Radboud Universiteit Nijmegen

Faculteit der Natuurwetenschappen, Wiskunde en informatica

Master Thesis

"Risico-analyse van het Landelijk Schakelpunt, hart van de informatievoorziening in de zorg."

Auteur:	René van Rossum
Afstudeerbegeleiders:	Dr. Martijn Oostdijk en Dr. Perry Groot
Referent:	Dr. Erik Poll
Afstudeernummer:	62 IK

Colofon

Auteur:	René van Rossum
Opleiding:	Informatiekunde
Afstudeernummer:	62 IK
Specialisatie:	Information Security
Opdracht:	“Risicoanalyse van het Landelijk Schakelpunt, hart van de informatievoorziening in de zorg.”
Universiteit:	Radboud Universiteit Nijmegen (RU) Comeniuslaan 4 6525 HP Nijmegen Postbus 9102 6500 HC Nijmegen Telefoon: 024-3616161 Fax: 024-3564606 Internet: www.ru.nl
Faculteit:	Faculteit Natuurwetenschappen, Wiskunde & Informatica (FNWI)
Instituut:	Nijmeegs Instituut voor Informatica en Informatiekunde (NIII)
Afstudeerbegeleider:	Dr. Martijn Oostdijk
Afstudeerbegeleider:	Dr. Perry Groot
Referent:	Dr. Erik Poll
Plaats, datum:	Nijmegen, 10 november 2007
Versie, status:	1.01, Definitief

Overal in dit document waar de voornaamwoorden “hij” of “zijn” staat, wordt “hij of zij” resp. “zijn of haar” bedoeld.

Voorwoord

Voor u ligt de definitieve versie van mijn afstudeeronderzoek bij de Security Of Systems (SOS) groep aan de Radboud Universiteit te Nijmegen.

Het blijft toch een vak apart, dat schrijven. *Wat* wil ik overbrengen aan de lezer, en *hoe* doe ik dat? Het continue kritisch kijken naar het product levert steeds weer hoofdbrekens op wanneer er toch weer een rare of kromme zin opduikt. Het is duidelijk dat het schrijven van goed te lezen en te begrijpen teksten het nodige zweet heeft gekost. Bloed en tranen gelukkig niet. Een last is er van me afgevallen. Hiermee komt dan ook een eind aan mijn studie Informatiekunde. Desondanks komt er geen einde aan het studeren, want de ontwikkelingen volgen op dit gebied elkaar in hoog tempo op en betekend stilstand gegarandeerd achteruitgang.

Dit onderzoek levert een bijdrage aan de informatiebeveiliging in de zorgsector. Het geplande zorgsysteem zorgt voor een vergaande digitalisering wat een revolutie teweeg zal gaan brengen in de zorg. Hiermee hoopt men de zorgverlening aan de patiënt efficiënter en effectiever te maken. Ook wil men het aantal fouten hiermee proberen te reduceren. Het resultaat van dit onderzoek wordt getracht aan te tonen dat er ondanks de goede bedoelingen er risico's zijn verbonden aan het uitwisselen van patiëntinformatie zoals het NICTIZ dat wil realiseren. De betrouwbaarheid van het systeem en de privacy van patiënten komen in het geding en kunnen alleen verbeterd worden door in ieder geval de risico's weg te nemen en de algehele infrastructuur te heroverwegen.

Dank ben ik verschuldigd aan iedereen die een bijdrage aan dit onderzoek heeft geleverd. En in het bijzonder aan: Dr. Martijn Oostdijk, Dr. Perry Groot en Dr. Erik Poll voor hun begeleiding van het onderzoekstraject, de interessante discussies, oplossingsgerichte ideeën en de bereidheid om uitwerkingen te beoordelen. Zonder hun vakkundige hulp was dit onderzoek een puddingtaart.

Een speciaal dankwoord ben ik verschuldigd aan de voormalige bewoners van N3080. Berucht, in de kamer als ver daar buiten! Het was geweldig.

René van Rossum

Nijmegen, 10 november 2007

Samenvatting (abstract)

De manier van uitwisselen van patiëntinformatie in de zorg ondergaat de komende tijd een transformatie. Na uitbreiding en aanpassing van de huidige basisinfrastructuur zullen zorgverleners beter en sneller met patiëntinformatie om kunnen gaan. Het moet dan mogelijk zijn om alle informatie die van een patiënt bekend is direct in te kunnen kijken en nieuwe feiten aan het bestaande dossier toe te kunnen voegen. Dit met als doel de zorg efficiënt en effectief te maken, het aantal “medische missers” te reduceren en de patiënt gerichter te kunnen bedienen.

Deze informatie zal via het beoogde Landelijk Schakelpunt (LSP) beschikbaar komen voor zorgverleners die voor het uit kunnen voeren van hun functie beschikkingsbevoegdheid hebben. Voor hen is patiëntinformatie via het door NICTIZ ontworpen infrastructuur altijd direct opvraagbaar.

In dit onderzoek beschrijft hoe de infrastructuur er volgens de NICTIZ specificaties eruit komt te zien. Daarbij wordt inzichtelijk gemaakt welke functies het LSP herbergt. Specifiek wordt de wijze van toegang en de beveiliging daarom heen beschreven evenals het loggen van uitgevoerde acties. Resultaten zijn verkregen door het uitvoeren van een literatuurstudie. Met deze kennis en inzichten is het mogelijk om de uiteindelijk risicoanalyse uit te kunnen voeren. Deze risicoanalyse bevat vele mogelijkheden die vanuit het oogpunt van een kwaadwillende aantoont op welke onrechtmatige wijze toegang tot het LSP kan worden verkregen. Door het toevoegen van een risicofactor is uiteindelijk inzichtelijk welke risico’s daadwerkelijk in aanmerking komen om direct te worden opgelost en welke risico’s vanwege een lagere score ook pas op een later moment kunnen worden opgelost. Dit met als doel de infrastructuur en met name het LSP veiliger en betrouwbaarder te maken. Hierdoor zijn confidentiality, integrity en availability van de patiëntinformatie gewaarborgd.

Inhoudsopgave

"Electronic health information will provide a quantum leap in patient power, doctor power and effective health care."

Tommy Thompson

1. Inleiding

1.1 Berichtgeving uit de media

Een artikel over ernstige beveiligingslekken in het Elektronische Patiënten Dossier (EPD) van ziekenhuizen.

HET MEDISCH GEHEIM IS IN GEVAAR

03 september 2005, Karin Spaink [VOL05]

"Om de proef op de som te nemen liet ik experts van de beveiligingsbedrijven ITSX, Fox-IT en Madison Gurka de beveiliging van twee ziekenhuizen testen. De resultaten waren schrikbarend. Beide ziekenhuizen waren ernstig lek. Bij een ziekenhuis hebben 'mijn' hackers twee weken lang toegang gehad tot 1,2 miljoen patiëntgegevens en niemand merkte dat op. Ik kon de gegevens bestellen die ik wilde en kreeg ze dan binnen tien minuten per e-mail aangeleverd. Namen, adressen, telefoonnummers, patiëntnummers, polisnummers, geslacht, geboortedatum, lengte, gewicht, dood of levend. Erbij zat ook een lijst met patiënten die een besmettelijke ziekte hadden. Bij het andere ziekenhuis konden ze eveneens vrijelijk zoeken in alle interne gegevens.
[...]

Enkele dagen later volgde een reactie op bovenstaand artikel op de website van Computable:

NICTIZ: "STOPPEN MET EPD IS GEEN OPTIE"

06 september 2005, NICTIZ [WEBCOM]

Stoppen met de ontwikkeling van het EPD is geen optie. Dat laat het Nationaal ICT Instituut in de Zorg (NICTIZ) weten in reactie op de bevindingen van publiciste Karin Spaink.

Zorginstellingen zijn verantwoordelijk voor een goede beveiliging van hun medische informatie, zowel op papier als elektronisch. Het mag nooit voorkomen dat onbevoegden inzage hebben in medische gegevens, laat staan dat ze deze kunnen wijzigen. Het is aan te bevelen dat ziekenhuizen periodiek hun beveiliging laten testen door hackers, laat het NICTIZ in een persbericht weten.

Het reageert hiermee op de onthulling dat onlangs specialisten erin zijn geslaagd de elektronische dossiers van 1,2 miljoen patiënten van twee Nederlandse ziekenhuizen te openen. Deze "proefhack" werd gedaan in het kader van het boek Medische Geheimen, dat Spaink schreef.
[...]

1.2 Aanleiding

Ondanks de bevindingen van Karin Spaink en uit de resultaten van vele projecten in andere landen op dit gebied, zal het EPD ook in Nederland worden ingevoerd. Hiervoor zal een nieuwe basisinfrastructuur worden geïntroduceerd waarbij het Landelijk SchakelPunt (LSP) een belangrijke centrale rol gaat spelen.

Het LSP zal als verkeerstoren miljoenen verwijzingen naar lokaal opgeslagen patiënteninformatie bevatten van alle geregistreerde Nederlanders. Deze database bevat geen cruciale gegevens, maar vormt wel de schakel naar deze belangrijke en privacy gevoelige patiëntengegevens.

Door de aangewakkerde commotie rondom de herstructurering in de zorg en voornamelijk de ophef over de hack op twee zorgsystemen waarbij ruim 1,2 miljoen patiëntendossiers werden buitgemaakt, rijzen zowel binnen als buiten de zorg de vragen op betreffende privacy, veiligheid, risico's en beveiliging over het digitaal uitwisselen van patiëntgegevens.

Vast staat dat het LSP, dat door automatiseerder CSC Nederland is ontwikkeld, al in gebruik wordt genomen en dat er patiëntgegevens via de digitale dossiers tussen zorgaanbieders worden uitgewisseld. Hierbij staan we aan de vooravond van een revolutie in de zorgsector en de manier van werken voor de zorgverleners waarbij de beveiligingsaspecten een grote rol gaan spelen.

1.3 Onderzoeksvraag en vraagstelling

1.3.1 Onderzoeksvraag

De basis van dit onderzoek is gebaseerd op de hierboven genoemde feiten. De onderzoeksvraag dat hieruit voorvloeit is als volgt verwoord:

> **Welke mogelijkheden heeft een kwaadwillende om toegang te krijgen tot het LSP en hoe kunnen de invloeden van de gevonden risico's worden beperkt.**

1.3.2 Vraagstelling

Uit de onderzoeksvraag zijn twee deelvragen afgeleid. De eerste vraag betreft het beschrijven van het LSP systeem zoals het NICTIZ dat heeft gespecificeerd. Dit om een indruk te geven van de infrastructuur en de bedoeling en werking van het geheel. De tweede vraag gaat in op de vraag hoe een kwaadwillende zich toegang verschaft tot het LSP door juist niet gebruik te maken van de gespecificeerde inlogprocedure en daarbij de risico's in kaart te brengen.

De betreffende onderzoeken kunnen worden onderscheiden in de volgende deelvragen:

1. Hoe zit het NICTIZ LSP in elkaar?

a. Hoe zit het LSP in elkaar?
b. Hoe verloopt de toegangprocedure?
c. Hoe verloopt de logprocedure?
d. Welke ontwerpkeuzes heeft men gemaakt?
e. Wat zijn de voor- en nadelen van een centraal of een decentrale LSP en/of een centrale of een decentrale gegevensopslag?
f. Welke implementatiekeuzes zou men kunnen overwegen?

2. Hoe kan er op onrechtmatige wijze toegang tot het LSP worden verkregen en hoe kunnen daaruit voortvloeiende risico's worden beperkt?

a) Met welke methode kunnen de mogelijkheden die een kwaadwillende heeft om zijn doel te bereiken worden geïdentificeerd en schematisch in kaart worden gebracht?
b) Hoe kan per risico bepaald of het noodzakelijk is maatregelen te treffen tegen het geïdentificeerde risico.
c) Hoe kunnen invloeden van geïdentificeerde risico's worden beperkt?

1.4 Begrenzingen van dit onderzoek

Dit onderzoek is uitgevoerd door René van Rossum in het kader van de Master Thesis voor studierichting Informatiekunde aan de Radboud Universiteit te Nijmegen. René is afstudeerder bij de SOS.

Dit onderzoek kent een aantal beperkingen:

- Onderzoek naar systemen anders dan het LSP vallen buiten het bereik van dit onderzoek,
- Dit onderzoek zal een beeld schetsen van het LSP waarbij de technische details zoveel mogelijk wordt beperkt.
- Het behoort niet tot het doel het LSP in zijn geheel te beschrijven. Daarvoor wordt doorverwezen naar de NICTIZ documentatie [NICT05a] [NICT05b].
- De RAM richt zich op de mogelijke attacks op het LSP. De beschreven attacks hebben niet tot doel allesomvattend te zijn.
- De RAM beschrijft alleen de mogelijkheden, anders dan door het NICTIZ is vastgesteld, om toegang te verkrijgen tot het LSP.

Gedurende dit exploratieve onderzoek is gebleken dat de originele onderzoeksvraag en gestelde deelvragen, geformuleerd in het plan van aanpak voor dit onderzoek te ambitieus waren. De onderzoeksvraag en de deelvragen zijn daarom tussentijds aangepast en scherper afgebakend.

1.5 Relevantie

De zorgsector staat aan de vooravond van een grote verandering. Door de geplande invoering van het EPD en de basisinfrastructuur zal ICT zich definitief gaan nestelen in de primaire zorgprocessen. Voor- en tegenstanders geven hierbij hun visie en voorspellen succes of grote problemen. Hoe dan ook, de overheid heeft bepaald dat het EPD, LSP, Elektronisch Medicatie Dossier (EMD), AORTA e.d. er komen. De overheid en de minister van Volksgezondheid, Welzijn en Sport, ten tijde van het besluit tot invoering, Hans Hoogervorst, zijn positief gezind over het slagen van dit project.

Maar, hoe zit het met de risico's, nadelen en andere problemen die hun invloed in meer of mindere mate kunnen hebben op die alles omvattende basisinfrastructuur? Het NICTIZ heeft dan wel een specificatieontwerp opgesteld waaraan alle zorgsystemen zullen moeten voldoen, maar een blauwdruk en daadwerkelijke realisatie behoren tot twee uiteenlopende disciplines. Daarbij mag niet vergeten worden dat de complexiteit fouten binnen het systeem in de hand werkt. Kortom, geen gemakkelijke klus.

Tot op heden is er op het gebied van deze nieuwe infrastructuur beperkt onderzoek gedaan terwijl deze zorgvoorziening van groot belang wordt in onze Nederlandse zorgsector. Het beantwoorden van de onderzoeksvraag en deelvragen zijn daarom de moeite waard.
De werking van het LSP wordt eenvoudig beschreven, mogelijke attacks om via andere manieren dan die van het NICTIZ de LSP binnen te komen zullen uitgebreid aanbod komen, maar ook te nemen beschermmaatregelen worden aangedragen om deze attacks te bestrijden. Dit onderzoek draagt dan ook bij aan een veiliger en verbeterde informatiehuishouding binnen de digitale zorg.

