COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

College bescherming persoonsgegevens

Onderzoek naar de beveiliging van het netwerk van het Groene Hart Ziekenhuis

z2012-00717

Rapport herziene definitieve bevindingen
Openbare versie

Oktober 2014

DATUM 6 oktober 2014

Inhoud

1 INLEIDING

Aanleiding onderzoek

Op 7 oktober 2012 verscheen het bericht[1] in de media dat tientallen medische dossiers en de gegevens van honderdduizenden patiënten van het Groene Hart Ziekenhuis (GHZ) via internet toegankelijk zijn geweest. Naar aanleiding van deze berichten heeft het College bescherming persoonsgegevens (CBP) bij brieven van 9 oktober 2012 en 23 oktober 2012 en telefonisch op 14 december 2012 informatie opgevraagd over dit beveiligingslek. Bij brieven van 18 oktober 2012, 1 november 2012 en e-mail van 14 december 2012 heeft het GHZ de gevraagde informatie aan het CBP doen toekomen.

Uit de verkregen informatie blijkt dat het GHZ na het beveiligingslek een onderzoek door [Bedrijfsnaam] heeft laten doen. [Bedrijfsnaam] constateerde dat de beveiliging van het GHZ gebreken vertoonde. Een deel van deze gebreken was al geconstateerd in een eerder onderzoek van [Bedrijfsnaam] (2010).

Het CBP heeft het GHZ bij brief van 17 januari 2013 verzocht middels bewijstukken aan te tonen dat de gebreken, zoals geconstateerd door [Bedrijfsnaam] in de onderzoeken van 2010 en 2012 zodanig zijn opgelost of geadresseerd, dat de beveiliging van patiëntgegevens door het GHZ in overeenstemming is gebracht met artikel 13 van de Wet bescherming persoonsgegevens (Wbp).

Bij brief van 14 maart 2013 heeft het GHZ het CBP daartoe een rapport van [Bedrijfsnaam] toegestuurd.[2] Uit dit rapport blijkt dat het GHZ een aantal verbetermaatregelen heeft getroffen. Uit het rapport blijkt echter tevens dat het GHZ diverse medische systemen op het netwerk heeft aangesloten, waarop *end of life* besturingssoftware draait.[3] De systemen hebben via het netwerk toegang tot het internet. *End of life* (besturings)software op systemen die op het netwerk zijn aangesloten, vormt een risico voor de beveiliging van persoonsgegevens doordat deze niet langer door de softwareleverancier bijgewerkt wordt op beveiligingstekortkomingen.[4]

Dit risico wordt groter doordat het netwerk, waarop het GHZ deze medische systemen met *end of life* software heeft aangesloten, niet gesegmenteerd is, zoals blijkt uit het [Bedrijfsnaam]rapport.[5] Een eenmaal geïnfecteerd systeem vormt daardoor een bedreiging voor de beveiliging van andere aan het netwerk gekoppelde systemen waaronder systemen waarin medische persoonsgegevens worden verwerkt.

Omdat het gebruik van medische systemen die draaien op *end of life* (besturings)software ernstige beveiligingsrisico's met zich mee brengt voor de

---

[1] Http://www.nu.nl/binnenland/2927832/groene-hart-ziekenhuis-lekt-medische-dossiers.html.
[2] [Bedrijfsnaam] [Titel rapport].
[3] [Bedrijfsnaam] [Titel rapport].
[4] Microsoft informeert zijn klanten hierover: "*Wanneer een versie van Windows niet wordt ondersteund, heeft dat tot gevolg dat er geen software-updates meer beschikbaar zijn via Windows Update. Deze updates omvatten beveiligingsupdates die uw pc helpen beveiligen tegen virussen en andere schadelijke software waarmee uw persoonlijke informatie kan worden gestolen. Windows Update installeert daarnaast de meeste recente software-updates om de betrouwbaarheid van Windows te verbeteren, waaronder nieuwe stuurprogramma's voor uw hardware.* http://windows.microsoft.com/nl-nl/windows/help/what-does-end-of-support-mean.
[5] [Bedrijfsnaam] [Titel rapport].

bescherming van de medische (persoons)gegevens van patiënten van het GHZ en deze systemen daarnaast zijn aangesloten op een niet gesegmenteerd netwerk, heeft het CBP op grond van deze informatie besloten een ambtshalve onderzoek in te stellen naar de beveiliging van het netwerk van het GHZ. Dit heeft het CBP bij brief van 19 april 2013 aan het GHZ medegedeeld.

Doel van het onderzoek

Het doel van het onderzoek is te onderzoeken of het GHZ voldoende passende technische en organisatorische maatregelen ten uitvoer brengt om de (medische) persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.
Het onderzoek richt zich hierbij met name op het gebruik medische systemen die draaien op *end of life* (besturings)software en die zijn aangesloten op het netwerk van het GHZ.

Het onderzoek richt zicht hierbij specifiek op de volgende vragen:

- Worden de beveiligingsrisico's (doorlopend) in kaart gebracht?
- Worden (doorlopend) organisatorische en/of technische maatregelen getroffen om de geconstateerde risico's zoveel mogelijk te beperken?
- Is het netwerk beveiligd door (technische) scheiding, bijvoorbeeld door segmentering van de diverse domeinen?

Verloop onderzoek

In dit kader heeft het CBP bij brieven van 19 april 2013 en 3 mei 2013, tijdens een overleg op 14 juni 2013, bij e-mail van 9 juli 2013, 15 november 2013, 23 januari 2014 en telefonisch op 9 juli 2013, 16 juli 2013, 19 juli 2013 en 12 december 2013 nadere vragen gesteld aan het GHZ.
Het GHZ heeft deze vragen bij brieven van 3 mei 2013, 26 juni 2013, 17 oktober 2013, 21 november 2013, 18 december 2013 en 30 januari 2013, tijdens het overleg op 14 juni 2013, bij e-mail van 20 juni 2013, 12 juli 2013 en 16 juli 2013 en telefonisch op 16 en 19 juli 2013 beantwoord.

Bij brief van 13 maart 2014 heeft het CBP de voorlopige bevindingen aan het GHZ doen toekomen. Bij brief van 26 maart 2014 heeft het GHZ uitstel gevraagd voor de schriftelijke zienswijze. Telefonisch en bij brief van 1 april 2014 heeft het CBP twee weken uitstel verleend. Bij brief van 16 april 2014 heeft het GHZ haar zienswijze gegevens op de voorlopige bevindingen.

Bij brief van 15 mei 2014 heeft het CBP nadere vragen gesteld over de inhoud van de zienswijze van het GHZ. Bij brief van 22 mei 2014 heeft het GHZ uitstel gevraagd voor de beantwoording van de vragen. Het CBP heeft bij e-mail van 26 mei 2014 uitstel verleend tot 13 juni 2014. Bij brief van 12 juni 2014 heeft het GHZ de vragen beantwoord.

Bij brief van 4 september 2014 heeft het CBP de definitieve bevindingen doen toekomen aan het GHZ.

Bij brief van 15 september 2014 heeft het GHZ aangegeven welke informatie zij beschouwt als (bedrijfs)vertrouwelijk zoals bedoeld in artikel 10, eerste lid, aanhef en onder c van de Wob.
Omdat in deze brief nieuwe informatie is opgenomen over de voorgenomen werkwijze, heeft het CBP hierover telefonisch op 22 september nadere vragen gesteld aan het GHZ. Het GHZ heeft de vragen tijdens dit gesprek beantwoord en heeft tevens verslag gedaan van het telefoongesprek bij e-mail van 22 september 2014.

Het CBP heeft de nieuwe informatie in het onderliggende rapport herziene definitieve bevindingen verwerkt.

2 JURIDISCH KADER

Ingevolge artikel 13 van de Wbp dient een verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer te brengen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van de te bescherming gegevens met zich meebrengen.

In het begrip "passende" ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Daarnaast duidt het begrip "passende" op een proportionaliteit tussen beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van deze gegevens. In het netwerk van het GHZ worden de medische gegevens van (voormalige) patiënten verwerkt. Medische gegevens behoren tot de categorie bijzondere gegevens als bedoeld in artikel 16 Wbp. Dit betekent dat hoge eisen gesteld worden aan de technische en organisatorische maatregelen ter bescherming van deze gegevens.

