden bewaard in een key vault infrastructuur.

Maatregel 2.3 Op vraag van de klant zijn de veiligheidsinstellingen van de server waarop het eHealth certificaat wordt bewaard, onderwerp van een audit.