1.6 Beoogde resultaten

Resultaten van dit onderzoek zijn samen te vatten in de volgende punten:

1. Dit onderzoek zal inzicht geven in de voorgestelde LSP-infrastructuur waardoor een beter beeld ontstaat van de werking van de basisinfrastructuur en het LSP.
2. De toegangs- als de logprocedure worden uitgelicht en gedetailleerd beschreven.
3. De NICTIZ configuratie wordt besproken alsmede zullen voor- en nadelen van deze configuratie ten opzichte van andere configuratiemogelijkheden worden gegeven waarna uiteindelijk voorstel wordt gegeven over de te kiezen configuratie.
4. Mogelijkheden die door kwaadwillenden kunnen worden gebruikt om op onrechtmatige wijze toegang te verkrijgen tot het LSP worden in kaart gebracht.
5. Beschreven attacks zullen met behulp van risicofactor geclassificeerd worden waardoor er inzicht verkregen wordt voor welke risico's direct maatregelen noodzakelijk is en voor welke niet.
6. Van elke attack zal een aanbeveling worden gegeven hoe deze kan worden bestreden waardoor risico's tot het minimaal wordt beperkt.

1.7 Leeswijzer

De inhoud van dit onderzoeksrapport bestaat uit de volgende hoofdstukken en bijlagen.

Hoofdstuk 1: In het eerste hoofdstuk van deze scriptie is de aanleiding en de doelstelling met de relevantie voor dit onderzoek beschreven.

Hoofdstuk 2: De methodische verantwoording betreffende dit onderzoek komt in hoofdstuk 2 aan bod.

Hoofdstuk 3: Het traject naar een Elektronisch Patiëntendossier en de daarbij behorende transformatie van traditionele naar digitale communicatie wordt in dit hoofdstuk nader uiteen gezet.

Hoofdstuk 4: Dit hoofdstuk geeft invulling aan de term information security en vormt een theoretische basis voor het begrijpen van de onderwerpen die aanbod komen in de volgende hoofdstukken.

Hoofdstuk 5: Het Landelijk SchakelPunt en de onderlinge samenhangende infrastructuur met de daarbij behorende diensten van het LSP worden beschreven in dit hoofdstuk.

Hoofdstuk 6: In hoofdstuk 6 zal stil worden gestaan bij de reguliere toegangsprocedure zoals het NICTIZ deze heeft opgesteld in haar specificaties en de hierbij gebruikte technieken.

Hoofdstuk 7: Hoofdstuk 7 beschrijft vervolgens de gehanteerde logprocedures en welke mogelijkheden men kan nemen om er voor te zorgen dat de vele data die wordt opgeslagen in de verschillende logbestanden bruikbaar en hanteerbaar blijven voor de beheerders van het LSP.

Hoofdstuk 8: Een nieuwe infrastructuur kan risico's met zich meebrengen voor de LSP en voornamelijk de informatie die hierop wordt uitgewisseld. Met behulp van een attack tree zal in hoofdstuk 8 inzicht gegeven worden op welke wijze men toegang kan krijgen tot de LSP en met welke middelen en methodes deze zijn te ondervangen of anders zoveel mogelijk te beperken.

Hoofdstuk 9: Afsluitend van deze scriptie zullen conclusies worden getrokken betreffende dit onderzoek. In dit laatste hoofdstuk zal onderzoeksvraag worden beantwoord en conclusies en aanbevelingen ten behoeve van het LSP en de basisinfrastructuur worden gegeven.

Appendix A: Tabellenlijst met gebruikte tabellen en hun locatie.

Appendix B: Figurenlijst met gebruikte figuren en hun locatie.

Appendix C: Gebruikte afkortingen in de scriptie zijn terug te vinden in deze lijst met afkortingen waarbij de volledige betekenis van de afkortingen wordt gegeven.

Appendix D: De gebruikte literatuur en verwijzingen naar literatuur in de scriptie zijn gebundeld in deze literatuurlijst.

"It is common sense to take a method and try it; if it fails,
admit it frankly and try another. But above all, try something."
Franklin D. Roosevelt

2. Methodische verantwoording

2.1 Onderzoeksmethode

Volgens de classificaties van [VER01] is dit onderzoek deels probleemsignalerend deels diagnostisch. Probleemsignalerend richt zich op het vaststellen van de oorzaken van een probleem. Het LSP zal vanaf het moment dat deze online gaat te maken krijgen met attacks om gegevens via onrechtmatige wijze te verkrijgen. Hierbij kan dus onderscheid gemaakt worden tussen de feitelijke situatie en wenselijke situatie. Tijdens het probleemsignalerend onderzoek zullen feitelijk mogelijke oorzaken in kaart worden gebracht en af worden gelegd tegen de wenselijke situatie. De aard van het probleem wordt daarmee in kaart gebracht. Met diagnostisch onderzoek wordt inzicht verkregen in de achtergronden van de bedreigingen en het ontstaan daarvan.

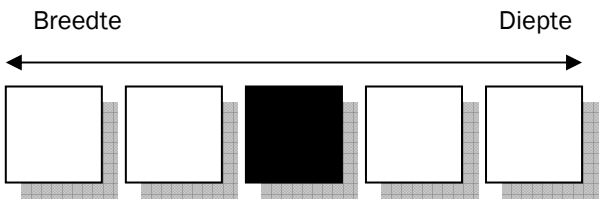
2.2 Onderzoekstypering

2.2.1 Typeringen

"De meest bepalende beslissing die u bij het maken van een technisch ontwerp voor uw afstudeerproject moet nemen is de keuze van een aanpak, ofwel onderzoeksstrategie. Onder een onderzoeksstrategie verstaan wij een geheel van met elkaar samenhangende beslissingen over de wijze waarop u het onderzoek gaat uitvoeren." [VER01]. Hierin wordt beschreven dat de wijze waarop een onderzoek dient te worden uitgevoerd gebaseerd is op een aantal kernbeslissingen. Deze worden bepaald door de breedte of diepgang, kwantificering of kwalificering en veldonderzoek of bureauonderzoek. Deze kernbeslissingen zijn ook toegepast op dit onderzoek en worden hieronder nader beschreven.

2.2.2 Breedte vs. Diepgang

Hoewel dit onderzoek niet de intentie heeft volledig te zijn, wordt wel geprobeerd enige diepgang mee te geven. Desondanks is ook de breedte van belang om een helder beeld te verkrijgen van de basisinfrastructuur.

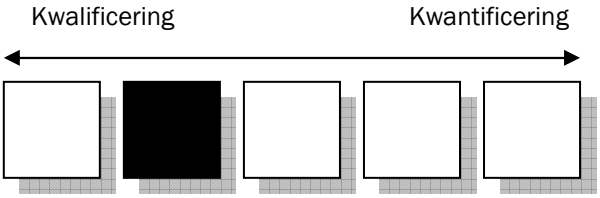


Figuur 2.1: Typering breedte versus diepgang

De diepgang wordt verkregen door dat het onderzoek een duidelijk beeld schept van de voorgestelde infrastructuur en gedetailleerd de mogelijke attacks en oplossingen voor deze attacks beschrijft. De breedte wordt gehaald uit het feit dat zowel de beschrijving van de gehele infrastructuur en niet alleen de LSP wordt beschreven. Immers het LSP maakt deel uit van de basisinfrastructuur en is dus afhankelijk van deze systemen. Om inzicht te krijgen in de werking van de basisinfrastructuur en om een correcte risicoanalyse mogelijk te maken is brede kijk op het geheel van belang.

2.2.3 Kwantificering vs. Kwalificering

Het onderzoek is meer kwalificerend en minder kwanticerend van aard.

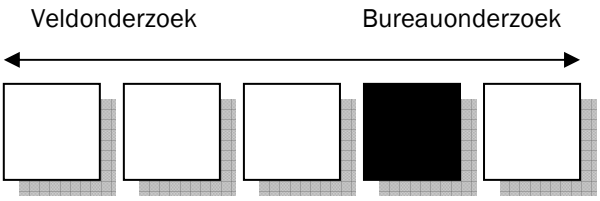


Figuur 2.2: Typering kwalificering vs. kwantificering

Het onderzoek leunt vooral op het beschouwende en verbale vlak ondersteund met bevindingen die worden weergegeven in tabellen en figuren.

2.2.4 Veldonderzoek vs. Bureauonderzoek

Het vergaren van informatie via de literatuur wordt in dit onderzoek aangevuld met belangrijke informatie verkregen van betrokken organisaties en deskundigen.



Figuur 2.3: Typering veldonderzoek vs. bureauonderzoek

Voornamelijk het eerste gedeelte van dit onderzoek is gebaseerd op het verzamelen van gegevens uit de bestaande literatuur. Echter, er is ook informatie verkregen door het uitvoeren van analyses waarmee het onderzoek een empirisch karakter krijgt. Beide middelen worden gebruikt in dit onderzoek. De balans op dit gebied neigt in de richting van bureauonderzoek.

2.3 Onderzoeksaanpak

Het onderzoek is opgedeeld in twee deelonderzoeken. Deze zijn reeds in sectie 1.3.2 beschreven. Om tot een antwoord te komen voor elk deelonderzoek kennen deze een specifieke aanpak. In deze sectie zal beschreven worden welke stappen ondernomen zullen worden om tot een antwoord te komen.

2.3.1 Wat is het voorgestelde LSP

Het doel van dit deelonderzoek is het achterhalen van de technische en organisatorische specificaties betreffende het LSP en de basisinfrastructuur. Daarnaast zal de toegangsprocedure en logprocedure nader worden belicht.

Het onderzoek concentreert zich in deze fase hoofdzakelijk op documentatie en rapporten van het NICTIZ. Daarnaast dient aanverwante literatuur om beter zicht te verkrijgen op onder andere de mogelijkheden, gemaakte keuzes, voor- en nadelen van diverse configuratieopties en verbeterpunten waardoor een ideale configuratie van de basisinfrastructuur kan worden gegeven.

2.3.2 Welke risico's zijn er door gebruik van een LSP-infractructuur?

Het tweede deelonderzoek is te betitelen als een casestudy waarbij attack mogelijkheden in kaart worden gebracht om toegang krijgen tot het LSP zonder gebruik te maken van de vastgestelde procedure. Het ontdekken van attacks en het in kaart brengen van deze mogelijkheden die veelal opgebouwd zijn uit al dan niet van elkaar afhankelijke onderliggende attacks wordt middels de attack tree van [SCH00] in kaart gebracht.

Door de geïdentificeerde attacks behoort het vervolgens tot de mogelijkheid om eventuele risico's bloot te leggen en daaraan een risicofactor te koppelen. Op basis van dit gegeven kan een uitspraak gedaan worden over de noodzaak om het risico van een attack te verlagen of weg te nemen, waardoor schade zoveel mogelijk wordt beperkt.

Het resultaat van dit deelonderzoek is een attack tree, opgedeeld in diverse niveaus, over eventuele attack mogelijkheden tot het LSP, een beschrijving van de attack, hoogte van het risico en uiteraard eventuele oplossingen om de risico's voor zover dat nodig is te beperken.

2.4 Onderzoeksstrategie

Onder onderzoeksstrategie verstaat [VER01]: "een geheel van met elkaar samenhangende beslissingen over de wijze waarop het onderzoek moet worden uitgevoerd. Bij deze uitvoering wordt voornamelijk gedoeld op het vergaren van relevant materiaal en de verwerking van dit materiaal tot antwoorden op de vragen uit de vraagstelling".

De strategie dat voor dit onderzoek wordt gebruikt is die van bureauonderzoek. Bij dit type onderzoek speelt zich hoofdzakelijk af achter het bureau, bibliotheek en/of archieven. Dit type onderzoek wordt ook wel getypeerd als literatuuronderzoek waarbij gebruik wordt gemaakt van door andere geproduceerde kennis vastgelegd in vakliteratuur. Het literatuuronderzoek zal voornamelijk plaats vinden bij beantwoorden van deelvraag 1. Voor deelvraag 2 zal een casestudy uitgevoerd worden om mogelijke attacks en hun risico's te achterhalen waarna beoordeling en aanbevelingen worden gegeven.

"Transmurale zorg impliceert shared care en shared care vereist shared patient data."

ZonMw

3. Naar een Elektronisch Patiëntendossier

3.1 Inleiding

Zorginstellingen zien al jaren het aantal patiënten toenemen. Zonder daarbij de kwaliteit uit het oog te verliezen wordt er meer flexibiliteit verwacht en dient men dit te realiseren met dezelfde bezetting. De zorgverleners zullen door deze ontwikkeling steeds intensievere prestaties moeten leveren waarbij de beschikbare tijd voor een patiënt feitelijk zal afnemen. Daartegenover staat dat de eisen die de patiënt stelt stijgen door zijn mondigheid [HAN05]. En andere partijen als de verzekeraar graag op de hoogte willen zijn van eventuele consequenties. Tel daarbij de regelgeving en de versnipperde informatievoorziening op en men kan concluderen dat men de controle dreigt te verliezen. Met als uiteindelijke gevolg: groeiende wachtlijsten, stijgende administratieve lasten, miscommunicatie- en interpretatie, dubbele dossiers en uiteindelijk dus ook medische missers die men misschien wel had kunnen voorkomen.

Dat medische missers moet worden voorkomen is ook door de Inspectie voor de Volksgezondheid (IGZ) onderstreept. Zij sloten een onderzoek af waaruit bleek dat de communicatie tussen medisch personeel in ziekenhuizen niet goed is. Deze miscommunicatie zou elke week leiden tot een medische misser op de operatietafel. Als hoofdoorzaken ligt volgens [DEG07] de volgende punten hieraan ten grondslag:

- Diverse informatiebronnen die per ziekenhuis van naam verschillen en voor medische behandelaars niet altijd direct voor handen zijn,
- Het ontbreken van regie en overzicht doordat iedereen zijn eigen discipline centraal stelt,
- Het ontbreken van een centraal dossier die onder een arts valt die de patiënt onder handen krijgt,
- Het niet delen van patiëntgegevens met andere zorgverleners alsmede het niet opnemen van relevante gegevens in het dossier,
- De patiëntgegevens niet zijn te vinden waar men ze verwacht.

Met de realisatie van het EPD kan men de communicatie, structuur, onoverzichtelijkheid en betrouwbaarheid kunnen verbeteren en de kans op medische missers door slechte communicatie verlagen. Om dat te kunnen realiseren is er wel infrastructuur nodig dat het ook mogelijk maakt om miscommunicatie onmogelijk te maken.

In dit hoofdstuk zal nader worden ingegaan op het principe van een EPD, de wijze waarop toekomstige communicatie zal kunnen plaatsvinden en welke gevolgen dit heeft voor de bestaande basisinfrastructuur.