Zoals aangegeven in de CBP richtsnoeren 'beveiliging van persoonsgegevens' dient software up-to-date te worden gehouden.[6] Dit is een belangrijke maatregel. In de NEN-ISO/IEC 27002 staat hierover: "*Er behoren passende en tijdige handelingen te worden genomen als reactie op identificatie van mogelijke technische kwetsbaarheden.*"[7]
De norm NEN-7510 die aanwijzingen geeft voor het toepassen van de Code voor informatiebeveiliging NEN-ISO/IEC 27002 in de gezondheidszorg stelt: "*Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.*"[8]

Indien het beheer van een systeem niet in handen is van een verantwoordelijke maar door een bewerker wordt uitgevoerd dient de verantwoordelijke afspraken te maken met de bewerker over de beveiliging. In de CBP richtsnoeren 'beveiliging van persoonsgegevens' staat hierover: "*Indien de verantwoordelijke persoonsgegevens te zijner behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen.*"[9]

In NEN-7510[10] staat "*Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.* […] *Een methode voor het beveiligen van grote netwerken is het opsplitsen van de netwerken in afzonderlijke logische domeinen, bijvoorbeeld het interne*

[6] CBP Richtsnoeren beveiliging van persoonsgegevens, pag. 23.
[7] NEN-ISO/IEC 27002:2007 nl, paragraaf 12.6.
[8] NEN-2710:2011nl, paragraaf 12.6.1.
[9] CBP Richtsnoeren beveiliging van persoonsgegevens, pag. 11.
[10] NEN-2710:2011nl, paragraaf 11.4.5.

netwerkdomeinen van een organisatie en externe netwerkdomeinen, die elk wordt beschermd door een afgegrensd beveiligd gebied. Er kan een getrapte verzameling beheersmaatregelen worden toegepast in verschillende logische netwerkdomeinen om de beveiligingsomgevingen van het netwerk verder te scheiden, bijvoorbeeld openbaar toegankelijke systemen, interne netwerken en kritische bedrijfsmiddelen. Definieer de domeinen aan de hand van een risicobeoordeling en de verschillende beveiligingseisen binnen elk van de domeinen."

Samengevat weergegeven worden aan het GHZ in ieder geval de volgende eisen gesteld om aan artikel 13 Wbp te kunnen voldoen:

- beveiligingsrisico's dienen (doorlopend) in kaart te worden gebracht;
- er moeten (doorlopend) organisatorische en/of technische maatregelen worden getroffen om de geconstateerde risico's zoveel mogelijk te beperken, bijvoorbeeld door updates uit te voeren of andere maatregelen te treffen indien het niet mogelijk is om bepaalde (besturings)software te updaten;
- grote netwerken dienen beveiligd te worden door (technische) scheiding, bijvoorbeeld door segmentering van de diverse domeinen.

3 VOORLOPIGE BEVINDINGEN

Het CBP heeft een rapport voorlopige bevindingen van het onderzoek bij brief van 13 maart 2014 aan het GHZ doen toekomen. Onderstaand volgt de integrale tekst zoals deze is opgenomen in het rapport voorlopige bevindingen.

Feiten *end of life* (besturings)software en segmentatie netwerk

Uit het rapport van [Bedrijfsnaam], de ontvangen stukken van het GHZ (brieven van 3 mei 2013 en 26 juni 2013, e-mails van 20 juni 2013, 12 juli 2013 en 16 juli 2013) en de gesprekken die zijn gevoerd met het GHZ (telefoongesprekken van 26 maart 2013, 16 juli 2013, 19 juli 2013 en het gesprek met GHZ op 14 juni 2013) blijkt dat er, zoals in 2012 ook is vastgesteld door [Bedrijfsnaam],[11] medische systemen, die met het netwerk verbonden zijn, draaien op *end of life* software, zoals Windows 2000 en Windows XP.[12] In het gesprek op 14 juni 2013 is door het GHZ aangegeven dat er veel medische apparaten op het netwerk zijn aangesloten waarvan het GHZ niet zelf het beheer doet / kan doen en waarvan het GHZ niet weet op welke besturingssoftware deze apparaten draaien. Er kunnen op deze systemen geen beveiligingsupdates worden uitgevoerd door het GHZ zelf.

Windows 2000 is sinds 20 juni 2005 *end of life* en de uitgebreide ondersteuning is beëindigd op 13 juli 2010.[13] Dit wil zeggen dat voor Windows 2000 vanaf juli 2010 geen beveiligingsupdates meer beschikbaar zijn. In het rapport van [Bedrijfsnaam] is aangegeven dat er voor deze systemen een uitfaseringsplan is opgesteld maar dat uitfasering niet op korte termijn kan plaatsvinden zonder de continuïteit van de bedrijfsvoering in gevaar te brengen. Voor Windows XP geldt dat deze nog tot 8 april 2014 door Microsoft wordt ondersteund. Dit betekent dat ook voor dit systeem vanaf dat moment geen reguliere beveiligingsupdates meer beschikbaar zijn en derhalve uitfasering noodzakelijk is.

Naast de *end of life* software op de medische systemen zijn er ook diverse *end of life* gebruikersapplicaties aangetroffen bij de [Bedrijfsnaam]-scan van februari 2013.[14] De [Bedrijfsnaam]-scan geeft daarbij een beperkt beeld van de stand van zaken van updates, omdat met deze tool alleen op Windows computers draaiende software bevraagd wordt. Software op medische systemen die niet op Windows draait, of systemen waarop het niet mogelijk is om de [Bedrijfsnaam]-tool te installeren zijn niet mee gescand. Het GHZ geeft in het gesprek van 14 juni 2013 aan dat ook bepaalde systemen niet kunnen worden gescand met een (virus)scanner omdat het risico bestaat dat een systeem uitvalt door de scan, wat in ieder geval geldt voor de [VERWIJDERD] systemen die ook op het netwerk van het GHZ zijn aangesloten.[15]

[11] [Bedrijfsnaam][Titel rapport].
[12] Windows XP wordt door Microsoft tot 8 april 2014 ondersteund. URL: http://windows.microsoft.com/nl-nl/windows/products/lifecycle.
[13] URL: http://support.microsoft.com/gp/lifean36.
[14] Brief van het GHZ aan het CBP van 26 juni 2013, bijlage 4.
[15] [VERWIJDERD].

De apparatuur met *end of life* (besturings)software is aangesloten op het netwerk van het GHZ dat niet gesegmenteerd is. Alle apparatuur, systemen, pc's zijn met hetzelfde netwerk verbonden zonder dat hierin een scheiding is aangebracht. In de praktijk betekent dit dat alle apparaten 'elkaar kunnen zien'.
Dit blijkt onder andere uit het rapport van [Bedrijfsnaam][16] uit 2012, waarin tevens wordt verwezen naar een bevinding van [Bedrijfsnaam] in 2010[17] waarin dit ook is geconstateerd.
Uit de brief van GHZ van 11 oktober 2013, 21 november 2013, 18 december 2013 en 30 januari 2014 blijkt dat GHZ een gesegmenteerd netwerk heeft opgebouwd [VERWIJDERD].[18] In de brief van 21 november 2013 stelt GHZ: "*Bij de migratie naar het nieuwe netwerk is het oude netwerk gekopieerd in één VRF segment daarbij gebruikmakend van de oude IP-nummering. […] De start van het project* [Projectnaam] *is gepland voor januari 2014*." In de brief van 20 januari 2014 stelt GHZ over dit project: "*De geplande startdatum van dit project was initieel januari 2014 maar is nu, door uitloop van het initiële netwerkproject, enigszins vertraagd. De verwachte startdatum is nu februari 2014*." Het oude netwerk is geplaatst in een segment van het nieuwe netwerk dat GHZ het legacy segment noemt. De migratie van de apparatuur in het legacy segment naar het gesegmenteerde netwerk zal vanaf 1 oktober 2013 nog 2,5 jaar in beslag zal nemen.[19]

Beoordeling *end of life* (besturings)software en segmentatie netwerk

End of life (besturings)software
Het feit dat bij het GHZ op dit moment medische systemen, die met het netwerk verbonden zijn, draaien op besturingssystemen met *end of life* (besturings)software, zoals Windows 2000 en Windows XP[20], maakt het netwerk zeer kwetsbaar voor inbreuken. De software wordt niet up-to-date gehouden, zoals is voorgeschreven in de richtsnoeren beveiliging van het CBP. Hierdoor worden bekende beveiligingsrisico's niet meer hersteld. Ook kunnen er in de *end of life* (besturings)software onbekende beveiligingsrisico's aanwezig zijn omdat deze software niet meer wordt gecontroleerd. Hieruit vloeit voort dat er geen passende en tijdige handelingen kunnen worden genomen als reactie op identificatie van mogelijke technische kwetsbaarheden zoals is voorgeschreven in de NEN-ISO/IEC 27002.
Het risico dat de medische persoonsgegevens binnen het netwerk van het GHZ worden benaderd door onbevoegden en vervolgens worden gestolen, vernietigd of gewijzigd neemt hierdoor toe.

Het GHZ heeft aangegeven dat uitfasering van deze systemen niet op korte termijn kan plaatsvinden. Het gebruik van *end of life* (besturings)software vormt een ernstig beveiligingsrisico. Indien geen aanvullende maatregelen worden getroffen waardoor dit risico wordt beperkt of weggenomen, is het gebruik van *end of life* (besturings)software in strijd met artikel 13 Wpb.

[16] [Titel rapport], [Bedrijfsnaam].
[17] [Titel rapport].
[18] [VERWIJDERD].
[19] Dit is door het GHZ gezegd in het gesprek dat het CBP met het GHZ heeft gevoerd op 14 juni 2013 en staat in paragraaf 6 van de brief van het GHZ aan het CBP van 26 juni 2013.
[20] Windows XP wordt tot 8 april 2014 ondersteund.

Niet gesegmenteerd netwerk
Uit het onderzoek blijkt tevens dat de apparaten/systemen met deze *end of life* (besturings)software zijn verbonden met het niet gesegmenteerde netwerk van GHZ.[21] Qua opzet vormt een niet gesegmenteerd netwerk een risico voor de informatiebeveiliging, zowel in kans als in impact.
In het huidige netwerk staan apparaten en systemen met elkaar in (directe) verbinding in het legacy segment.[22] Daarbij is het merendeel van de apparaten en systemen niet alleen aan het netwerk gekoppeld maar tevens met het internet verbonden. Naast de medische apparatuur zijn er ook diverse [VERWIJDERD] aan het netwerk gekoppeld[23] en wordt ook op de aangesloten pc's gebruik gemaakt van *end of life* software. Als er kwetsbaarheden/tekortkomingen (vulnerabilities) zijn in één van de aangesloten systemen waardoor een hacker het netwerk binnendringt, bijvoorbeeld zoals bij de hack die plaatsvond op 7 oktober 2012, is het gehele netwerk bereikbaar voor verdere inbreuken.[24]
Dit probleem kan tevens ontstaan als een gebruiker binnen het GHZ op internet gaat en daardoor kwaadaardige software zoals virussen, malware en/of botnets binnenhaalt die misbruik maken van oude versies van de gebruikte applicaties.

Het feit dat het GHZ gebruik maakt van een niet gesegmenteerd netwerk brengt ernstige beveiligingsrisico's met zich mee, zeker in combinatie met de aanwezigheid van apparatuur met *end of life* (besturings)software. Indien geen aanvullende maatregelen worden getroffen waardoor de risico's wordt beperkt of weggenomen, is het verwerken van (bijzondere) persoonsgegeven in een groot niet gesegmenteerd netwerk in strijd met artikel 13 Wbp.

Door GHZ voorgenomen maatregelen

Het GHZ heeft in het gesprek van 14 juni 2013 en bij brieven van 26 juni 2013, 17 oktober 2013, 21 november 2013, 18 december 2013 en 30 januari 2014 aangegeven maatregelen te treffen.

Uit het onderzoek blijkt dat het GHZ het netwerk gaat segmenteren.[25] Het GHZ verklaart[26]:
"*Het netwerk voorziet in segmentatie door middel van:*

- *VRF securitydomeinen* [VERWIJDERD].
- *Scheiding door VLAN's* [VERWIJDERD].
- *Het plaatsen van interne firewalls* [VERWIJDERD].

[21] Het feit dat er [VERWIJDERD] een gesegmenteerd netwerk aanwezig is betekent niet dat het nieuwe netwerk al is gesegmenteerd omdat het oude netwerk in één segment van het nieuwe netwerk is gekopieerd en derhalve functioneert als een niet gesegmenteerd (deel)netwerk.
[22] Aangezien dit een kopie is van het niet gesegmenteerde netwerk [VERWIJDERD].
[23] [VERWIJDERD].
[24] Hierbij moet gedacht worden aan het verspreiden van virussen, het wijzigen dan wel verwijderen van gegevens, het stelen van gegevens, het platleggen van systemen/apparatuur en overige manipulaties van het systeem.
[25] [Titel rapport], [Bedrijfsnaam].
[26] Brief van het GHZ aan het CBP van 17 oktober 2013.

- *Indien een specifieke situatie dit vereist kunnen wij additionele maatregelen implementeren zoals network based IPS*."

In de brief van 17 oktober 2013 geeft het GHZ aan dat het gesegmenteerde netwerk per december 2013 klaar is (formele afronding project [Projectnaam])[27]. De diverse apparaten en medische systemen zijn hier echter nog niet op aangesloten. Het migreren van de verschillende medische systemen naar het gesegmenteerde netwerk, dat zal beginnen in februari 2014[28] zal vanaf oktober 2013 nog 2,5 jaar in beslag nemen, zo heeft het GHZ aangegeven in het gesprek met het CBP van 14 juni 2013.
Op dit moment is er een kopie van het netwerk [VERWIJDERD] geplaatst in één segment van het netwerk [VERWIJDERD]. Er is derhalve op dit moment nog sprake van verwerking van medische persoonsgegevens in een niet gesegmenteerd (deel)netwerk.

Van de medische apparatuur die op het netwerk is aangesloten is van een groot deel niet bekend welke (besturings)software gebruikt wordt.[29] Het GHZ gaat de komende jaren alle medische systemen in kaart brengen (identificeren van de systemen en bepalen van de eigenaren) en, indien mogelijk, migreren naar het gesegmenteerde netwerk.[30] Uiteindelijk zullen alle aangesloten systemen in het ziekenhuis worden ondergebracht in de segmenten: '[VERWIJDERD]', '[VERWIJDERD]', '[VERWIJDERD]'. In het segment [VERWIJDERD] komen de systemen waarvan het GHZ geen inzicht heeft in en controle heeft op de beveiliging.[31]

Het GHZ heeft in het gesprek van 14 juni 2013 aangegeven dat men in overleg gaat met de leveranciers van de medische apparatuur, maar dat het lastig is om deze aan te spreken over medische apparatuur die het GHZ in het verleden heeft gekocht. Het CBP heeft naar aanleiding daarvan met NVZ gesproken over het gebruik van apparatuur die draait op *end of life* (besturings)software door ziekenhuizen. Uit dat gesprek blijkt dat het vaker voorkomt dat de leveranciers van deze apparatuur om uiteenlopende reden niet bereid zijn om (de beveiliging van) besturingssoftware van de door hun geleverde apparatuur up to date te houden. Het GHZ stelt dat zij bij de inkooptrajecten van nieuwe apparatuur wel de nadruk legt op de verplichting van leveranciers om te voldoen aan criteria die het ziekenhuis noodzakelijk acht voor een optimaal beveiligde omgeving, rekening houdend met het ontwerp van het netwerk. In de brief van 26 juni 2013 stelt het GHZ dat er ook [VERWIJDERD] ingezet wordt om de leveranciers te bewegen tot medewerking en dat er door het GHZ zelf wordt gecommuniceerd met de leveranciers.[32]

Het GHZ geeft aan dat zij voor de huidige situatie maatregelen heeft getroffen door het netwerk te monitoren. Er zijn twee dienstverleners voor het GHZ actief die zich hiermee bezighouden.[33] Een van de dienstverleners is de beheerder van de firewall,

[27] Brief van GHZ aan het CBP 17 oktober 2013.
[28] Brief van het GHZ aan het CBP van 30 januari 2014.
[29] Brief van 26 juni 2013 van het GHZ aan het CBP, paragraaf 1, pagina 3.
[30] Brief van het GHZ aan het CBP van 17 oktober 2013.
[31] Brief van 26 juni 2013 van het GHZ aan het CBP, paragraaf 1, pagina 2.
[32] Brief van het GHZ aan het CBP van 26 juni 2013, paragraaf 6.
[33] Brief van het GHZ aan het CBP van 18 december 2013.

met onder andere een IPS module, tussen het netwerk van het GHZ en het internet.[34] Het bedrijf doet melding als er sprake is van verdachte verkeersstromen tussen het netwerk van GHZ en het internet. De andere dienstverlener is een IT beveiligingsbedrijf dat zich voor het GHZ bezighoudt met het monitoren van het interne GHZ netwerk.[35] Hiermee kunnen verdachte wijzigingen in het netwerkverkeer (bijvoorbeeld door malware attacks) worden gedetecteerd. Dit bedrijf levert standaard een maandrapportage aan en in het geval van incidenten wordt ook hier een rapportage van aangeleverd.