3.2 Doelen van het EPD

“Een EPD biedt alle relevante patiëntinformatie, 24 uur per dag, vanaf elke werkplek” [SMI03]. Met een dergelijk dossier zal men trachten een veilige omgeving te creëren waarmee relevante patiëntgegevens, opgeslagen bij systemen van diverse zorgverleners, kunnen worden opgehaald, uitgewisseld en getoond aan bevoegde zorgverleners ter ondersteuning van het zorgproces.
Met het EPD wenst men een aantal doelen te realiseren waaraan voldoen moet worden. Volgens [SPA05] zijn dat de volgende doelen:

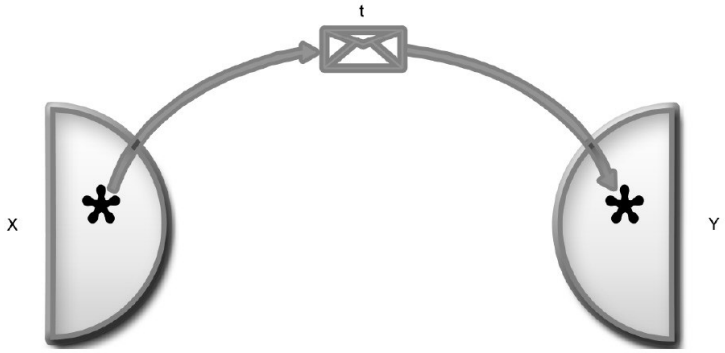
- **Centralisatie**; zorgen dat de deelinformatie die her en der over een patiënt beschikbaar is, verzameld wordt en vanaf elke plek in Nederland, zo nodig voor meerdere medici tegelijkertijd, toegankelijk is,
- **Efficiëntie**; papieren rompslomp vermijden (zoals het heen en weer sturen van verwijsbrieven, onderzoeksresultaten, deeldossiers, recepten en declaraties) en voorkomen dat onderzoeken dubbel worden uitgevoerd,
- **Foutreductie**; de kans verkleinen op een verkeerde diagnose of behandeling, door vast te leggen wat een patiënt mankeert of gebruikt,
- **Kwaliteitsverbetering**; door diagnoses en behandelingen gestructureerd vast te leggen kan beter worden beoordeeld wat het effect is van een bepaalde behandelwijze. Daarnaast kan de informatie uit geaggregeerde (en geanonimiseerde) EPD’s nuttig zijn voor management, planning en budgetbewaking, en tevens voor wetenschappelijk onderzoek,
- **Kostenbesparing**; minder papierwerk, vermijden van doublures in onderzoek, minder medische missers zoals medicatiefouten, eenvoudiger voorschrijven van gelijkwaardige maar goedkopere middelen, voorkomen van fraude, voorkomen dat patiënten gaan shoppen.

Volgens ICT-leverancier UZORG kleven er ook een aantal nadelen aan deze doelen. Zo stellen zij dat er fouten gemaakt worden bij de invoer van gegevens, de interpretatie van gegevens voor grote problemen gaat zorgen omdat iedereen gegevens anders beschrijft en verwoordt, er tijd verloren gaat bij het invoeren en opzoeken van gegevens, de kosten voor ICT aanzienlijk zullen stijgen en er dus geld dat normaliter voor de zorg bedoeld was nu geïnvesteerd moet worden in ICT en er minder samengewerkt zal worden tussen zorgverleners maar meer tussen zorgverleners en computer [UZO05].

Alvorens men ook daadwerkelijk van het EPD gebruik kan maken, zal de communicatie en het uitwisselen van informatie, zoals men die gewend is, moeten aanpassen. De volgende sectie gaat nader in op deze wijziging.

3.3 Van traditionele naar elektronische communicatie

De nieuwe basisinfrastructuur zal een impact hebben op de wijze van werken en communiceren in de zorg zoals wij die nu kennen. Het voornaamste doel is om communicatie en de uitwisseling van patiëntinformatie sneller te laten verlopen dan nu het geval is. Op dit moment kan de communicatie tussen zorgverleners als volgt worden weergegeven:

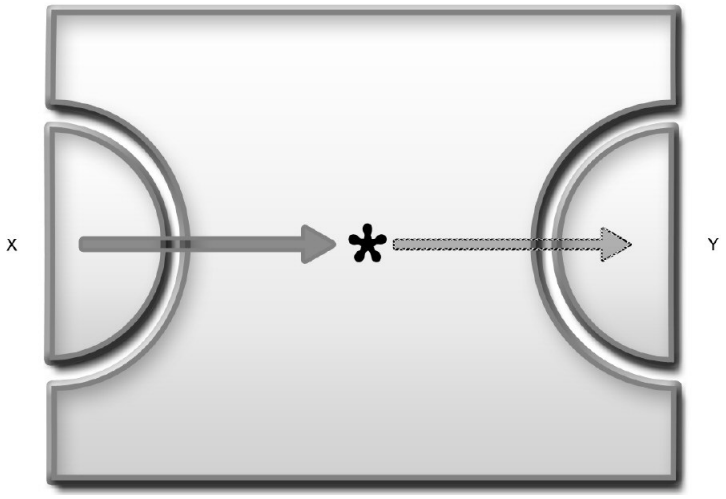


Figuur 3.1: Traditionele communicatie [ZON02]

Zorgverlener X schrijft een bericht naar zorgverlener Y om deze op de hoogte te stellen van een aantal bevindingen ten aanzien van een patiënt Z (figuur 3.1). De communicatie verloopt veelal via normale brievenpost wat als nadeel heeft dat deze vorm van communicatie de traagheid en de duplicatie van gegevens in de hand werken.

De traagheid zit in het feit dat wanneer zorgverlener X een bericht heeft samengesteld en deze doorstuurt naar zorgverlener Y, Y op dat bericht moet wachten (push-techniek). Er treedt vertraging op tussen het moment van verzenden en ontvangen. Dit vanwege de afhankelijkheid van derden om de informatie af te leveren. Tevens ontstaat er duplicatie van de patiëntinformatie vanwege het feit dat deze zich nu ook bij zorgverlener Y bevind. Vanwege de statische vorm is synchronisatie niet mogelijk. Waardoor de informatie niet meer door de rechthebbende zorgverlener is te beschermen en dus de privacy niet meer is te waarborgen.

Door invoering van elektronische communicatie is de afhankelijkheid van derden aanzienlijk verminderd maar blijft redundantie bestaan. Immers, ontstaan er twee asynchrone patiëntendossiers doordat de informatie als kopie van het origineel wordt verzonden naar de ontvangende zorgverlener.



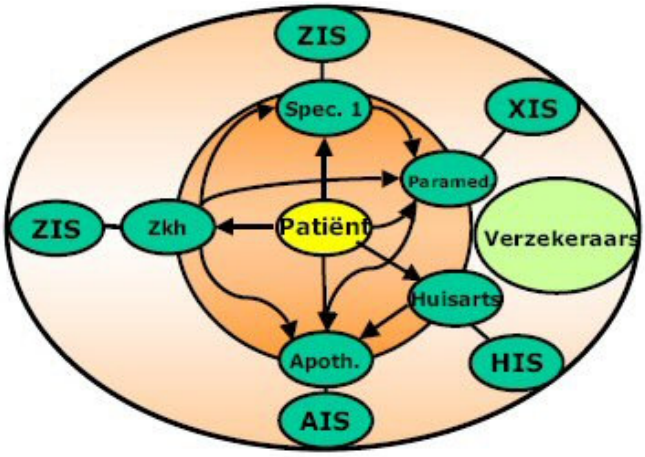
Figuur 3.2: Virtuele communicatie via EPD [ZON02]

Door het patiëntendossier virtueel beschikbaar te maken door zorgverlener X aan zorgverlener Y (figuur 3.2), kan zorgverlener Y op basis van zijn autorisatierechten de actuele patiëntgegevens opvragen en ontvangen (pull-techniek). Hoewel de zorgverlener over de meest actuele gegevens beschikt blijft er een risico bestaan dat er dubbele dossiers ontstaan waarover de verantwoordelijke zorgverlener geen controle heeft. UZORG heeft dit opgelost door dossiers via webapplicatie beschikbaar te maken en de gegevens niet te downloaden naar de lokale computer. Er ontstaat zodoende een virtueel patiëntendossier waarbij redundantie is uitgesloten.

Het grote voordeel van de pull techniek is dat zorgverleners op ieder willekeurig tijdstip informatie kunnen inzien die voor de behandeling van hun patiënt op dat moment noodzakelijk is. Het delen en direct beschikbaar hebben van patiëntgegevens waar dan ook zal uiteindelijk ten goede komen aan een betere zorg voor de patiënt.

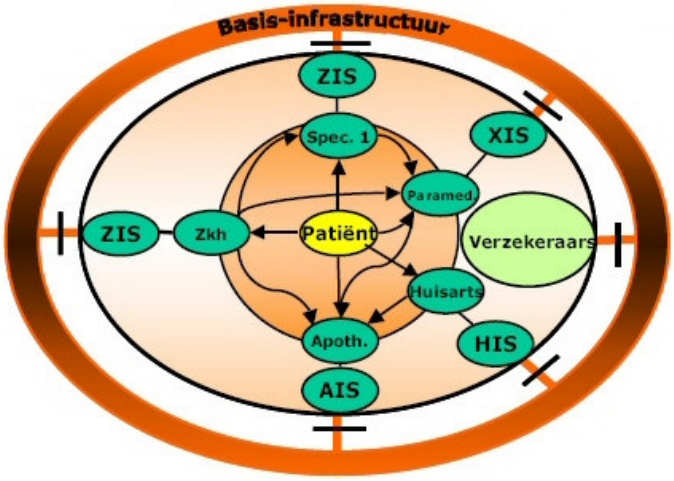
3.4 Basisinfrastructuur

Een nieuwe ontwikkeling zal ook zijn impact hebben op de huidige situatie met betrekking tot huishouding rondom de patiëntinformatie. Deze huishouding kan worden weergegeven als in onderstaande afbeelding (figuur 3.3). Hieruit is op te maken dat de patiënt centraal staat in de zorgketen en tijdens de zorg relaties heeft met diverse zorgverleners die gegevens over hem opslaan in hun informatiesystemen. Elke zorgverlener heeft zijn eigen informatiesysteem. Zo heeft het ziekenhuis een Ziekenhuis Informatie Systeem (ZIS), een huisarts een HIS (Huisarts Informatie Systeem) en een apotheker een AIS (Apotheek Informatie Systeem).



Figuur 3.3: Huidige situatie zorginhoudelijke patiëntinformatie [NIC05a]

De huidige infrastructuur is niet voor digitale informatie-uitwisseling is bedoeld. De systemen kwamen eigenlijk ter ondersteuning van de dossiers op locatie en waren een eerste maar voorzichtige stap richting digitalisering. Bevraging door andere externe systemen vanwege het ontbreken van de koppelingen met deze systemen is hierdoor niet mogelijk.



Figuur 3.4: Gewenste situatie zorginhoudelijke patiëntinformatie [NIC05a]

Door deze koppeling wel tussen de verschillende zorgsystemen te leggen en ze middels het gestandaardiseerde HL7v3-protocol met elkaar te laten communiceren, ontstaat er een voorziening die over de organisatiegrenzen heen reikt en alle aangesloten systemen met elkaar verbindt (figuur 3.4).

Deze technologische schil tracht te voorzien in een veilige en betrouwbare communicatie tussen de verschillende zorgsystemen, onafhankelijk van tijd en plaats. Gebruik van deze basisinfrastructuur stelt wel hoge eisen aan de aangesloten systemen. Het systeem zal zowel betrouwbaar als vertrouwelijk moeten zijn waarbij gebruikers via identificatie, authenticatie en autorisatie veilig gegevens kunnen opvragen die ook past bij de functie. Het aspect veilige uitwisseling en opslag van gegevens tussen verschillende zorginstanties en systemen dient nauwgezet in de gaten te worden gehouden maar brengt grote voordelen.

3.5 Toekomstige toepassingen

ICT in de zorg heeft in de toekomst als uitgangspunt het creëren van maximale kwaliteit en efficiency in de zorg. Binnen deze visie is een centrale rol voor het EPD weggelegd. Hierbij zal het mogelijk moeten worden dat, in principe, alle gegevens van een patiënt voor alle zorgapplicaties op een standaardwijze toegankelijk worden gemaakt. Wanneer het EPD succesvol is geïmplementeerd en opgenomen in de zorginfrastructuur zal in fasen de basisinfrastructuur uitgebreid worden met nieuwe mogelijkheden. Zo zijn er plannen voor de realisatie van: telemedicine, kennismanagement, behandeling op afstand en het online toegang verlenen van mensen in hun persoonlijke patiëntendossier.

3.6 Conclusie

De zorg is continue onderhevig aan nieuwe ontwikkelingen waardoor verwachtingen alleen maar stijgen. Vast staat dat het EPD de manier van communiceren in de zorg zal veranderen. Hoewel de plannen veelbelovend zijn en feitelijk niet meer dan een logisch gevolg van de digitalisering van de maatschappij, zal dit niet direct resulteren in een betere zorg. Voorstanders zeggen dat er minder fouten zullen voorkomen in de diagnoses door de komst van het EPD. Men kan zich ook afvragen hoeveel fouten er optreden welke te wijten zijn aan het gebruik van het informatiesysteem. Het gebruik van het EPD zorgt voor minder fouten, maar kan ook weer nieuwe fouten opwerpen. Immers, een nieuw systeem brengt nieuwe fouten en problemen met zich mee. En ook deze kunnen uiteindelijk tot ernstige gevolgen leiden.

Het EPD rijst uit de diverse bronnen op als de heilige graal voor het managen van de zorg. Het zou de zorg transparanter en efficiënter maken, kosten en activiteiten in de zorg transparant, beheersbaar en planbaar maken en daarnaast foutreductie, kostenbesparing, fraudebestrijding marktwerking en bevolkingsonderzoek een cruciale duw in de goede richting geven, somt [SPA05] op. Het zijn bijna allemaal woorden die al vaker een voorbode waren van verslechtering voor mensen in een zwakke positie. Profijt van het EPD heeft men pas wanneer een dossier daadwerkelijk alle essentiële gegevens bevat, de vele losse informatiebronnen niet meer voorkomen, kennis over een patiënt ook gedeeld wordt en men kan begrijpen wat de andere zorgverlener doet en waar hij de gegevens heeft opgeslagen. Daarnaast kan men de garantie dat de medische gegevens kloppen vergroten wanneer de patiënt zelf kan controleren of zijn dossier klopt met de werkelijkheid. Desondanks blijft het risico bestaan dat men op basis van gegevens in het dossier een inschattingsfout maakt. Het EPD is daarvoor slechts een deeloplossing om dit risico te verkleinen.

Feit is dat door gebruik van digitale patiëntinformatie de kans stijgt dat kwaadwillenden gegevens in handen krijgen en vervolgens misbruik maken van deze gegevens door op onrechtmatige wijze verkregen toegang tot het LSP. Om toegang te beschermen tegen kwaadwillenden is het noodzakelijk om informatiebeveiliging te implementeren in het zorgsysteem alsmede de organisatie.

"The opposite of security is insecurity,
and the only way to overcome insecurity is to take risks."
Theodore Forstmann

4. Informatiebeveiliging

4.1 Inleiding

Om te zorgen dat gegevens alleen door bevoegde personen kunnen worden opgevraagd of privacy van personen te beschermen is beveiliging van informatie noodzakelijk. Daarnaast zorgen de huidige technologische ontwikkelingen ervoor dat er steeds meer informatie digitaal wordt bewaard. Voor patiëntinformatie zoals die in de zorg wordt gebruikt is zelfs dermate privacygevoelig dat deze te allen tijde voorhanden moet zijn (beschikbaarheid), vrij dient te zijn van fouten en ongewenste wijzigingen (integriteit) en uit handen moet blijven van onbevoegde personen (vertrouwelijkheid). Het beveiligen van deze informatie is dus absolute noodzakelijk.

Dit hoofdstuk beschrijft wat informatiebeveiliging is, waarom het noodzakelijk is, op welke wijze het kan worden gemeten en hoe belangrijk informatiebeveiliging voor de gezondheidszorg is.