Ten aanzien van het identificeren van de risico's die bestaan doordat er *end of life* apparatuur op het netwerk is aangesloten, stelt het GHZ onder andere[36]:
"*In deze fase heeft het GHZ er niet voor gekozen om penetratiestesten uit te voeren op apparatuur die met end-of -life software draait. Dit is gedaan om de volgende redenen:*

- *Het vermoeden bestaat nu al dat een deel van de apparatuur kwetsbaarheden zal vertonen. Opnieuw deze kwetsbaarheden in kaart brengen door middel van een penetratietest brengt risico's met zich mee en vergt tijd. Deze tijd kan beter worden besteed aan het stuk voor stuk inventariseren van de apparatuur en het creëren van een risicoprofiel. Deze activiteit is onderdeel van het project segmentering en IP-omnummering. Wellicht is dit risicoprofiel grover, maar de beschikbare informatie hieruit is kwalitatief meer dan voldoende om daarmee de apparatuur in het juiste netwerksegment te kunnen plaatsen.*
- *Inventarisatie van kwetsbaarheden vindt op dit moment al deels plaats door de inzet van* [Bedrijfsnaam]. *Hiermee wordt in feite al een groot deel van de kwetsbaarheden gevonden die ook met een penetratietest aan het licht zouden komen.*[37]
- *Bij het uitvoeren van penetratietesten wordt potentieel een risico gecreëerd in de bedrijfsvoering. Met name wanneer daar oudere apparatuur bij is betrokken. Zo zijn er voorbeelden bekend van gebouwbeheersingssystemen die niet meer werkten na het uitvoeren van* [VERWIJDERD] *scans die doorgaans worden gezien als niet indringend (unobtrusive).*"

Beoordeling voorgenomen maatregelen GHZ

Zoals in het juridisch kader is aangegeven worden aan het GHZ tenminste de volgende eisen gesteld om te kunnen voldoen aan artikel 13 Wbp:

- beveiligingsrisico's dienen (doorlopend) in kaart te worden gebracht;
- er moeten (doorlopend) organisatorische en/of technische maatregelen worden getroffen om de geconstateerde risico's zoveel mogelijk te beperken, bijvoorbeeld door updates uit te voeren of andere maatregelen te treffen indien het niet mogelijk is om bepaalde (besturings)software te updaten; en
- grote netwerken dienen beveiligd te worden door (technische) scheiding, bijvoorbeeld door segmentering van de diverse domeinen.

[34] Brief van het GHZ aan het CBP van 18 december 2013, pagina 1.
[35] Brief van het GHZ aan het CBP van 18 december 2013, pagina 1-2.
[36] Brief van het GHZ aan het CBP van 30 januari 2014.
[37] Opmerking CBP: De [Bedrijfsnaam]-scan geeft daarbij een beperkt beeld van de stand van zaken van updates, omdat met deze tool alleen op Windows computers draaiende software bevraagd wordt. Software op medische systemen die niet op Windows draait, of systemen waarop het niet mogelijk is om de [Bedrijfsnaam]-tool te installeren zijn niet mee gescand. Ook kunnen bepaalde systemen niet worden gescand met een virusscanner omdat het risico bestaat dat een systeem uitvalt door de scan, aldus het GHZ in het gesprek van juni 2013.

Beveiliging van het netwerk van het GHZ tot maart 2016
Het netwerk van het GHZ is een groot netwerk dat beveiligd dient te zijn door (technische) scheiding. Het GHZ is inmiddels gestart met segmentering van het netwerk. Het GHZ heeft aangegeven dat het traject om te komen tot segmentatie van het gehele netwerk vanaf 1 oktober 2013 nog 2,5 jaar in beslag neemt. De segmentering van het netwerk zal naar verwachting dus in april 2016 gerealiseerd zijn.

Op het netwerk is apparatuur met *end of life* (besturings)software aangesloten . Het GHZ geeft aan dat zij de komende jaren alle medische systemen in kaart gaat brengen (identificeren van de systemen en bepalen van de eigenaren) en, indien mogelijk, migreren naar het gesegmenteerde netwerk.[38] Dit project zal naar verwachting in april 2016 gereed zijn.
Tot 2016 zullen er systemen met *end of life* (besturings)software op het niet (volledig) gesegmenteerde netwerk van het GHZ zijn aangesloten.

Het GHZ heeft aangegeven dat zij maatregelen treft om ervoor te zorgen dat het netwerk gedurende die periode toch beveiligd is. Het verkeer tussen de binnenkant van het netwerk en de buitenkant (internet) wordt gemonitord met een firewall met onder andere een IPS module. Ook de binnenkant van het netwerk wordt, door een externe partij, gemonitord op verdachte verkeersstromen.

De monitoring middels de firewall is echter beperkt. De beheerder van de firewall levert niet structureel rapportages op over de beveiliging en maakt uitsluitend melding van verdachte verkeersstromen naar servers of (IP)-adressen waarvan bekend is dat zij malware verspreiden of deel uitmaken van een botnet.[39]
De externe partij die het interne netwerk monitort levert een standaard maandrapportage op aangevuld met in voorkomend geval een incidentenrapportage van verdachte verkeersstromen binnen het netwerk van GHZ.[40] Ook deze partij monitort alleen op basis van bekende verdachte verkeersstromen.[41]
Juist in systemen met *end of life* (besturings)software kunnen onbekende kwetsbaarheden aanwezig zijn. Onbekende kwetsbaarheden worden op bovenstaande manier niet, dan wel pas achteraf gedetecteerd.
Kwetsbaarheden die wel bekend zijn, worden door het GHZ pas opgemerkt als er al een beveiligingsincident heeft plaatsgevonden.

Uit bovenstaande blijkt dat het GHZ het netwerk op reactieve wijze monitort en hiermee onvoldoende passende technische en organisatorische maatregelen treft om de persoonsgegevens te beveiligen. Het GHZ zou het netwerk proactief moeten monitoren, bijvoorbeeld door de logbestanden dagelijks te controleren en te bepalen of er sprake is van (al dan niet bekende) technische kwetsbaarheden, en hier vervolgens opvolging aan geven.

[38] Brief van het GHZ aan het CBP van 17 oktober 2013.
[39] Zie brief van het GHZ aan het CBP van 18 december 2013, pagina 1.
[40] Zie brief van het GHZ aan het CBP van 18 december 2013, pagina 1.
[41] Zie brief van het GHZ aan het CBP van 18 december 2013, pagina 1-2.

Met de door het GHZ genoemde maatregelen worden derhalve de risico's van de *end of life* (besturings)software niet voldoende en tijdig geïdentificeerd en onder controle gebracht.

Het CBP heeft het GHZ derhalve gevraagd of zij naast het monitoren van het netwerk nog andere maatregelen treft, zoals bijvoorbeeld het uitvoeren van penetratietesten op de apparatuur met *end of life* (besturings)software.

Het GHZ stelt in de brief van 13 januari 2013 dat er geen penetratietesten zullen plaatsvinden op de medische apparatuur die met *end of life* software draait. Het GHZ stelt: "*Het vermoeden bestaat nu al dat een deel van de apparatuur kwetsbaarheden zal vertonen. Opnieuw deze kwetsbaarheden in kaart brengen door middel van een penetratietest brengt risico's met zich mee en vergt tijd. Deze tijd kan beter worden besteed aan het stuk voor stuk inventariseren van de apparatuur en het creëren van een risicoprofiel. Deze activiteit is onderdeel van het project* [Projectnaam]"

De stelling van het GHZ dat het in kaart brengen van kwetsbaarheden risico's met zich mee brengt en tijd kost geeft onvoldoende reden om van inventarisatie van kwetsbaarheden af te zien. Daartoe is tevens van belang dat deze stelling door het GHZ onvoldoende is gemotiveerd. Zo heeft het GHZ niet aangegeven of dit ook het geval is voor de apparatuur die aan het netwerk van het GHZ is aangesloten, en zo ja, welke apparatuur dit betreft.
Het feit dat het GHZ aangeeft dat het vermoeden bestaat dat een deel van de apparatuur kwetsbaarheden vertoont, en hierop door het GHZ niet direct actie wordt ondernomen om deze vermoedelijke kwetsbaarheden weg te nemen, betekent dat het GHZ geen opvolging geeft aan geconstateerde beveiligingsrisico's.

Uit bovenstaande blijkt dat het GHZ in ieder geval tot april 2016 in strijd handelt met artikel 13 Wbp door gebruik te maken van een niet gesegmenteerd netwerk waarop apparatuur met *end of life* (besturings)software is aangesloten. Het GHZ heeft onvoldoende aanvullende maatregelen getroffen om de risico's te beperken of weg te nemen.

Beveiliging van het netwerk van het GHZ vanaf april 2016
Het GHZ heeft in de fase voorafgaand aan de voorlopige bevindingen aangegeven dat de segmentering van het netwerk naar verwachting in april 2016 gerealiseerd is.
Uit het onderzoek van het CBP blijkt dat ook na voltooiing van het gesegmenteerde netwerk (mogelijk) sprake zal zijn van apparatuur met *end of life* (besturings)software in het netwerk, namelijk die apparaten/systemen die zich in het segment '[VERWIJDERD]' bevinden.
Ten aanzien van deze apparatuur heeft het GHZ aangegeven beperkte mogelijkheden te hebben om ervoor te zorgen dat geen gebruik meer wordt gemaakt van *end of life* software. De inzet van de werkgroep van de [VERWIJDERD] om de leveranciers te bewegen mee te werken en het zelf communiceren met de leveranciers zijn maatregelen die mogelijk effect kunnen hebben maar die geen uitsluitsel geven dat de situatie binnen afzienbare tijd is opgelost.
Het GHZ zal, als de verantwoordelijke voor de gegevensverwerking met de leveranciers (die het beheer uitvoeren), afspraken moeten maken over zowel het

uitfaseren van *end of life* software als het zoveel mogelijk beperken van veiligheidsrisico's waar deze uitfasering (nog) niet heeft plaatsgevonden. Daarbij zouden voorwaarden moeten worden opgenomen over het gebruik van *end of life* software en het update-beleid van de leverancier. Voor zover deze leveranciers kunnen worden aangemerkt als bewerker in de zin van artikel 1, onderdeel e van de Wbp zullen dergelijke voorwaarden deel uit moeten maken van de bewerkersovereenkomst zoals bedoeld in artikel 14 van de Wbp.
Zoals ook eerder aangegeven zijn de aanvullende maatregelen die het GHZ heeft getroffen ten aanzien van de monitoring van het interne netwerk en de firewall tussen het interne en het externe netwerk niet voldoende om de risico's van apparatuur met *end of life* (besturings)software te beperken of weg te nemen. Dit geldt ook als het een gesegmenteerd netwerk betreft. De kwetsbaarheden die niet bekend zijn (en die juist in systemen met *end of life* (besturings)software kunnen voorkomen) kunnen niet gedetecteerd noch verholpen worden en kwetsbaarheden die wel bekend zijn worden pas opgemerkt als het alarm afgaat en het beveiligingsincident dus al heeft plaatsgevonden.

Het GHZ dient uiteindelijk toe te werken naar een situatie waarbij geen apparatuur met *end of life* (besturings)software op het netwerk is aangesloten, aangezien het gebruik van *end of life* (besturings)software een ernstig beveiligingsrisico vormt voor (bijzondere) persoonsgegevens. Uit het onderzoek van het CBP blijkt niet dat het GHZ op termijn alle apparatuur met *end of life* (besturings)software zal uitfaseren.

Conclusie voorlopige bevindingen

GHZ verwerkt medische gegevens van patiënten in een netwerk waarop medische apparatuur is aangesloten met *end of life* (besturings)software. Het (deel)netwerk met de *end of life* (besturings)software is in ieder geval tot maart 2016 niet gesegmenteerd. Het gebruik van *end of life* (besturings)software en het gebruik van een niet gesegmenteerd netwerk leidt afzonderlijk en in combinatie bezien tot ernstige beveiligingsrisico's.
Hoewel het GHZ inmiddels maatregelen heeft genomen om het netwerk te segmenteren is dit proces nog niet voltooid en blijven ook daarna de beveiligingsrisico's als gevolg van het gebruik van *end of life* (besturings)software bestaan.
De beveiligingsrisico's van de apparatuur met deze software dienen, zolang deze apparatuur nog in het netwerk aanwezig is, (voortdurend) in kaart te worden gebracht en er dienen (doorlopend) technische en/of organisatorische maatregelen te worden getroffen om deze risico's zoveel mogelijk te beperken dan wel weg te nemen. Uiteindelijk moet door het GHZ worden toegewerkt naar een situatie waarbij geen *end of life* (besturings)software meer gebruikt wordt.

De maatregelen die GHZ heeft getroffen ten aanzien van het gebruik van apparatuur met *end of life* (besturings)software zijn, zowel nu als na april 2016, onvoldoende om de beveiligingsrisico's zoveel mogelijk te beperken of weg te nemen.

Het GHZ heeft derhalve vooralsnog niet voldaan aan het in artikel 13 Wbp bepaalde vereiste dat de verantwoordelijke passende technische en organisatorische

maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking en handelt hiermee in strijd met artikel 13 Wbp.

4 ZIENSWIJZE VAN HET GHZ OP DE VOORLOPIGE BEVINDINGEN

Het GHZ is in de gelegenheid gesteld een zienswijze te geven op het rapport van voorlopige bevindingen van 13 maart 2014. Bij brief van 16 april 2014 heeft GHZ zijn zienswijze gegeven. Het CBP heeft vervolgens naar aanleiding daarvan op 15 mei 2014 aanvullende verduidelijkende vragen gesteld die zien op de *end of life* (besturings)systemen. Bij brief van 12 juni 2014 heeft GHZ deze vragen beantwoord. Het CBP vat deze antwoorden op als een aanvulling op de zienswijze van GHZ.

Zienswijze over het onderzoek van het CBP
In de zienswijze van het GHZ van 16 april 2014 gaat het GHZ onder andere in op de scope van het onderzoek van het CBP, de uitleg van passende maatregelen en de toetsing aan de richtsnoeren voor de beveiliging van persoonsgegevens.

Het GHZ stelt[42] dat het CBP een onderzoek is gestart naar de beveiliging van het netwerk van het GHZ naar aanleiding van de berichtgeving in de media over de inbraak / hack en de melding daarvan door het GHZ bij het CBP. "*Dit onderzoek heeft zich gaandeweg van de inbraak / hack uitgebreid tot een onderzoek naar de algehele beveiliging van de persoonsgegevens van het GHZ en het gebruik van end of life software door het GHZ in combinatie met netwerksegmentatie.*
Gelet hierop heeft het CBP de scope van zijn onderzoek tussentijds dus aanzienlijk verbreed"

Daarnaast stelt het GHZ[43] dat het CBP de lat waarlangs het CBP de beveiliging toetst heeft aangepast. "*Wij wijzen hierbij op de toets aan de hand van de CBP Richtsnoeren die pas per 1 maart 2013 in werking zijn getreden, dus ruim na de datum van de hack / inbraak en de start van het onderzoek daarnaar.*"
"*De richtsnoeren zijn pas op 1 maart 2013 in werking getreden terwijl de onderzoeksperiode van het CBP ook de periode van daarvoor beslaat (immers vanaf oktober 2012).* "[44]
Ook stelt het GHZ: "*Voorheen gold als uitleg voor artikel 13 Wbp als handvat A&V23, hetgeen een veel eenvoudigere en voor de praktijk werkbare indeling in risico-klassen kende, terwijl de huidige Richtsnoeren de veel ingewikkeldere Plan-do-check-act methodiek hanteren.*"[45]

Het GHZ stelt in de zienswijze[46] dat zij de gesprekken met het CBP "*steeds als open, positief kritisch en opbouwend heeft ervaren en niet als een onderzoek dat in de perceptie van het GHZ zou kunnen leiden tot bestuursrechtelijke handhavingsmaatregelen […] In die zin zijn de voorlopige bevindingen van het CBP voor het GHZ onverwacht anders van toon en niet conform het beeld dat het CBP in zijn gedragingen heeft geschetst."*

[42] Brief van 16 april 2014, randnummer 1.3, pagina 3.
[43] Brief van 16 april 2014, randnummer 1.4, pagina 4.
[44] Brief van 16 april 2014, randnummer 2.3, pagina 4.
[45] Brief van 16 april 2014, randnummer 2.3, pagina 4.
[46] Brief van 16 april 2014, randnummer 1.5, pagina 5.