4.2 Definitie

De term informatiebeveiliging wordt op vele manieren gebruikt. Ook in de literatuur heeft men vele definities voorhanden, waarbij de een de nadruk legt op de beveiliging van een systeem, en een ander vindt dat beveiliging van een systeem al deel uit dient te maken vanaf de ontwerpfase van het systeem.

Voor dit onderzoek wordt gebruik gemaakt van een brede definitie. Volgens [MCD94] is information security te definiëren als: "the concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use".

Deze definitie geeft aan dat er meer is dan het beveiligen van de toegang. Het geeft een handvat naar de hulpmiddelen die er zijn voor informatiebeveiliging. Zo zijn er technische als administratieve maatregelen die samen zorg kunnen dragen voor een veilig en betrouwbaar systeem. Men moet in acht nemen dat de mate van information security moet worden afgewogen tegen de mate van beveiliging. "De beveiliging is daarom situatie afhankelijk waarbij het nooit geheel mogelijk is een systeem te bouwen dat gegarandeerd veilig is" [SCH00].

4.3 Waarom informatiebeveiliging

De afhankelijkheid van de computer wordt voor ons steeds groter. Waren we eerst vooral bedrijfsmatig afhankelijk, nu treedt de computer ook steeds meer ons dagelijks leven binnen. En die ontembare honger naar informatie, heet van de naald, groeit nog steeds.
Wat doen we als die afhankelijkheid zo groot is, dat het een onmisbare informatiebron is waarvan we vrijwel geheel afhankelijk worden? Dat er een bedreiging succesvol wordt uitgevoerd en de informatiebron op zijn kop weet te zetten?

In feite is het bovenstaande waarom informatiebeveiliging zo belangrijk is. Immers, kwaadwillende personen hebben genoeg mogelijkheden voor handen om bij anderen, om welke reden dan ook, schade aan te richten. Voorop staat dat door het internet en de beschikbaarheid van vele bronnen om bedreigingen succesvol uit te kunnen voeren. Met als gevolg dat informatie wordt afgeluisterd, gewijzigd, verwijderd of bijvoorbeeld als chantage middel wordt ingezet. Deze dreiging kan zowel extern als intern door eigen mensen uit de organisatie worden uitgevoerd. Deze vorm van directe schade kan een verstoring opleveren in de informatiebronnen, waarbij schade onder andere bestaat uit het niet correct kunnen uitvoeren van de nodige taken door medewerkers, schade zelf weer moet worden hersteld evenals de nodige inspanningen vergt om maatregelen te treffen dat dergelijke dreigingen niet meer werkelijkheid worden.
Daarnaast is er ook indirecte schade. Immers, het imago loopt een deuk op, klanten lopen vanwege onbetrouwbaarheid weg waardoor marktaandeel wegslinkt. En allemaal vanwege het niet op orde hebben van de informatiebeveiliging.

4.4 Voorkomen van schade

Met informatiebeveiliging in de hand is er nog geen garantie op een 100 % waterdicht systeem. Kosten rijzen dan de pan uit, en dat terwijl zelfs dan is de beveiliging nog niet is te garanderen. Verschillende factoren liggen hier aan ten grondslag, maar veelal blijkt toch de mens de zwakste schakel in de beveiliging te zijn. Voorbeeld hiervan is dat medewerkers in een organisatie kwaadwillende bedoelingen kunnen hebben, bewust essentiële informatie laten verdwijnen of met opzet de verleiding niet kunnen weerstaan de beveiliging te omzeilen.

In alle gevallen dient informatiebeveiliging er voor om eventuele schade te voorkomen, maar ook om schade te beperken wanneer onverhoopt er toch iets mis is gegaan. Het voorkomen van schade kan door gericht detectie in te schakelen die voortijdig waarneemt dat er een mogelijke dreiging op handen is die een risico kan zijn voor het systeem. Door deze detectie wordt het effect van de dreiging te niet gedaan en ontzenuwt.

Dat nooit alle dreigingen zijn te weren is ook niet het uitgangspunt van informatiebeveiliging. Dat is namelijk het bepalen welke dreigingen essentieel zijn om bijvoorbeeld de bedrijfsvoering correct uit te voeren. Door kritische processen en de kans dat er een dreiging kan ontstaan in te schatten, wordt

duidelijk welke processen in aanmerking komen om te worden aangepakt en in welke mate. Aan de hand van eventuele financiële consequenties is uiteindelijk te bepalen welke risico's men wel wil lopen en welke maatregelen er wel moeten worden genomen. Informatiebeveiliging draait om een beeld te krijgen van de beveiligingsituatie en het ontdekken van eventuele zwakke plekken.

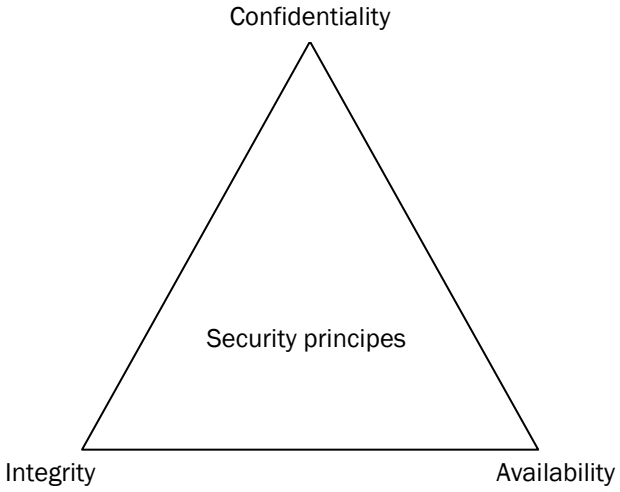
4.5 Kernbegrippen

Informatiebeveiliging is het beveiligen van informatie tegen ongewenste toegang, ongewenste wijziging van informatie (door mensen), ongewenste aantasting (bijvoorbeeld fysiek geweld of brand) en garanties voor de beschikbaarheid.

Informatiebeveiliging in de zorg wordt vertaald als het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om patiënten verantwoorde zorg te kunnen bieden.

De drie kernbegrippen die het doel van Informatiebeveiliging volgens de definitie van [MCD94] definiëren zijn, Confidentiality, Integrity, Availability. Deze attributen vormen samen de CIA drie-eenheid oftewel de CIA-triad (figuur 4.1). De CIA-triad kan vertaald worden naar een allesomvattende definitie: "the right information to the right people at the right time" [MAR86]. Deze definitie, welke is vastgelegd in het [NNI97], beschrijft de CIA-triad als een methode voor het indelen van automatiseringssystemen in de zorgsector in risicocategorieën.

De CIA-triad is een veel toegepaste methode gedurende een risicoanalyse van een informatiesysteem. Met behulp van deze driehoek kan het gewenste niveau van de beveiliging voor een nader te bepalen aspect worden geschat. De CIA-triad helpt, gedurende de risicoanalyse, bij het classificeren van het beveiligingsniveau waardoor op basis van de score maatregelen in het systeem kunnen worden geïmplementeerd.



Figuur 4.1: De "CIA-triad"

4.5.1 Confidentiality

Vertrouwelijkheid is door het International Organization for Standardization (ISO) als volgt gedefinieerd: “ensuring that information is accessible only to those authorized to have access" [WEBAVE].
Vertrouwelijkheid is een kwaliteitskenmerk van gegevens. Met vertrouwelijkheid wordt bedoeld dat een gegeven alleen te benaderen is door iemand die hiervoor gerechtigd is. De eigenaar van de informatie bepaald wie rechten krijgt om de gegevens te benaderen. De vertrouwelijkheidfunctie zorgt er ook voor dat de verzender van informatie de garantie heeft dat de verzonden gegevens door niemand anders kan worden gelezen of gewijzigd. De ontvanger van de betreffende informatie heeft daarbij de garantie dat de informatie afkomstig is van degene die zegt deze verzonden te hebben.

Overeenkomstig met de Wet Bescherming Persoonsgegevens (WBP) en Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) is de zorgverlener in eerste instantie verantwoordelijk voor het waarborgen van de vertrouwelijkheid en de bescherming van de persoonsgegevens (of patiëntgegevens). In de normale wereld wordt het beschermen van patiëntgegevens geregeld doordat artsen de eed van Hippocrates hebben afgelegd. Hiermee beloven zij de patiënteninformatie waarover zij als arts beschikken te zullen respecteren en beschermen. In de digitale wereld zal dit moeten worden geregeld door rechten toe te kennen aan de gebruikers.

Er zijn diverse manieren mogelijk om vertrouwelijkheid in een informatiesysteem te implementeren. Dit kan door gebruik te maken van bijvoorbeeld cryptografie en autorisatie.

4.5.2 Integrity

Volgens de [NCS87] zorgt het kernbegrip integriteit er voor dat data op een systeem hetzelfde is als die van de bron. Deze data mag niet worden blootgesteld aan kwaadwillige wijziging of vernietiging. Door integrity kan informatie alleen door een geautoriseerde partij worden gewijzigd of verwijderd. Dit punt is vooral van groot belang binnen het zorgsysteem. Integriteit binnen de basisinfrastructuur kan men op verschillende wijze waarborgen. Een daarvan is door het identificeren van een bevoegde gebruiker met behulp van de UZI-pas en het daaraan gekoppelde autorisatieprofiel.

Ook is integriteit een kwaliteitskenmerk van gegevens in het kader van de informatiebeveiliging. Het staat synoniem voor betrouwbaarheid. Een betrouwbaar gegeven gegarandeerd dat deze;

- **Juist is**; rechtmatigheid is hier een kernbegrip,
- **Volledig is**; niet te veel en niet te weinig,
- **Tijdig is**; op tijd,
- **Geautoriseerd is**; gemuteerd door een persoon die gerechtigd is de mutatie aan te brengen.

Opgemerkt moet worden dat het begrip integriteit in de informatiebeveiliging kan worden opgesplitst in twee smaken en de integriteit pas is gewaarborgd wanneer beide zijn te vertrouwen;

- **Betrouwbaarheid van de bron**; wat inhoud dat de verzender van de betreffende informatie is, wie hij zegt dat hij is.
- **Betrouwbaarheid van de data**; data integriteit houdt in dat de data de ontvanger bereikt zonder dat de informatie vanaf het moment van verzenden is gewijzigd.

4.5.3 Availability

Het kernbegrip beschikbaarheid is volgens [MCC05]: “ensuring timely and reliable access to and use of information”. Doel van availability is dat systemen, de infrastructuur en informatiesystemen altijd beschikbaar moeten zijn en dat er alles aan gedaan is dit mogelijk te maken en niet beschikbaar hebben ervan zoveel mogelijk wordt uitgesloten. De beschikbaarheid van het zorgsysteem met de patiëntgegevens zijn van cruciaal belang voor het goed kunnen behandelen van patiënten. De beschikbaarheid wordt veelal vastgelegd in Service Level Agreements (SLA’s) waarin procedures zijn vastgelegd om deze beschikbaarheid te kunnen garanderen.

Het NICTIZ heeft deels ingezien dat availability belangrijk is voor de continuïteit van informatievoorziening. Het LSP wordt daarom in triple vorm uitgevoerd. Een echte LSP, een test LSP en een backup LSP. Echter is dit geen garantie dat het LSP bij grote calamiteiten bereikbaar blijft zonder dat men hiervan de gevolgen ondervindt.

Op basis van de bevinding die men door middel van het toekennen van scores aan de verschillende CIA onderdelen, kan men bepalen welke onderdelen extra aandacht nodig hebben. In hoofdstuk 8 zal de CIA-triad worden gebruikt bij het classificeren van geïdentificeerde dreiging. Hiermee wordt een beeld verkregen op welke gebieden een dreiging juist kwaad zou kunnen doen en op welke gebieden deze geen of betrekkelijk weinig invloed heeft.

4.6 Informatiebeveiliging in de zorg

De zorgsector leunt sterk op de kwaliteit van haar dienstverlening. Typerend voor de zorg is dat de kwaliteit van deze dienstverlening van levensbelang is voor de patiënt alsmede de betrouwbaarheid van de zorgsector. Om patiënten het gewenste niveau van dienstverlening te kunnen bieden, is het noodzakelijk dat zorgverleners op ieder moment over betrouwbare informatie kunnen beschikken. Tegelijkertijd is het van belang dat gevoelige informatie niet in handen van ongeautoriseerde partijen valt om de privacy van de patiënt te beschermen. Om hieraan te kunnen voldoen is er een, nog niet verplichte, norm voor informatiebeveiliging in de zorg opgesteld, de NEN 7510 [NEN04].

De gangbare definitie voor informatiebeveiliging in de zorg is: “het beveiligen van informatie tegen ongewenste toegang, ongewenste wijziging van informatie (door mensen), ongewenste aantasting (door fysiek geweld of door brand) en garanties voor de beschikbaarheid. Informatiebeveiliging heeft tot doel om

de kwaliteit van de informatie te waarborgen" [NEN04]. Hierbij staat de kwaliteit van medische informatie voor de integriteit (juistheid van gegevens), beschikbaarheid, vertrouwelijkheid en accountability.

Door beveiligingsmaatregelen in het zorgsysteem te implementeren wordt getracht de informatie betrouwbaar te houden en het verspreiden naar onbevoegde personen of systemen tegen te gaan. Echter, de complexiteit van informatiebeveiliging in de zorgsector maakt dit een lastig onderdeel en heeft daarom de behoefte aan een zorgstandaard op het gebied van gegevensopslag, berichtenopmaak, communicatieprotocollen, definities, medische termen en informatiebeveiliging. De NEN 7510 is een norm speciaal voor de zorg opgezet en uitgebreid voor specifieke zorginstellingen met de NEN 7511 [NEN04] en NEN 7512 [NEN04] norm. Deze norm bevat richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die een organisatie in de gezondheidszorg minimaal dient te nemen ter beveiliging van haar systeem en informatie. De NEN normen zijn nog niet verplicht maar een reden om deze niet op te volgen betekend straks gegarandeerd uitsluiting van het LSP.

De NEN 7510 norm geeft een leidraad voor het organisatorisch en technisch inrichten van informatiebeveiliging en biedt een basis voor vertrouwen in de zorgvuldige informatievoorziening tussen zorginstellingen. De NEN 7512 norm daarentegen is in twee opzichten een aanvulling op de NEN 7510. In de eerste plaats richt deze zich op de zekerheid die partijen elkaar moeten bieden als voorwaarde voor vertrouwde gegevensuitwisseling. Ten tweede levert deze norm een invulling voor een aantal van de richtlijnen van NEN 7510. Het betreft voornamelijk de aanzet tot het uitvoeren van een risicoanalyse en het opstellen van risicoclassificatie en de uitwerking van de eisen over identificatie en authenticatie die bij een bepaalde risicoklasse horen.