Zienswijze over de beveiliging
In de zienswijze van GHZ van 16 april 2014 en 12 juni 2014 gaat het GHZ tevens in op de conclusies van het CBP ten aanzien van de segmentering van het netwerk en de *end of life* (besturings)software. De zienswijze ten aanzien van deze aspecten is als volgt samen te vatten.

End of life (besturings)software
Het GHZ geeft in de zienswijze aan dat zij inmiddels gebruik maakt van geautomatiseerde scan software[47] om doorlopend een volledig beeld te hebben van de in het netwerk aanwezige apparatuur. De rapportages van de scan software geven inzicht in onder andere de besturingssoftware.[48]
Het GHZ stelt in de brief van 16 april 2014 dat door het actief scannen van het netwerk "*meer systemen met end of life software (Windows 2000 en ouder) aanwezig zijn dan oorspronkelijk gedacht*."[49]

Het GHZ stelt dat zij op 9 april 2014 voor 97% gereed is met het uitfaseren van *end of life* (besturings)software.[50] Voor "*de systemen die nog wel gemigreerd moeten en kunnen worden naar* [VERWIJDERD]*, maar die niet tijdig gemigreerd konden worden*" (dit betreft [aantal] systemen)[51] is een aanvullende en daarmee tijdelijke beveiligingsmaatregel genomen. Deze maatregel bestaat uit extra beveiliging met speciale [VERWIJDERD] software [VERWIJDERD].[52]
Als aanvulling op deze technische maatregel is een organisatorische maatregel getroffen, die ziet op het gecontroleerd wijzigen van de configuratie van de [VERWIJDERD] software.
[VERWIJDERD]."[53]

Het GHZ geeft aan dat op 9 april 2014 in totaal [aantal] systemen[54] niet gemigreerd konden worden of [VERWIJDERD]. Deze systemen worden uiterlijk oktober 2014 in een toepasselijk netwerksegment geplaatst. In de brief van 12 juni 2014 geeft het GHZ met een nieuwe tijdsplanning aan dat inmiddels [VERWIJDERD] en dat [aantal] systemen al opgenomen zijn in een apart segment.[55]

Het GHZ licht met drie argumenten toe waarom de [aantal] systemen niet gemigreerd of [VERWIJDERD]:[56]

1. "*er is sprake van een gecertificeerde toepassing in een kritisch proces waardoor het moment van aanpassing zeer zorgvuldig in de tijd gepland moet worden omdat labuitslagen anders als niet betrouwbaar worden aangemerkt voor de periode waarin de certificering is onderbroken*."

[47] [VERWIJDERD] Scanner. Brief GHZ van 16 april 2014, randnummer 3.11, pagina 8 en Brief GHZ van 12 juni 2014, pagina. 1.
[48] Brief GHZ van 12 juni 2014, bijlage 1, pagina 5 bevat een sample van de uitdraai van [VERWIJDERD].
[49] Brief GHZ van 16 april 2014, randnummer 3.10, pagina 6.
[50] Brief GHZ van 16 april 2014, randnummer 3.12 en bijlage 2 en brief GHZ van 12 juni 2014.
[51] Brief GHA van 16 april 2014, bijlage 2.
[52] [VERWIJDERD].
[53] Brief GHZ van 12 juni 2014, pagina 2.
[54] Brief GHZ van 16 april 2014, bijlage 2: [VERWIJDERD]
[55] Brief GHZ van 16 april 2014, pagina 2, en planning in bijlage 2, pagina 6-7.
[56] Brief GHZ van 16 april 2014, randnummer 3.15, pagina 7.

2. "(*on)beschikbaarheid van* [VERWIJDERD]-*ondersteunende functionele software. Waar mogelijk heeft het GHZ deze applicaties geupgrade*."
3. "*specifieke signalen vanuit de daarvoor verantwoordelijke gebruikers van de systemen in het GHZ, leveranciers en ICT-deskundigen over de negatieve effecten van* [VERWIJDERD] *op de adequate werking van deze systemen*."

In de brief van 12 juni 2014 stelt het GHZ:
"*De systemen die wij niet kunnen upgraden naar* [VERWIJDERD]*, niet extra kunnen beveiligen of niet kunnen vervangen, maar toch moeten blijven gebruiken vanwege hun specifieke werkzaamheid, worden in een apart segment geplaatst. Het betreft hier systemen die we niet mogen updaten zonder langdurige voorbereiding en planning. Het betreft hier met name systemen die onderdeel uitmaken van een bedrijfskritische gekalibreerde en gecertificeerde opstelling.[…] Kalibratie en certificering zijn uitgebreide en zeer tijdrovende processen*."
In de brief geeft het GHZ aan dat de combinatie van apparaten waar dit systeem onderdeel van uitmaakt (de straat) niet gebruikt worden tijdens kalibratie en certificering. "*Dit betekent een technisch risico indien van de inwerking zijnde straat om technische redenen apparatuur uitvalt. Indien dit gebeurt valt de gehele productie stil en daarmee komt de patiënt mogelijk in gevaar omdat de uitslag niet meer betrouwbaar is of niet tijdig beschikbaar komt waarbij de behandeling niet kan starten. Deze systemen updaten zichzelf daarom ook per definitie niet via het internet want deze ongecontroleerde updates doorbreken in ieder geval de certificering, maar kunnen ook tot ongewenste resultaten leiden. Upgrades van deze apparatuur is kostbaar en risicovol en verloopt uitsluitend op lange termijn gepland en in zeer nauwe samenwerking/afstemming met de leverancier en de apparatuur. Om het risico van besmetting van deze systemen verder te minimaliseren worden de systemen op de internet firewall en proxy volledig geblokkeerd voor internettoegang*."

In de brief van 16 april 2014 stelt het GHZ dat voor de resterende [aantal] systemen "*alleen na een risico- en impactanalyse per systeem op toepassing en omgeving kan worden bepaald wat de juiste aanpak moet zijn voor een migratie naar een ander netwerksegment. Dit is een arbeidsintensief proces, dat gestart is en dat loopt volgens de planning uiterlijk tot en met oktober 2014.*

Uit het onderzoek blijkt dat het GHZ de volgende (aanvullende) maatregelen zal treffen/heeft getroffen voor deze [aantal] systemen:[57]
1. "*Blokkering van alle interactie […] met het internet*."[58]
2. Monitoren van het netwerkverkeer tussen de verschillende segmenten waaruit het netwerk is opgebouwd.[59]
3. De invoering (uiterlijk begin september 2014) van een IPS op de interne firewall.[60]
4. "*Plaatsing in het Quarantaine-segment van het netwerk, zodra mogelijk per systeem*."[61]

[57] Brief GHZ van 16 april 2014, randnummer 3.17, pagina 7-8 en brief GHZ van 12 juni 2014, pagina 3.
[58] Brief GHZ van 16 april 2014, randnummer 3.17.1, pagina 7.
[59] Brief GHZ van 16 april 2014, pagina 5, randnummer 3.5.
[60] Brief GHZ van 12 juni 2014, pagina 3.
[61] Brief GHZ van 16 april 2014, randnummer 3.17.2, pagina 7.

5. Analyse van en overleg over de lijst met nog niet gemigreerde systemen "*om de mogelijkheden van (tijdelijke) buitengebruikstelling te onderzoeken en ook actie daarop te ondernemen.*" [62]
6. Het voornemen om "*gerichte, regelmatige, differentiële (vulnerability-)scans*" uit te voeren.[63]
7. Indien een zwaarwegend beveiligingsrisico ontdekt wordt, wordt deze direct opgepakt, beoordeeld op (geaccepteerde) risico's, nieuwe risico's en te nemen (aanvullende) maatregelen.[64]
8. Het monitoren en (laten) verifiëren van de maatregel(en) voor geïdentificeerde risico's door het lijnmanagement op de afdeling ICT.[65]
9. "*Een actieve houding (in woord en daad)*" naar de leveranciers van de [VERWIJDERD] systemen voor het verkrijgen van systeemupgrades.[66]

Segmentering netwerk
Ten aanzien van de netwerksegmentering geeft het GHZ aan dat het rapport van voorlopige bevindingen gebaseerd is op gedateerde informatie. De basissegmentering zal eind oktober 2014 zijn doorgevoerd.[67] Het GHZ stelt "*Het GHZ heeft 2016 aangegeven als de termijn waarop verdere deelsegmentering naar de specifieke behoeften en maatstaven van het GHZ zelf zijn afgerond. Dit betreft dus een nadere verfijning, die niet strikt noodzakelijk is om te voldoen aan artikel 13 Wbp.*"

Aan het netwerk van het GHZ zijn momenteel [aantal] systemen aangesloten.[68] Voor het beheer van het (gesegmenteerde) netwerk wordt gebruik gemaakt van [VERWIJDERD]: [Bedrijfsnaam] voor het beheer van het LAN, [Bedrijfsnaam] voor het monitoren van het netwerk verkeer, [Bedrijfsnaam] voor het beheer van de firewall, de IPS en het spamfilter, en [Bedrijfsnaam] voor het beheer van de virusscanning.[69] Het interne beheer is belegd bij [VERWIJDERD], waaronder een Chief Information Security Office (CISO).[70]
Het GHZ geeft aan dat zij ruim [aantal] applicaties heeft en een inspanning levert om deze te standaardiseren tot ca. [aantal] applicaties.[71]
GHZ geeft aan het migratietraject voltooid zal zijn voor eind oktober 2014.[72] GHZ geeft aan dat tegen die tijd "alle systemen met daarop *end of life* (besturings)systemen die niet gemigreerd kunnen worden in een apart quarantaine segment zijn geplaatst.[73] Dit betreft [percentage] van alle systemen.[74]

[62] Brief GHZ van 16 april 2014, randnummer 3.17.3, pagina 7.
[63] Brief GHZ van 16 april 2014, randnummer 3.17.4, pagina 7.
[64] Brief GHZ van 12 juni 2014, pagina 2 en 3.
[65] Brief GHZ van 12 juni 2014, pagina 3.
[66] Brief GHZ van 16 april 2014, randnummer 3.17, pagina 8.
[67] Brief GHZ van 16 april 2014, randnummer 3.3, pagina 4
[68] [VERWIJDERD].FD. Brief GHZ van 16 april 2014, randnummer 3.1, pagina 15 en bijlage 2..
[69] Brief GHZ van 16 april 2014, bijlage 1, pagina 16, randnummer 3.5, pagina 5.
[70] Brief GHZ van 16 april 2014, bijlage 1, pagina 15.
[71] Brief GHZ van 16 april 2014, randnummer 5.2, pagina16
[72] Brief GHZ van 16 april 2014, randnummers 3.3, pagina4 en 3.7, pagina 5 en 3.13, pagina 6 en 3.18, pagina 8 en 3.20, pagina8 en 3.23 pagina9 en 3.16, pagina 7, en brief GHZ van 12 juni 2014, pagina 2 en bijlage 2, pagina 6-7.
[73] Brief GHZ van 16 april 2014, randnummer 3.4 en 3.6 – 3.8, pagina 5.
[74] Brief GHZ van 16 april 2014, randnummer 3.13, pagina 6.

GHZ geeft aan dat voor de resterende [percentage] (de [aantal] systemen), een (technische) maatregel getroffen *zal gaan* worden (uiterlijk begin september 2014) in de vorm van IPS filtering tussen de netwerk segmenten. IPS filtering is een maatregel die ziet op het bewaken van het interne netwerkverkeer.[75]

Uit de brief van 15 september 2014, het telefoongesprek van het CBP met het GHZ op 22 september 2014 en de e-mail van het GHZ aan het CBP van 22 september 2014 blijkt dat inmiddels [aantal] kwetsbare systemen zijn vervangen of uitgefaseerd.
Ook is inmiddels IPS op de interne firewall ingevoerd.

Het GHZ heeft in de brief van 15 september 2014 aangegeven dat er vanaf week 46 (week van 10 november) vulnerability scans zullen plaatsvinden. Deze zullen worden uitgevoerd door [Bedrijfsnaam] "*Daarbij gaat* [Bedrijfsnaam] *periodiek vanaf het interne netwerk van het GHZ (dus volledig intern gericht) de Vulnerability scan uitvoeren.*" Het GHZ geeft aan dat hiermee wordt gecontroleerd of de maatregelen die zij heeft getroffen ten aanzien van de kwetsbare systemen, zoals het plaatsen in een apart segment waarbij de systemen door een interne firewall beperkt worden in hun communicatie, voldoende zijn of dat er eventueel extra maatregelen moeten worden getroffen.
Tevens geeft het GHZ in de e-mail van 22 september 2014 aan dat het GHZ op dit moment door verschillende partijen[76], periodiek een scan laat uitvoeren vanaf het internet (dus van buiten naar binnen gericht) om eventuele kwetsbaarheden de detecteren en te verhelpen.
De genoemde interne en externe vulnerability scans, zijn een wijziging van de aanvullende maatregel (bovengenoemd punt 6): het voornemen om "gerichte, regelmatige, differentiële (vulnerability-)scans" uit te voeren. Het GHZ gaf tijdens het telefoongesprek van 22 september 2014 aan dat er toch geen penetratietesten op apparatuur met *end of life* (besturings)software zullen worden uitgevoerd, omdat al bekend is dat er in die systemen kwetsbaarheden aanwezig zijn.

Tot slot stelt het GHZ in de e-mail van 22 september 2014 dat, als de [aantal] resterende kwetsbare systemen in een apart VRF segment zijn geplaatst, "*is gerealiseerd dat deze laatste* [aantal] *systemen door de interne firewall beperkt worden in hun communicatie omdat bij de communicatie met deze systemen alleen goedgekeurde IP adressen en poorten toegestaan zijn. Tevens wordt al het verkeer van deze systemen met de IPS module op de interne firewall gemonitord. Hiermee is het risico op besmetting van de systemen geminimaliseerd. Mochten deze systemen alsnog besmet worden dan wordt dit tijdig gedetecteerd en kunnen de systemen eenvoudig van het netwerk verwijderd worden.*"

Beoordeling zienswijze

Beoordeling 'zienswijze ten aanzien van het onderzoek'
Het GHZ stelt ten eerste dat de scope van het onderzoek breder is geworden tijdens het onderzoek. "*Dit onderzoek heeft zich gaandeweg van de inbraak / hack uitgebreid tot een onderzoek naar de algehele beveiliging van de persoonsgegevens van het GHZ en het gebruik van end of life software door het GHZ in combinatie met netwerksegmentatie.*"

[75] Brief GHZ van 16 april 2014, randnummer 3.14, pagina 6.
[76] In 2013 is dit uitgevoerd door [Bedrijfsnaam], in 2014 wordt dit uitgevoerd door [Bedrijfsnaam].

Anders dan het GHZ stelt, is er geen sprake van verbreding van de scope van het onderzoek. Het CBP heeft na het bekend worden van het datalek inlichtingen gevraagd aan het GHZ.
Het GHZ heeft na het datalek zelf onderzoek laten doen door [Bedrijfsnaam] naar dit beveiligingslek. Ook in 2010 heeft [Bedrijfsnaam] onderzoek gedaan naar de beveiliging van het GHZ. Daarbij heeft [Bedrijfsnaam] verschillende kwetsbaarheden geïdentificeerd waaronder het gebruik van *end of life* (besturings)software.[77] Het CBP heeft het GHZ verzocht aan te tonen dat zij voldoende opvolging heeft gegeven aan kwetsbaarheden die [Bedrijfsnaam] constateerde in 2010 en 2012. Het GHZ heeft daartoe een onderzoek laten uitvoeren door [Bedrijfsnaam].[78] Uit dit onderzoek bleek dat bij het GHZ diverse medische systemen op het netwerk waren aangesloten, waarop *end of life* besturingssoftware draaide.[79] Ook bleek uit dit rapport dat het netwerk niet gesegmenteerd was.[80] Het CBP constateerde dat dit, gelet op artikel 13 van de Wbp, substantiële beveiligingsrisico's voor de bescherming van de medische (persoons)gegevens van patiënten van het GHZ tot gevolg had en heeft op grond hiervan besloten een ambtshalve onderzoek in te stellen naar de naleving van artikel 13 Wbp. Het CBP heeft het GHZ hiervan bij brief van 19 april 2013 op de hoogte gesteld.

Daarnaast stelt het GHZ[81] dat het CBP de lat waarlangs het CBP de beveiliging toetst heeft aangepast. "*Wij wijzen hierbij op de toets aan de hand van de CBP Richtsnoeren die pas per 1 maart 2013 in werking zijn getreden, dus ruim na de datum van de hack / inbraak in de start van het onderzoek daarnaar*."