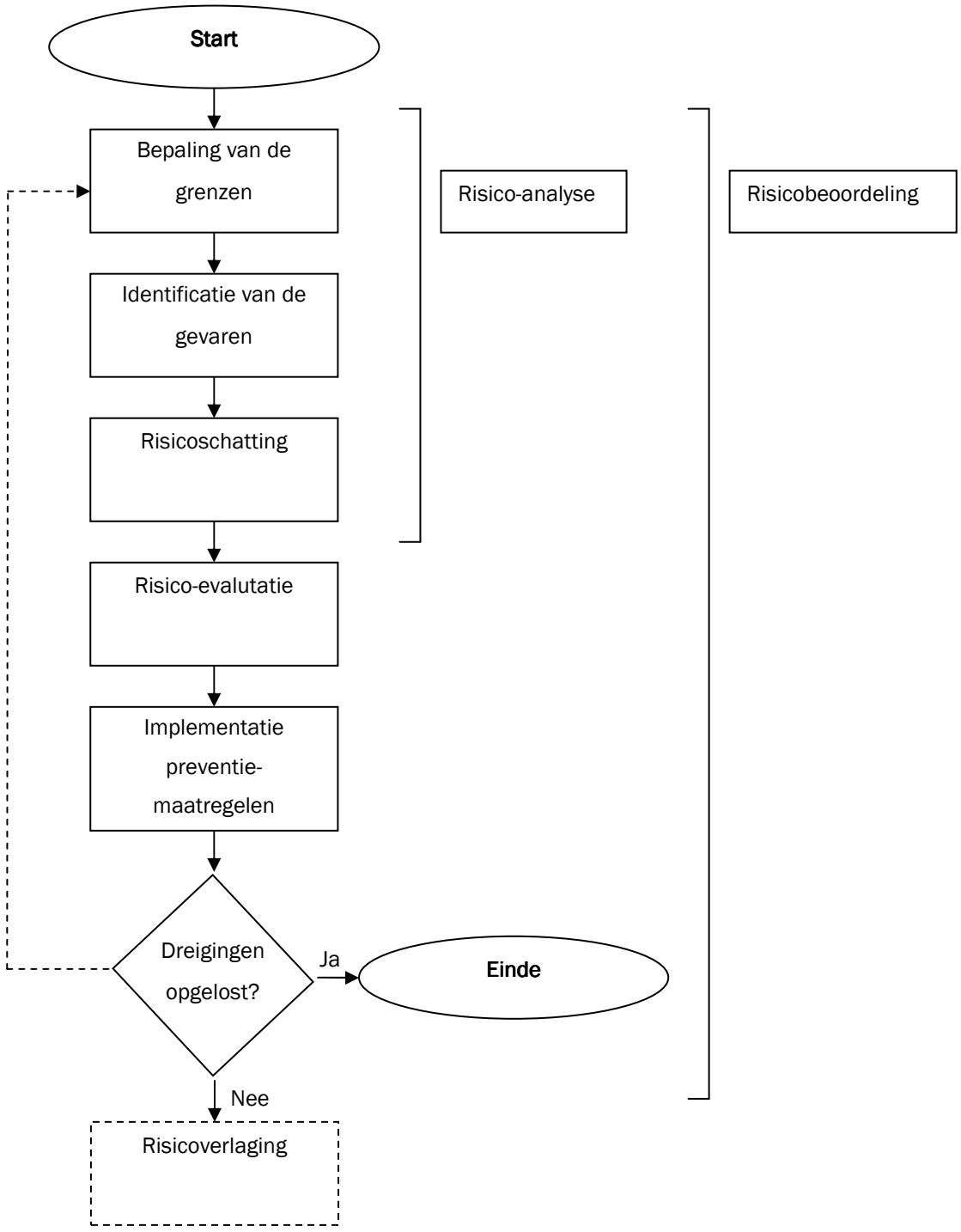
4.7 Risicoanalyse

4.7.1 Wat is een risicoanalyse

Een risicoanalyse draagt er aan bij dat op voorhand bekend is welke risico's er zijn en in hoeverre deze, in dit geval, een bedreiging vormen voor het LSP. Volgens het [NEN97] is een risico een combinatie van de omvang van de mogelijke schade en de kans dat de schade optreedt. Ook het LSP zal te maken krijgen met bedreigingen die risico's en dus schade zouden kunnen veroorzaken. Door het uitvoeren van een risicoanalyse wordt inzicht verkregen in eventuele dreigingen en daaruit voortvloeiende risico's.

De in dit onderzoek gebruikte risicoanalyse wordt in Figuur 4.2 weergegeven. Kenmerkend is dat de activiteiten elkaar opvolgen en uiteindelijk zullen resulteren in het wegnemen of verlagen van risico's als gevolg van mogelijkheden van kwaadwillenden om op onrechtmatige wijze toegang tot het LSP te krijgen. Dit is dan ook tevens de scope van het te onderzoeken onderdeel, dit om te voorkomen dat onduidelijk is wat er wordt onderzocht. Een risicoanalyse vormt de uiteindelijke basis voor het beschrijven van de huidige beveiligingsstatus van het systeem [PFL03], en is daarom onmisbaar bij het vormen van een beeld over mogelijke risico's.

Opgemerkt moet worden is dat een risicoanalyse een momentopname is en op een later moment de een andere score kan hebben. Door het risicoanalyseproces periodiek plaats te laten vinden worden veranderingen meegenomen en opnieuw gewogen. Volgens dit iteratieve proces van risicobeoordeling blijven organisaties zicht houden op risico's die mogelijkerwijs een bedreiging kunnen zijn en hier gepaste maatregelen voor treffen om de risico's te beperken.



Figuur 4.2: Het iteratieve risicoverlagingsproces (gebaseerd op [NEN97])

4.7.2 Risico bepaling

Om te bepalen hoe hoog het risico is, is het gebruikelijk om risico's kwantificeerbaar te maken .

RISICO	=	OMVANG	(X)	KANS
				frequentie en duur van de blootstelling
gerelateerd aan het beschouwde gevaar		van mogelijke schade door het beschouwde gevaar		kans dat de gevaarlijke gebeurtenis optreedt
				mogelijkheid om de schade te vermijden of te beperken

Figuur 4.3: Kwantificeerbare risicoformule [OVE99]

Een risico bestaat uit de schadeverwachting en de kans dat deze plaats vindt (figuur 4.3).

4.8 Attack trees

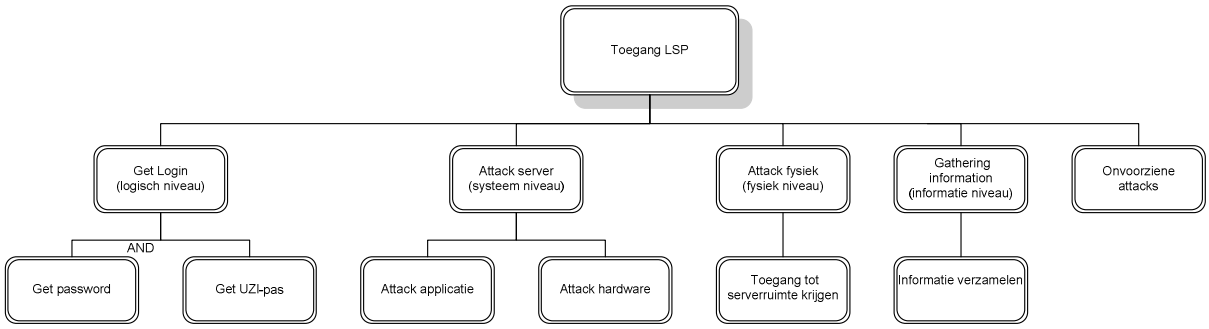
4.8.1 Wat zijn attack trees?

Voordat risico's kunnen worden gekwantificeerd en er daadwerkelijk maatregelen genomen kunnen worden, is het noodzakelijk te weten welke dreigingen er zijn. Voor het identificeren hiervan heeft [SCH00] een methode ontwikkeld waarmee, vanuit de ogen van een kwaadwillende, bedreigingen op het systeem middels een boomstructuur in kaart worden gebracht, de attack trees. Deze methode zal in dit onderzoek worden gebruikt om een gestructureerd overzicht te geven van mogelijke dreigingen op het LSP.

Een attack tree heeft als doel de mogelijke aanvallen op een systeem schematisch in kaart te brengen [MAU05]. Deze kan in figuur 4.2 geplaatst worden onder de activiteit "identificatie van gevaren". Een attack tree biedt de mogelijkheid om een goed beeld te krijgen van de mogelijkheden van de aanvaller [MAU06]. Een attack binnen de scope van informatiebeveiliging kan volgens [WEI05] gedefinieerd worden als: "een kwaadwillende activiteit dat gericht is tegen een computersysteem door onbevoegde toegang, teistering door een virus, het wijzigen of vernietigen van gegevens of door Denial of Service attacks".
Bij deze methode gaat men ervan uit dat de aanvaller een bepaald doel voor ogen heeft (de wortel van de boom) en dat deze op een aantal manieren bereikt kan worden (vertakkingen). Een dergelijke boom kan vanwege variabele attack mogelijkheden variëren van een enkele vertakking tot een boom met daarin vele aanvallen met allen het zelfde einddoel.

De kracht van attack trees is dat de boom, zie figuur 4.4, een formele relatie tussen verschillende aanvallen uitdrukt waarbij aanvallen in natuurlijke taal zijn beschreven en de mate van detaillering door de gebruiker zelf zijn aan te geven [MAU06]. Een Attack Tree kan ook zicht geven op risico's welke veel aandacht vragen en in aanmerking komen om opgelost te worden. Samen maakt dit een eenvoudig te gebruiken methode om mogelijke risicovolle attacks boven tafel te krijgen.

Het verkrijgen van een complete attack tree is een utopie vanwege de continu vernieuwende ontwikkelingen. Daardoor is het verstandig de attack trees bij te werken. Daarnaast is het van belang om te leren van organisaties die al eerder attack trees hebben opgesteld en daarbij risico's gevonden. Dit met als doel een zo compleet mogelijke attack tree te verkrijgen. Helaas, is verkrijgen van informatie afkomstig van andere organisaties veelal een probleem. Hoewel dit positieve invloed kan hebben op het niveau van beveiliging, blijft dit soort informatie veelal ontoegankelijk. Dit is te wijten aan het feit dat men deze kennis niet openbaar wenst te maken en daardoor negatieve publiciteit en de consequenties die daaraan zijn verbonden probeert te ontlopen [AND93]. Ondanks deze problematiek is een attack tree een goede en relatief eenvoudige methode om een helder beeld te verkrijgen van mogelijke attacks en de daaruit voortvloeiende dreigingen op het informatiesysteem zodat het informatiesysteem verbeterd kan worden.



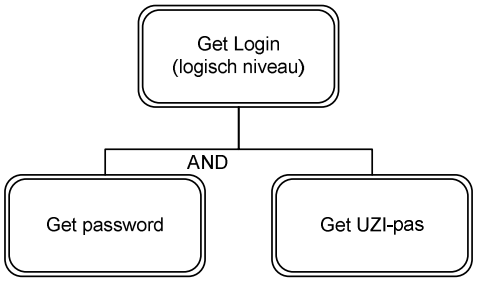
Figuur 4.4: Voorbeeld van een attack tree

4.8.2 Opbouw attack tree

Een attack tree is eenvoudig in het gebruik. Zowel het opstellen van een attack tree als het begrijpen ervan is makkelijk aan te leren. Een attack tree heeft uiteindelijk één hoofddoel, in geval van figuur 4.4, het toegang krijgen tot het LSP. Het eerste niveau daaronder laat een aantal attack-opties zien om het doel te bereiken. En elke daaronderliggende vertakking zijn subdoelen die al dan niet onafhankelijk van elkaar het bovenliggende doel haalbaar maken. Het is uiteindelijk aan de domeinspecialisten en riscoanalysten om de attacks en de onderliggende niveaus van het hoofddoel te achterhalen en in kaart te brengen.

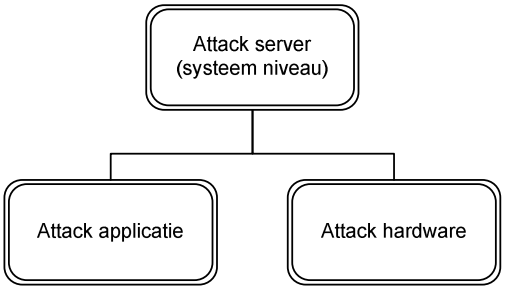
4.8.3 And en OR

Een attack tree kent twee soorten vertakkingen om het uiteindelijk bovenliggende doel te bereiken, namelijk de AND-tak en de OR-tak.



Figuur 4.5: Attack tree met een AND vertakking

De AND-tak (figuur 4.5) wordt gekenmerkt door het woord “and” dat onder het bovenliggende doel is weergegeven. Deze notatie houdt in dat aan alle onderliggende subdoelen moet worden voldaan om het bovenliggende doel te kunnen bereiken. Indien niet aan één van de AND-opdrachten kan worden voldaan, dan kan de betreffende attack niet succesvol uitgevoerd worden.



Figuur 4.6: Attack tree met een OR vertakking

Bij de OR-tak (figuur 4.6) zijn de subdoelen niet afhankelijk van elkaar. De OR geeft aan dat er een keuze gemaakt moet worden uit één van de onderliggende subdoelen om het bovenliggende hoofddoel te bereiken.

4.8.4 Attributen

Als de attack tree opgesteld is, kunnen attributen aan de attack tree worden toegevoegd. Deze attributen laten specifiek informatie zien waardoor de attack tree verrijkt wordt met extra informatie. Op basis van de gebruik van attributen kan bepaald worden welke realistische attacks zich eventueel zouden kunnen voordoen op het informatiesysteem. Afhankelijk daarvan kan men prioriteiten geven aan het risico en bepalen of maatregelen getroffen moet worden.

4.9 Conclusie

Informatiebeveiliging is essentieel bij het gebruik van systemen waarbij men onder andere privacy, veilige communicatie en veilige opslag van informatie van cruciale betekenis zijn. Het LSP en de daaraan ondergelegen infrastructuur is zeer gebaat bij een zorgvuldige en gegarandeerd veilige communicatie. Het is dan ook een van de prioriteiten om te zorgen dat het systeem onder (vrijwel) alle omstandigheden blijft functioneren en haar diensten aan de zorgverleners kan blijven afgeven.

Voordat deze garantie kan worden afgegeven is het noodzakelijk dat men middels een risicoanalyse het systeem doorlicht waar zich de risico’s bevinden, in welke mate deze schade kunnen aanrichten en wat de kans op schade is. Op basis hiervan krijgt men een beeld welke risico’s er zijn en in aanmerking komen om te worden aangepakt om zo de risico’s te verminderen of zelfs weg te nemen.

Met behulp van de CIA-triad, de risicofactor en de attack tree methoden worden in dit onderzoek dan ook gebruikt om de risico's in kaart te brengen. Met als uiteindelijke doel het systeem veiliger te maken en kwaadwillenden minder kans te geven het LSP op onrechtmatige wijze te betreden.

Echter, het moet duidelijk zijn dat het echter geen garantie biedt dat alle risico's worden weggenomen. Want alleen met technische oplossingen of maatregelen zijn niet genoeg. Wil men een effectief beleid voeren waardoor risico's vroeg worden geïdentificeerd en wanneer nodig worden weggenomen dan zal informatiebeveiliging ingebed dienen te worden in de organisatie.

In hoofdstuk 8, Risicoanalyse van het LSP, zal de in dit hoofdstuk besproken theorie worden toegepast en gebruikt om een beeld te geven van de risico's die zouden kunnen ontstaan. Om enigszins te kunnen bepalen welke risico's er zijn is inzicht in het LSP en een aantal processen noodzakelijk. De volgende hoofdstukken geven wat meer inzicht in het LSP.