De Richtsnoeren beveiliging zijn op 1 maart 2013 in werking getreden. De normen evenwel, met betrekking tot de beveiliging zoals in dit onderzoek gehanteerd ten aanzien van *end of life* (besturings(software) en segmentatie van het netwerk, zijn ontleend aan de Code voor informatiebeveiliging NEN-ISO/IEC 27002 (2007) en NEN-7510 (2011).
De richtsnoeren hebben de lat waarlangs het CBP de beveiliging toetst dan ook niet gewijzigd. De Richtsnoeren zijn slechts een nadere uitleg van deze wijze waarop het CBP de normen uit de bestaande beveiligingsstandaarden toepast. Dit blijkt ook uit de samenvatting in de Richtsnoeren beveiliging persoonsgegevens[82]: "*Deze richtsnoeren leggen uit hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. De richtsnoeren vormen de verbindende schakel tussen enerzijds het juridisch domein, met daarbinnen de eisen uit de Wbp, en anderzijds het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen. Dat betekent dat de richtsnoeren in samenhang moeten worden gebruikt met algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de Code voor Informatiebeveiliging of de ict-beveiligingsricht-lijnen voor webapplicaties van het Nationaal CyberSecurity Centrum.*"

[77] Rapportage [Bedrijfsnaam], [Titel rapport].
[78] [Bedrijfsnaam]: [Titel rapport].
[79] [Bedrijfsnaam]]: [Titel rapport].
[80] [Bedrijfsnaam]]: [Titel rapport].
[81] Brief van 16 april 2014, randnummer 1.4, pagina 4.
[82] Richtsnoeren beveiliging persoonsgegevens, februari 2013, pagina 2.

Het GHZ stelt in de zienswijze van 16 april 2014 dat zij de gesprekken met het CBP niet heeft ervaren *"als een onderzoek dat in de perceptie van het GHZ zou kunnen leiden tot bestuursrechtelijke handhavingsmaatregelen. […] In die zin zijn de voorlopige bevindingen van het CBP voor het GHZ onverwacht anders van toon en niet conform het beeld dat het CBP in zijn gedragingen heeft geschetst."*
Bij brief van 19 april 2013 heeft het CBP uitdrukkelijk aan het GHZ medegedeeld dat het CBP een ambtshalve onderzoek ex artikel 60 van de Wbp instelt naar de beveiliging van persoonsgegevens door het GHZ. Artikel 65 Wbp luidt: "*Het College is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van de bij of krachtens deze wet gestelde verplichtingen."* Indien uit een onderzoek blijkt dat een verantwoordelijke de Wbp overtreedt, kan dit derhalve tot bestuursrechtelijke handhavingsmaatregelen leiden.

Beoordeling 'zienswijze ten aanzien van de beveiliging"
Zoals in het juridisch kader is aangegeven worden aan het GHZ tenminste de volgende eisen gesteld om te kunnen voldoen aan artikel 13 Wbp:

1. beveiligingsrisico's dienen (doorlopend) in kaart te worden gebracht;
2. er moeten (doorlopend) organisatorische en/of technische maatregelen worden getroffen om de geconstateerde risico's zoveel mogelijk te beperken, bijvoorbeeld door updates uit te voeren of andere maatregelen te treffen indien het niet mogelijk is om bepaalde (besturings)software te updaten;
3. grote netwerken dienen beveiligd te worden door (technische) scheiding, bijvoorbeeld door segmentering van de diverse domeinen.

Ad.1. Het GHZ heeft in de zienswijze van 16 april 2014 en 12 juni 2014 aangegeven dat zij aanvullende maatregelen gaat treffen/heeft getroffen om de beveiligingsrisico's van de kwetsbare apparatuur doorlopend in kaart te brengen zoals:

- het monitoren van het netwerkverkeer;
- het voornemen om "gerichte, regelmatige, differentiële (vulnerability-)scans" uit te voeren[83]; en
- de invoering van een IPS op de interne firewall.

Ad.2. Het GHZ heeft in de zienswijze aangegeven dat zij tevens aanvullende maatregelen heeft getroffen om de geconstateerde risico's zoveel mogelijk te beperken zoals:

- de [VERWIJDERD] oplossing voor de systemen die nog wel gemigreerd moeten en kunnen worden naar [VERWIJDERD], maar die niet tijdig gemigreerd konden worden;
- blokkering van alle interactie van de nog niet gemigreerde systemen met het internet;
- analyse van en overleg over de lijst met nog niet gemigreerde systemen "*om de mogelijkheden van (tijdelijke) buitengebruikstelling te onderzoeken en ook actie daarop te ondernemen.*";

[83] In het telefoongesprek en de e-mail van 22 september 2014 is door het GHZ aangegeven dat periodiek zowel vanaf het internet als vanaf het interne netwerk van het GHZ (dus volledig intern gericht) vulnerability scans (zullen) worden uitgevoerd."

- indien een zwaarwegend beveiligingsrisico ontdekt wordt, wordt deze direct opgepakt, beoordeeld op (geaccepteerde) risico's, nieuwe risico's en te nemen (aanvullende) maatregelen;
- het (beleggen van de verantwoordelijkheid van) monitoren en verifiëren van de maatregel(en) voor geïdentificeerde risico's door het lijnmanagement op de afdeling ICT; en
- "*Een actieve houding (in woord en daad)*" naar de leveranciers van de (medische) systemen voor het verkrijgen van systeemupgrades.

Ad.3. Het GHZ heeft in de zienswijze aangegeven dat het plaatsen van de systemen met *end of life* software in de toepasselijke segmenten uiterlijk eind oktober 2014 gereed zal zijn.

Met deze door het GHZ voorgenomen en reeds getroffen aanvullende maatregelen in combinatie met de al eerder genomen maatregelen, wordt, zodra de systemen met *end of life* (besturings)software in het toepasselijke segment zijn geplaats, door het GHZ voldoende opvolging gegeven aan de genoemde beveiligingseisen en voldoet het GHZ daarmee ten aanzien van deze eisen aan artikel 13 Wbp.

Het GHZ heeft op dat moment passende technische en organisatorische maatregelen ten uitvoer gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van diefstal. De door het GHZ getroffen maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen

Aangezien de plaatsing van de systemen met *end of life* software in de toepasselijke segmenten naar verwachting eind oktober 2014 zal zijn afgerond, betekent dit dat tot deze datum niet is voldaan aan de eis dat grote netwerken beveiligd dienen te worden door (technische) scheiding, bijvoorbeeld door segmentering van de diverse domeinen. In de periode dat deze scheiding nog niet is gerealiseerd handelt het GHZ dus (nog) in strijd met artikel 13 Wbp.

5 Conclusie

Het GHZ verwerkt medische gegevens van patiënten in een netwerk waarop medische apparatuur is aangesloten met *end of life* (besturings)software. Het (deel)netwerk met de *end of life* (besturings)software is in ieder geval tot eind oktober 2014 niet gesegmenteerd. Het gebruik van *end of life* (besturings)software en het gebruik van een niet gesegmenteerd netwerk leidt zowel op zichzelf als in combinatie met elkaar tot ernstige beveiligingsrisico's.

Het GHZ heeft in de zienswijze van 16 april 2014 en 12 juni 2014 aangetoond dat zij maatregelen heeft getroffen en gaat treffen om de beveiligingsrisico's van de apparatuur met *end of life* besturingssoftware (voortdurend) in kaart te brengen en (doorlopend) technische en/of organisatorische maatregelen te treffen om deze risico's zoveel mogelijk te beperken dan wel weg te nemen.

Het GHZ heeft tevens maatregelen getroffen om het netwerk te segmenteren. In de zienswijze van 16 april 2014 heeft het GHZ aangegeven dat de basis segmentatie eind oktober 2014 zal zijn afgerond. Op dit moment is dit proces nog niet voltooid.
Het GHZ voldoet derhalve op dit moment niet aan de eis dat grote netwerken beveiligd dienen te worden door (technische) scheiding, bijvoorbeeld door segmentering van de diverse domeinen. Het GHZ handelt hiermee in strijd met artikel 13 Wbp.

Wanneer de systemen met *end of life* (besturings)software daadwerkelijk zijn ondergebracht in het toepasselijke segment, handelt het GHZ, óók gelet op de overige getroffen maatregelen, niet meer in strijd met artikel 13 Wbp.