"Medical data are only useful if shared."

Bruce Schneier

5. Hoe zit het LSP in elkaar

5.1 Inleiding

Het uiteindelijke doel om elektronische uitwisseling van patiëntinformatie mogelijk te maken is met de ondertekening van een intentieverklaring door de zorgsector in 2000 is besloten om zo snel mogelijk een landelijke ICT-infrastructuur te realiseren. Het NICTIZ is daarvoor in het leven geroepen en heeft de blauwdrukken voor het LSP en de infrastructuur opgeleverd.

In dit hoofdstuk zullen zowel de technische alsmede de organisatorische structuur van het LSP beschreven worden. Door beide gebieden te beschrijven wordt een algemeen beeld verkregen van het voorgestelde infrastructuur en de keuzes die het NICTIZ heeft gemaakt. Tevens worden twee belangrijke processen binnen de het uitwisselen van patiëntinformatie beschreven.

5.2 Basisinfrastructuur op technisch gebied

5.2.1 Voorlopers NICTIZ specificatie

De specificatie zoals het NICTIZ deze heeft opgeleverd, zijn onder andere gebaseerd op resultaten uit kleinschaligere maar soort gelijke projecten. Twee van deze projecten, met een verschillend resultaat, zijn hieronder uitgewerkt.

Project Eemland

Een project dat medio 2001 in de regio Eemland is uitgevoerd en door [SPA05] beschreven als een kansloos project. Gedurende dit project heeft men getracht een systeem te bouwen waarmee computers en applicaties van alle zorgaanbieders en zorgverzekeraars via een veilige infrastructuur met elkaar in verbinding staan. Via een centraal ingerichte server, met daarop de verzekeringsgegevens van patiënten binnen de proefregio, hadden zorgaanbieders, zorgverzekeraars en patiënten toegang tot de centraal opgeslagen patiënt- en verzekeringsgegevens.

De proef mislukte volgens [SPA05] doordat de beveiliging van het systeem niet optimaal bleek te zijn en het systeem niet deed wat het moest doen. Er traden fouten op in de patiëntinformatie en computer- en verbindingsstoringen met de infrastructuur waren eerder regel dan uitzondering. Hierdoor waren de patiëntgegevens op de centrale server niet actueel en was er dus wel sprake van digitale communicatie maar dan wel met verouderde gegevens.

Het NICTIZ heeft dit meegenomen in haar specificatie waarbij centralisatie van gegevens als ongunstig te bestempelen. Initiatieven om te bekijken of met aanpassingen dit principe alsnog een succes kon worden zijn door de grote aantal oorzaken als storingen en verspreiden van verkeerde informatie gestaakt.

Project UZORG

Een succesvol geïmplementeerde infrastructuur waarbij men gebruik heeft gemaakt van een centrale LSP en decentraal opgeslagen patiëntinformatie is het systeem bij UZORG. Hier wisselt men via het Universele Patiënten Identificatie Database (UPID) lokaal opgeslagen patiëntgegevens via een LSP uit. Op het LSP is een verwijsindex ingericht die laat zien welke informatie waar over patiënten voorhanden is. Wanneer een zorgaanbieder via een korte beschrijving de gewenste informatie heeft gevonden en de volledige informatie wenst op te halen maakt de verwijsindex contact met het lokale computer van de informatie leverende zorgaanbieder. De gegevens worden via het LSP doorgezonden naar de vragende partij. Middels logging wordt continue bijgehouden welke acties een specifieke gebruiker op het systeem uitvoert.

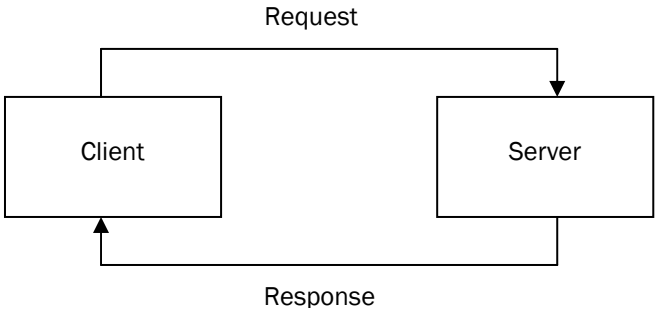
Op dit moment is vanwege de beperkte mogelijkheden het UPID nog niet multi-directioneel. Wat zoveel betekent als dat een huisarts patiëntgegevens bij de aangesloten ziekenhuizen kan inzien, maar een ziekenhuis de gegevens van de huisarts nog niet kan inkijken.

Het centrale karakter van het LSP en de decentrale opstelling van UZORG zijn ook door het NICTIZ als uitgangspositie gekozen.

Op dit moment ontstaan er op meerdere plaatsen in het land dergelijke regionale UPID-projecten, waarbij het de bedoeling is deze regionale verkeerstorens te koppelen met het NICTIZ LSP. Door, verplicht, deze systemen te laten aansluiten op het nationale LSP probeert men te voorkomen dat ook deze regionale LSP's hun patiëntinformatie kunnen delen, waardoor wordt voorkomen dat er eilandjes met informatie ontstaan. Er dient uiteindelijk een nationale bron te ontstaan waarin alle, maar dan ook alle gegevens van alle Nederlanders opvraagbaar zijn.

5.2.2 Server en clients

Een van de punten die het NICTIZ heeft overgenomen is het gebruik van een server en een client. De server wordt in dit geval het LSP. Deze heeft een "dienende" taak en staat direct in contact met de aangesloten clients van de zorgverleners.



Figuur 5.1: Client-serverarchitectuur waarbij de server passief reageert op een verzoek van de client

Via een netwerk is het vervolgens mogelijk om informatie uit te wisselen waarbij een vraag (request) van een client door de server 24/7 dient te worden beantwoord (response) (figuur 5.1). Deze permanente informatievoorziening geeft de zorgverleners de mogelijkheid op elk gewenst moment de voor hem nuttige informatie over een patiënt op te vragen. De wachttijd op informatie wordt hierdoor beperkt.

5.2.3 Mogelijke configuraties

Het NICTIZ heeft in haar specificaties gekozen voor een verkeerstoren met daaraan verbonden de clients van de zorgverleners. Deze centrale – decentrale opstelling heeft een aantal voordelen en is niet zomaar gekozen. Hoewel het NICTIZ bij de totstandkoming van deze infrastructuur zich heeft gebaseerd op een aantal proefprojecten en bevindingen in andere landen, zijn er daarnaast nog een drietal infrastructuren mogelijk.

Configuraties LSP	Configuraties gegevensopslag
Centraal	Centraal
Centraal	Decentraal
Decentraal	Centraal
Decentraal	Decentraal

Tabel 5.1: LSP configuratieopties

De vier configuratie types (zie tabel 5.1) verschillen van een centrale tot een decentrale infrastructuur aangevuld met twee varianten. Aan de hand van een aantal voor- en nadelen van de diverse configuratiemogelijkheden wordt uiteindelijk een beeld verkregen welke configuratie het beste bij de behoefte past. Deze conclusie bekijkt welke technisch de meest wenselijk is. De kosten worden daarbij buiten beschouwing gelaten.

5.2.4 Voor- en nadelen centrale LSP

Een centrale LSP kent voor- en nadelen als het gaat om het gebruik ervan. Welke in het oog springende voor- en nadelen heeft een dergelijke configuratie? Onderstaande tabellen tonen een aantal belangrijke punten waarop het LSP voorbij streeft aan de decentrale variant. Zonder al te optimistisch te zijn, worden ook een aantal nadelen genoemd waar men wel degelijk rekening mee dient te houden.

Voordelen centrale LSP
• SPOC: Single Point of Contact. Systemen zijn met een systeem gekoppeld. De technische structuur blijft hierdoor overzichtelijk. Het beheer en de kennis zijn daarbij ook gecentraliseerd. Dit bevordert onder andere de betrouwbaarheid en verminderd de complexiteit.
• Alle gegevens zijn beschikbaar via één centrale connectie. Men weet dus waar de gegevens zich bevinden. Dat bevordert de duidelijkheid binnen een complex systeem en bevraging is hierdoor eenvoudiger af te handelen omdat controle eenmalig op deze LSP hoeft plaats te vinden.
• Doordat het LSP de identiteit uitvoert hoeven de aangesloten zorgsystemen dat niet meer te doen. Dat geldt ook voor de rechten die aan een zorgverlener worden toegewezen. Hierdoor ontstaat eenvormigheid in de toegangsverlening.
• De kans op fouten zijn vanwege het SPOC beperkter en eenvoudiger te herleiden.
• Door de centrale structuur is het gebruik van logging mogelijk waardoor onweerlegbaarheid van informatie-uitwisseling is aan te tonen,
• Beperkte complexiteit en hierdoor een besparing ten opzichte van het gebruik van een decentrale LSP.
• Uitrol van het systeem is sneller en eenvoudiger uit te voeren.
• Bij eventuele calamiteiten kan de service snel weer worden hervat.
• Versiebeheer en informatie van het centrale LSP zijn altijd onder controle

Tabel 5.2: Voordelen centrale LSP configuratie

Nadelen centrale LSP
SPOF: Single Point of failure. Availability afhankelijk van één contactpunt.
• Slechte load balance door een niet optimale schaalbaarheid.
• Door SPOC zijn beveiligingsmaatregelen essentieel om te zorgen dat systeem bij calamiteiten wordt opgevangen of overgenomen om garant te kunnen blijven staan voor de beschikbaarheid.
• Volgens [NIC05a] behoeft geen systeem synchroon met het LSP mee te draaien ten behoeve van het overnemen van de taken bij calamiteiten.
• Het LSP wordt geëxploiteerd en onderhouden door een commercieel bedrijf. Zij hebben toegang tot alle gegevens en kennen het systeem. Tevens hebben zij toegang tot alle gegevens op het LSP wat risico's met zich mee brengt voor privacy en de veiligheid van deze gegevens.
• Verhoogde kans op attacks, vanwege het feit dat een kwaadwillende zeker weet dat dit de server is met uiteindelijk verwijzingen naar belangrijke gegevens.

Tabel 5.3: Nadelen centrale LSP configuratie

5.2.5 Voor- en nadelen decentrale gegevensopslag

De bij het LSP beschreven voor- en nadelen van centralisatie zullen ook bij de gegevensopslag worden opgesteld. De bevindingen van decentralisatie worden in de twee onderstaande tabellen gegeven.

Voordelen decentrale gegevensopslag
• Gegevens blijven bij de rechthebbende zorgverlener.
• Het LSP heeft geen verantwoordelijkheid als het gaat om de opslag en beveiliging van patiëntgegevens. Deze liggen bij de eigenaar van de gegevens.
• Versiebeheer van patiëntdossier is eenvoudiger uit te voeren omdat de laatste versies van de patiëntinformatie altijd bij de lokale bronnen van de rechthebbende eigenaar staan.
• De dure zorgsystemen die bij de zorgaanbieders in gebruik zijn, kan men blijven gebruiken. Extra investeringen in nieuwe systemen en grote aanpassingen worden daardoor vermeden.
• Het LSP wordt door gebruik van decentrale gegevensopslag ontzien. Dit doordat de data zich bij de eigenaren bevinden en het opvragen van data vermindert omdat in eerste instantie met behulp van de verwijsindex een goed beeld kan worden verkregen welke informatie de betreffende partij nodig heeft. Informatie die men niet kan gebruiken wordt zodoende ook niet verzonden.
• In geval van problemen bij de LSP blijven de patiëntgegevens ongemoeid, omdat deze lokaal zijn opgeslagen.
• Het beheer en verantwoordelijkheid van datagegevens ligt bij de zorgverlener.

Tabel 5.4: Voordelen decentraal LSP configuratie

Nadelen decentrale gegevensopslag
• Decentralisatie van de gegevens heeft als nadeel dat de zorgverlener, groot en klein, zich dienen te verdiepen in de ICT. De zorgaanbieder wordt naast arts dus ook ict'er. Kennis van zaken op dit gebied heeft een zorgaanbieder, vooral in kleinere praktijken niet. Beheer, onderhoud en beveiliging van de lokale beschikbare patiëntgegevens verdienen extra aandacht.
• Indien een zorgaanbieder tijdelijke niet is aangesloten op het LSP, bijvoorbeeld vanwege een technische storing, betekent dit dat zijn patiëntgegevens niet oproepbaar zijn via het LSP voor andere zorgaanbieders, terwijl dit misschien wel van levensbelang voor de patiënt kan zijn.
• Omdat de zorgaanbieders gebruik blijven maken van het softwarepakket dat men reeds gebruikt heeft, wordt de kans op problemen rondom foutieve interpretatie van de gegevens door een ander vergroot. De gegevens kunnen nu door meer zorgverleners met diverse achtergronden in verschillende systemen worden opgevraagd dan nu het geval is. Tevens zal hierdoor de kans op overdrachts- en invoerfouten stijgen.

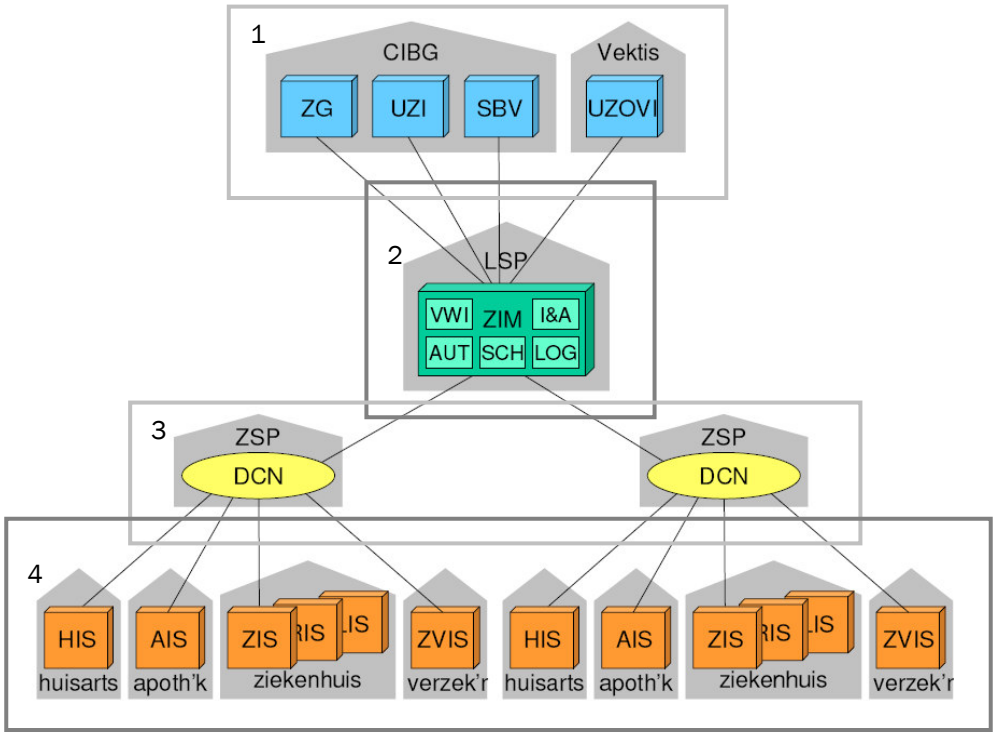
• Patiëntinformatie lokaal opslaan en beschikbaar maken via het internet heeft tot gevolg dat lokale systemen extra worden belast omdat gegevens van deze zorgsystemen moeten worden gedownload, de verbinding wordt daardoor zwaarder belast waardoor de communicatie wellicht trager kan verlopen. Tevens is de kans op problemen en verstoringen vele malen groter vanwege het feit dat men gebruik maakt van een open netwerk (het internet) waardoor misbruik of pogingen daartoe zullen toenemen en daardoor het systeem en de daarop beschikbare patiëntgegevens in gevaar kunnen brengen.
• De betrouwbaarheid van de infrastructuur is afhankelijk van de verbinding tussen de lokale zorgaanbieders en het LSP. Indien er een storing plaats vindt voor, tijdens of na gegevensuitwisseling, dan kunnen er grote problemen ontstaan.

Tabel 5.5: Nadelen decentraal LSP configuratie

5.3 Basisinfrastructuur op organisatorisch gebied

5.3.1 Inleiding

Het functioneren van het LSP is niet alleen afhankelijk van de aangesloten zorgaanbieders en de beschikbare patiëntgegevens. Het LSP fungeert niet zonder dat er leveranciers zijn betrokken die diverse diensten leveren aan het LSP waardoor deze een aantal taken correct kan uitvoeren. Zo is een leverancier verantwoordelijk voor het uitleveren van elektronische toegangspassen en is een andere leverancier verantwoordelijk voor het leveren van informatie betreffende alle zorgverleners.



Figuur 5.2: Onderlinge relaties basisinfrastructuur [NICT05a]

Naast de registerhoudende partijen (figuur 5.2 nr: 1.), levert het LSP (nr: 2.) een aantal diensten en verzorgen het ZSP (nr: 3.) en de aangesloten GBZ's (nr: 4.) ervoor dat de informatie van en naar de juiste zorgverleners wordt doorgezonden. In de volgende secties zal de gehele infrastructuur in vogelvlucht worden beschreven om de structuur enigszins te verhelderen.

5.3.2 Registerhouder CIBG

Het Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG) heeft als taak het registreren van gegevens en het verstrekken van informatie binnen de zorg. Het CIBG kan worden gezien als een kenniscentrum van de Nederlandse gezondheidszorg waarbij de kwaliteit wordt gewaarborgd door wetgeving of op basis van vastgesteld beleid. Een van de speerpunten van het CIBG is de ontwikkeling van ICT in de Zorg waarbij het een belangrijk aandeel levert bij de realisatie van de implementatie van het EMD en WDH.

Het CIBG zal een drietal diensten gaan beheren en leveren aan het LSP, namelijk:

- **Zorgaanbiedergids (ZG)**
  De ZG wordt een gemeenschappelijke ICT-voorziening waarin alle zorgaanbieders in Nederland met hun bereikbaarheidsgegevens worden opgenomen. De gids biedt zorgpartijen de mogelijkheid om te bladeren en het adres van een zorgverlener op te zoeken.

- **Unieke Zorgverlener Identificatie register (UZI-register)**
  Het UZI-register is een gemeenschappelijke ICT-voorziening waarin zorgaanbieders met hun zorgverleners en medewerkers worden geregistreerd die zijn voorzien van een UZI-pas.
  Het UZI-register levert of verifieert op verzoek van zorgpartijen het UZI-nummer van een zorgverlener op basis van een set identificerende gegevens. Daarvoor kunnen zorgpartijen rechtstreeks contact zoeken met het UZI-register via een website.

  De UZI-pas is een vertrouwensmiddel op basis van Public Key Infrastructure Overheid (PKIO). Wat inhoudt dat de UZI-pas aparte sleutelparen bevat voor authenticatie, versleuteling en handtekening. Het UZI-register verifieert op verzoek van zorgpartijen de geldigheid van een UZI-pas en geeft uitsluitsel omtrent wie de houder is, welke zorgverlenerfunctie die heeft en voor welke instelling hij werkt. Het UZI-register levert op verzoek ook certificaten van publieke sleutels.

- **Sectorale BerichtenVoorziening Zorg (SBV-Z)**
  De SBV-Z is een gemeenschappelijke ICT-voorziening ten behoeve van het gebruik van het BSN in de zorgsector. De SBV levert of verifieert op verzoek van zorgpartijen het BSN op basis van een set identificerende gegevens.

  Zorgpartijen kunnen rechtstreeks contact zoeken met de SBV-Z via een website en door middel van bestandsuitwisseling. Wanneer de ZIM is aangesloten op de SBV-Z kunnen zorgpartijen ook met hun Goed Beheerd Zorgsysteem (GBZ) via de ZIM de SBV bevragen. Als zodanig kan het BSN dienst doen als landelijk patiëntnummer.

5.3.3 Registerhouder Vektis

Het Vektis is het centrum voor informatie en standaardisatie voor de zorgverzekeraars. Gegevens over kosten van de gezondheidszorg in Nederland worden hier verzameld en geanalyseerd. Deze informatie is voor zorgverzekeraars van belang voor het vernieuwen van hun beleid, het maken van strategische keuzes, het verbeteren van operationele processen en de elektronische uitwisseling tussen zorgverzekeraars en anderen.

De identificatie van zorgverzekeraars is opgenomen in het zogenaamde UZOVI-register. Een register dat door Vektis wordt beheerd. Het register bevat zorgverzekeraars, gevolmachtigde assurantie-tussenpersonen, zorgkantoren, label-organisaties en nevenvestigingen en is ontwikkeld om eenduidig vast te kunnen stellen wie een zorg-verzekeraar is. Dit register draagt, samen met het UZI-register, bij aan de integriteit, authenticiteit en vertrouwelijkheid van elektronische communicatie.

5.3.4 Landelijke SchakelPunt

Het LSP zal het mogelijk maken om zorginformatie landelijk uit te wisselen. Het LSP heeft hiervoor een aantal functies ingebouwd om dit mogelijk te kunnen maken. Deze functies worden nader beschreven in sectie 5.4.

De technische functionaliteiten wordt niet door het LSP, maar door de zogenaamde Zorg Informatie Makelaar (ZIM) verzorgd. In feite levert deze de functies en vormt samen met andere organisatorische en technische diensten en functies het LSP.

Het LSP staat in contact met de Zorg Service Providers (ZSP's) die de verbinding verzorgt tussen LSP en een gecertificeerde GBZ van de zorgverleners. Het concept van het LSP steunt op het uitgangspunt dat alle zorggegevens bij de bron, de verantwoordelijke zorgverlener, blijven.

5.3.5 Zorg Service Providers (ZSP)

Een ZSP is een organisatie die de verbinding verzorgt tussen het GBZ en LSP. Via dit netwerk worden de gegevens verstuurd. Het ZSP draagt de zorg dat GBZ's aangesloten op de zorginfrastructuur voldoen aan de eisen die het LSP hieraan stelt. Wanneer een GBZ is goedgekeurd, kan deze op de LSP worden aangesloten. Zonder deze goedkeuring, welke in handen is van het ZSP, mag een systeem van een zorgverlener niet aangesloten worden op het LSP. Op deze manier probeert men in eerste instantie te voorkomen dat systemen die voor problemen kunnen zorgen niet worden aangesloten. Hoe de controle plaats vindt nadat een systeem goed is gekeurd en aan welke eisen een systeem moet voldoen is niet vastgelegd.

Een ZSP fungeert daarnaast ook als helpdesk voor de zorgaanbieders. Indien problemen niet door de ZSP kunnen worden opgelost, zal de helpdesk van het LSP de taak proberen op te lossen.

De rol van de ZSP is belangrijk aangezien het LSP niet in staat zal zijn alle zorgaanbieders in Nederland individueel te benaderen en te ondersteunen.

Data Communicatie Netwerk (DCN)

Een DCN is een gemeenschappelijke ICT voorziening die nodig is om de GBZ'en van verschillende zorgpartijen te kunnen aansluiten op het LSP.

Om een DCN te mogen aansluiten op het LSP zal de ZSP een aantal ondersteunende diensten moeten bieden aan zorgaanbieders die hun GBZ willen aansluiten. Deze diensten omvatten:

- De uitgifte van vaste IP-adressen aan GBZ'en toegekend door het LSP,
- De aanlevering van routeringsgegevens aan het LSP voor uitgegeven IP-adressen,
- Hulp aan zorgaanbieders bij het aansluiten van hun GBZ'en,
- De eerste-lijns hulp aan zorgaanbieders bij incidenten,
- De bewaking van de prestaties van het DCN.

5.3.6 Goed Beheerd Zorgsysteem (GBZ)

Een GBZ is een individuele ICT-voorziening van een zorgpartij (zorgaanbieder, zorgverzekeraar etc.) die voldoet aan een aantal eisen om te mogen worden aangesloten op de ZIM. Zo wordt er gebruik gemaakt van SSL, TLS, NEN7510, HL7 en XML/SOAP.

Een zorgsysteem, zoals dat bij een zorgpartij in gebruik is, is een combinatie van procedures, computers, randapparatuur, software en beheer die wordt gebruikt voor het vastleggen, bewerken en uitwisselen van patiëntgegevens in een zorgomgeving. Dat kan in schaal verschillen van een huisarts met een pc, printer en een modem tot een ziekenhuis met een grootschalig computernetwerk, honderden PC's en een ICT-afdeling met een helpdesk.

In algemene zin dient een GBZ aan de volgende eisen te voldoen:

- Te ontvangen en te versturen berichten op basis van standaarden,
- Autorisatie van gebruikers en logging van communicatie met andere GBZ'en en/of het LSP,
- Connectiviteit (koppelingen met systemen buiten de zorginstelling),
- Beveiliging van computersystemen en netwerk,
- 7 x 24 uur Beschikbaar,
- Betrouwbaarheid (worden de juiste gegevens vastgelegd en opgeleverd),
- Actualiteit van de gegevens,
- Performance (hoe snel worden berichten verstuurd en ontvangen),
- Het beheren van het zorgsysteem.

5.4 Wat levert het LSP

In sectie 5.3.4 werd het LSP al geïntroduceerd. Het NICTIZ maakt bij het LSP onderscheid tussen diensten en functies. In dit onderzoek worden alleen de belangrijkste functies beschreven. Het LSP zal in samenwerking met het ZIM, die de technische functies gaat leveren, de volgende functies bevatten:

- **Schakelpunt**; het Landelijk Schakelpunt wordt in de [NIC05a] gedefinieerd als: “Een loket voor het opvragen van patiëntgegevens, waar alle opvragingen van patiëntgegevens kan worden geplaatst, wordt doorgeschakeld naar de juiste patiëntendossier en resultaten doorschakelt naar de opvrager”. Het schakelpunt zal concreet gezien informatie naar de juiste partij doorsturen. Het schakelpunt fungeert hierbij als de verkeerstoren om de informatiestromen in goede banen te laten verlopen. Om de integriteit te waarborgen bevat het LSP geen gevoelige informatie. Echter, blijkt uit zelfde NICTIZ documentatie dat wel degelijk informatie tijdelijk wordt opgeslagen.
- **Verwijsindex**; een belangrijke functie van het LSP is die van de verwijsindex. Deze wordt in de [NIC05a] gedefinieerd als: “een tabel met verwijzingen naar patiëntendossiers waar patiëntengegevens met bepaalde kenmerken/attributen beschikbaar zijn voor opvraag. Doel van de verwijsindex is het doelmatig opvragen van alleen die dossiers die de gevraagde gegevens bevatten”. Het Landelijk Schakelpunt is dus continue, via de verwijsinformatie, op de hoogte waar de meest recente patiëntgegevens in zorginformatiesystemen zich bevinden. Het voordeel dat hiermee wordt behaald is dat men over de laatste informatie van een patiënt direct kan beschikken. Voorkomen wordt dat men oude gegevens gebruikt en daardoor verkeerde beslissingen neemt.
- **Identificatie**; toegang tot het LSP verloopt middels identificatie op basis van de UZI-pas. Zorgaanbieders worden na identificatie met deze pas door het Landelijk Schakelpunt geauthenticeerd. Er is dan vast te stellen of de betreffende gebruiker ook daadwerkelijk is wie hij zegt dat hij is. Zonder geldige UZI-pas is gebruik van het LSP door een zorgverlener niet mogelijk.
- **Autorisatie**; het autorisatieproces toetst een aantal zaken zoals controle of de patiënt vooraf bezwaar heeft gemaakt tegen een gegevensuitwisseling tussen zorgaanbieders. Deze bezwaren worden vastgelegd in een autorisatieprofiel per patiënt. Aanvankelijk heeft een patiënt de keuze om wel of niet mee te doen. Tevens behelst autorisatie ook het toekennen van rechten op basis van de functie die de gebruiker uitvoert binnen de gezondheidszorg. Het doel van autoriseren is dan rechten toe te kennen aan de gebruiker en er voor zorgen dat de gebruiker geen taken kan uitvoeren waarvoor hij geen bevoegdheden heeft. Maar ook controle achteraf of de uitgevoerde taken terecht door de gebruiker zijn uitgevoerd is onderdeel van het autoriseren.
- **Logging**; wie heeft op welk tijdstip toegang tot het LSP gezocht en wie heeft wanneer welke acties op het LSP uitgevoerd en vanaf welke locatie? Dergelijke vragen worden verkregen met het in logbestanden weggeschreven informatie afkomstig van acties die gebruikers op het LSP uitvoeren.

- **Helpdesk**; Het LSP en de ZSP's is voorzien van een helpdeskfunctie voor de aangesloten GBZ's. Hier worden de problemen gefilterd en opgelost. Blijkt het te gaan om een probleem van grotere aard dan zal de ZSP helpdesk het probleem doorgeven aan de tweedelijns helpdesk bij het LSP. Op deze wijze probeert men de helpdesk van het LSP zoveel mogelijk te ontdoen van problemen lager in de infrastructuur. De helpdesks zullen na de exploitatieperiode van twee jaar 24 uur, 7 dagen in de week bereikbaar zijn.

5.5 Opvragen en plaatsen van patiëntinformatie

5.5.1 Communicatie op basis van het BSN

De LSP functies zijn nodig om communicatie mogelijk te maken zoals het NICTIZ zich dat heeft voorgesteld. Een van die hoofdtaken die het LSP daarbij gaat uitvoeren is het opvragen en plaatsen van patiëntinformatie. Voor het identificeren van patiënten en de verwijsindex te instrueren welke informatie van diverse systemen verzameld dient te worden gaat het LSP gebruik maken van het Burger Service Nummer (BSN) van de patiënt. "Het BSN-nummer is een uniek identificerend nummer voor iedereen die een relatie heeft met de Nederlandse overheid" [WEBBSN]. Dit nummer is gelijk aan het huidige Sofinummer, maar zal voor meer doeleinden ingezet gaan worden. De relatie zal zich in eerste instantie beperken tot de zorg en fiscale sector, maar snel worden uitgebreid voor andere doeleinden. Het BSN wordt dus gekoppeld aan een patiënt en zijn patiëntendossier. Dit unieke nummer zorgt er voor dat een zorgverlener snel de juiste gegevens kan opvragen die bij dit nummer horen. [SPA05] stelt echter vast dat het BSN een gevaar kan zijn voor de privacy van een Nederlands staatsburger. Omdat met dit BSN nummer eenvoudig de koppeling tussen andere administraties is te leggen. Daarnaast stelt zij ook vast dat het nu nog gangbare SociaalFiscaal (SoFi)-nummer niet uniek is, wat problemen op diverse gebieden in de hand werkt.

5.5.2 Opvragen van medische patiëntinformatie

De basis van het verwijsindex is het opvragen van beschikbare patiëntinformatie met het BSN en deze gegevens vervolgens op te halen bij de verschillende zorgverleners waar informatie over de betreffende patiënt zich bevindt. In figuur 5.3 wordt het af te leggen traject om gegevens in te zien weergegeven. Hierbij worden cruciale procedures als identificatie, authenticatie en autorisatie buiten beschouwen gelaten.

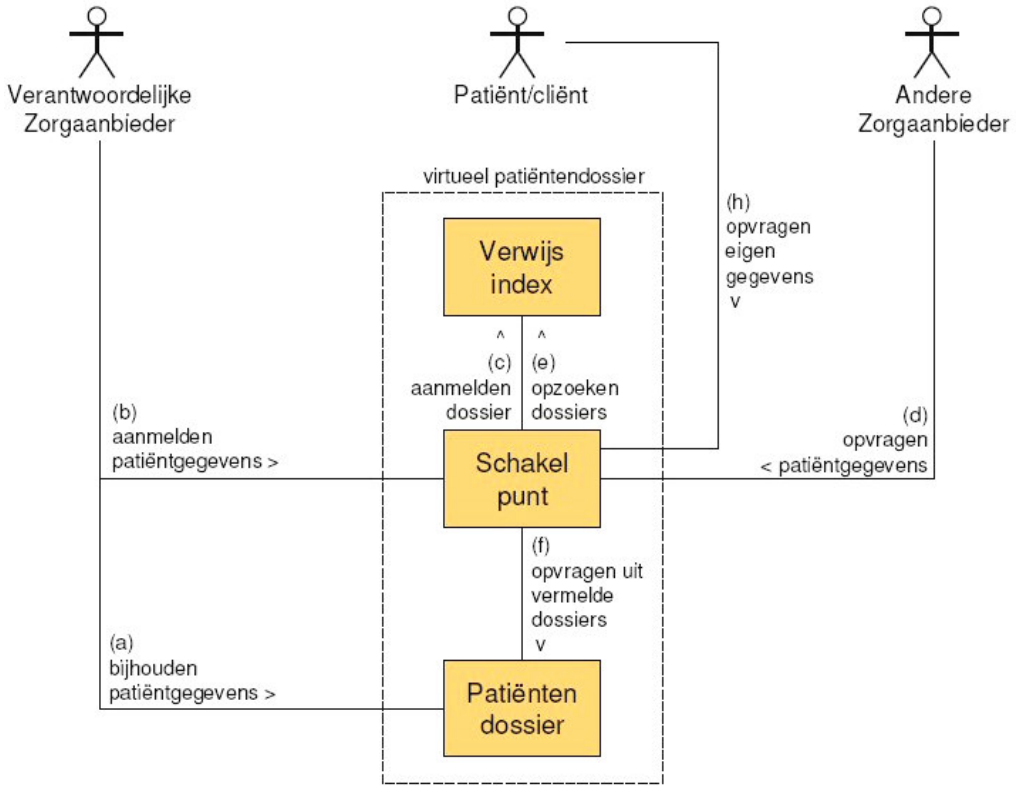
Het opvragen van patiëntinformatie door een zorgverlener verloopt volgens onderstaand patroon:

a) De verantwoordelijke zorgaanbieder houdt de patiëntstukken van zijn patiënt bij in zijn eigen dossier,
b) De verantwoordelijke zorgaanbieder meldt aan het schakelpunt van welke patiënt stukken beschikbaar zijn in zijn dossier,
c) Het schakelpunt legt de beschikbaarheid van die patiëntstukken in dat dossier vast in de verwijsindex,
d) Andere betrokken zorgaanbieders die bepaalde patiëntgegevens willen opvragen, ongeacht in welk dossier, richten zich tot het schakelpunt,

e) Het schakelpunt raadpleegt de verwijsindex om te weten in welke dossiers de gevraagde patiëntstukken te vinden zijn,

f) Het schakelpunt vraagt vervolgens de gevraagde patiëntstukken op bij alle in de verwijdindex vermelde dossiers en schakelt de respons door naar de opvragende zorgaanbieder,

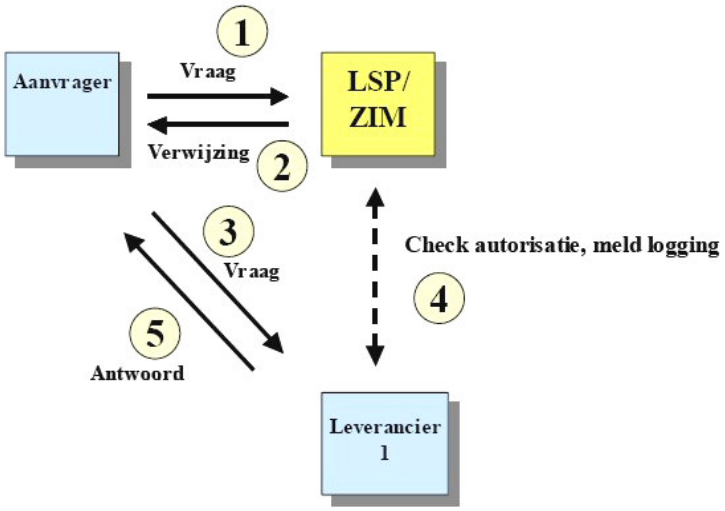
h) Op dezelfde wijze zal ook de desbetreffende patiënt in de toekomst toegang verkrijgen tot zijn gegevens.



Figuur 5.3: Opvragen patiëntinformatie [NICT05a]

Behandeling van grote bestanden

Er kan afgeweken worden van het hierboven beschreven communicatiepatroon wanneer veel data van bijvoorbeeld een patiëntdossier beschikbaar is bij diverse zorgverleners en de hoeveelheid van data het LSP negatief beïnvloed. In figuur 5.4 wordt weergegeven hoe men data zonder tussenkomst van het LSP alsnog bij de vragende partij aflevert zonder daarbij autorisatie uit het oog te verliezen.

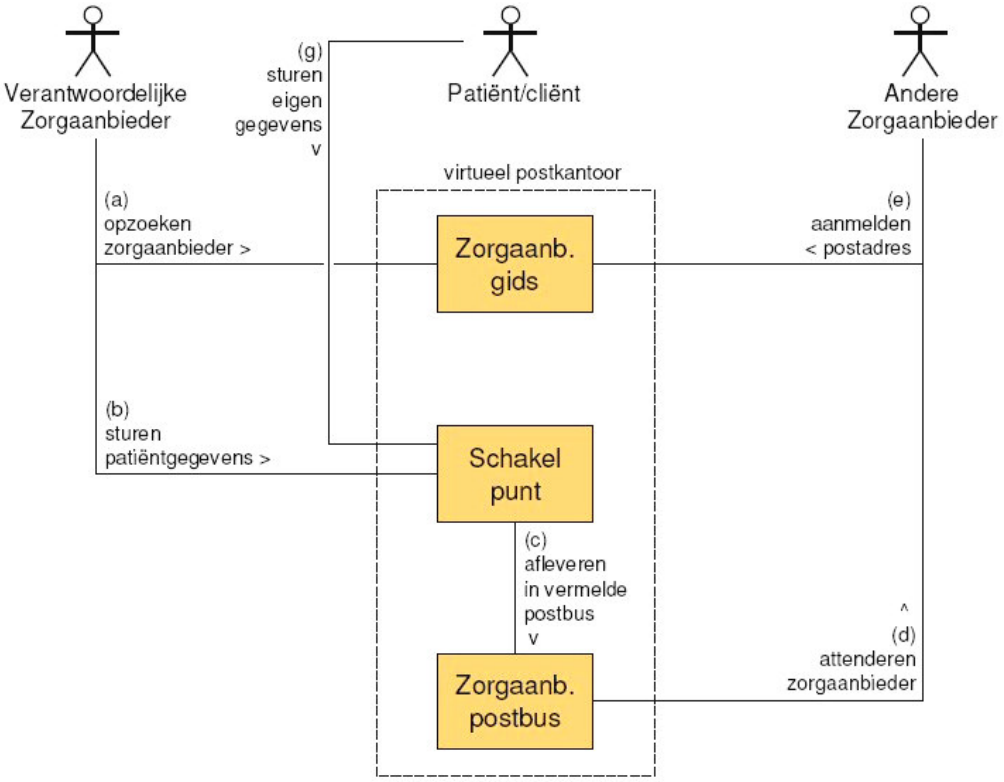


Figuur 5.4: Aanvraag en aflevering patiëntinformatie bij grote bestanden [NIC05a]

De keuze wanneer over moet worden gegaan naar dit afwijkende communicatiepatroon wordt gemaakt wanneer blijkt dat de te verzenden informatie boven de 1 MB per antwoord is. Per sessie van de aanvrager wordt bekeken wanneer er af wordt geweken van de standaardprocedure. Het LSP zal de verwijzing terugsturen naar de aanvrager (stap 2), die vervolgens hiermee direct de leverancier kan bevragen (stap 3). Doordat het gegevensleverende systeem een verzoek ontvangt van de aanvrager, controleert deze het verzoek via het LSP (stap 4). Deze ziet dat de aanvrager en de verzonden verwijzing zijn geïdentificeerd en goedgekeurd, waarna een bevestiging van het LSP aan de leverancier wordt terug gezonden. De leverancier krijgt hierbij het sein dat de gevraagde gegevens, zonder tussenkomst van het LSP, van de leverancier naar de aanvrager mag worden verzonden (stap 5). Of hierbij de gegevens, die direct tussen “leverancier” en “aanvrager” worden verzonden, ook zijn versleuteld is onduidelijk.

5.5.3 Plaatsen van medische patiëntinformatie

Om patiëntinformatie voor alle zorgverleners beschikbaar te kunnen maken zal elke zorgverlener de verwijzingen naar de patiëntinformatie waarover hij de verantwoordelijkheid heeft moeten aanmelden op het LSP. Figuur 5.5 toont het versturen van een medisch bericht naar de verwijsindex van het LSP.



Figuur 5.5: Bericht verzenden via LSP [NIC05a]

Het plaatsen van patiëntinformatie gaat als volgt in zijn werk:

a) De verantwoordelijke zorgaanbieder raadpleegt de zorgaanbiedersgids om een zorgaanbieder met een bepaalde specialisatie en postadres te vinden,
b) De verantwoordelijke zorgaanbieder stuurt een patiëntbericht met een vermelding van de bestemde zorgaanbieder naar het schakelpunt,
c) Het schakelpunt levert de patiëntberichten af in de postbus van de bestemde zorgaanbieder,
d) De postbus notificeert de bestemde zorgaanbieder op het beschikbaar komen van bepaalde patiëntberichten,
e) De bestemde zorgaanbieder dient zijn postadres vooraf te hebben aangemeld in de zorgaanbiedersgids,

g) In de nabije toekomst moet het mogelijk worden dat op een zelfde wijze ook de patiënt zelf berichten kan sturen naar zijn zorgaanbieders of telemedicine instructies ontvangen.

5.6 Conclusie

De voorgestelde configuratie voorziet erin dat gevoelige patiëntengegevens niet op één server worden bewaard, maar wel via een centraal punt beschikbaar zijn. Dit zorgt ervoor dat zorgaanbieders eindverantwoordelijk blijven over de patiëntgegevens van hun praktijk. Dat door deze configuratiekeuze het LSP geen enorme database bevat met de cruciale en privacy gevoelige gegevens wordt het risico wat betreft misbruik beperkt. De centrale positie en intelligentie van het LSP zorgt ervoor dat communicatie tussen LSP en informatiesysteem van de zorgaanbieder verloopt, zonder hiervoor grote aanpassingen op de in gebruik hebbende informatiesysteem te bouwen. Het gebruik van de bij de zorgverlener gebruikte informatiesystemen zorgt ervoor dat zorgverleners niet een nieuw systeem hoeven aan te schaffen en in hun vertrouwde omgeving kunnen blijven werken.

Keerzijde is dat controle door het LSP niet meer uitgevoerd kan worden als blijkt dat deze onbereikbaar is. Immers, identificatie, authenticatie en autorisatie vindt plaats via het LSP. Tevens is nadelig van deze configuratie is dat wanneer het LSP door een storing tijdelijk niet bereikbaar is en er geen informatie-uitwisseling tussen zorgverleners kan plaats vinden, digitaal uitwisseling onmogelijk wordt. Het LSP wordt doordat het optreedt als Single Point Of Contact (SPOC) een eenvoudig doelwit als Single Point Of Failure (SPOF). De voordelen die één contact punt met zich meebrengt, is ook meteen de zwakke plek. Wanneer het LSP niet optimaal functioneert door het uitvallen van alle of delen van functies, zijn ook de resultaten die de zorgverlener krijgt opgestuurd, nadat hij om informatie van een patiënt heeft verzocht, onbetrouwbaar of niet volledig. Verkeerde patiëntinformatie bij de zorgverlener kan leiden tot verkeerde beslissingen die men door gebruik van dit systeem juist zo graag wil voorkomen.

Daarnaast heeft het NICTIZ ook in de specificaties opgenomen dat patiëntgegevens feitelijk vanaf de leverende zorgaanbieder worden gekopieerd en doorgestuurd naar de vragende zorgaanbieder. Tijdens deze procedure zullen patiëntgegevens tijdelijk op het LSP worden geparkeerd en vervolgens worden doorgezonden. Wanneer de gegevens correct zijn ontvangen bij de vragende partij, zullen de gegevens alsnog worden verwijderd. Hiermee creëert het NICTIZ twee risico's. Ten eerste: dat het LSP ondanks allerlei berichten, hoewel tijdelijk, privacy gevoelige informatie bevat. Daarnaast beschikt de niet verantwoordelijke zorgverlener na ophalen van patiëntinformatie, over een kopie van het patiëntendossier waarover een andere zorgverlener eindverantwoordelijk is. Beide hebben grote gevolgen hebben voor de patiënt, het gebruik van de patiëntinformatie, de zorgverleners en dus het gezicht van de zorgsector. Want zijn deze dan nog wel te vertrouwen? En hoe stelt men vast dat de ontvangen gegevens ongeschonden aankomen bij de andere zorgverlener? Hoe groot is het risico dat een collega zorgverlener de juiste gegevens gebruikt voor de diagnose en niet gebruikt maakt van verouderde informatie die hij reeds had binnen gehaald en opgeslagen in zijn systeem? Hoe groot is het risico dat deze lokaal opgeslagen gegevens uitlekken, terwijl de verantwoordelijke zorgverlener verplicht is om de privacy van de patiënt ten alle tijden in bescherming te nemen. Wanneer deze gegevens ook ergens anders opgeslagen is, is dat dan nog wel mogelijk? Is de geheimhoudingsplicht dan nog wel uit te voeren? Ook deze gegevens kunnen uitlekken doordat een GBZ helemaal niet (meer) aan de gestelde certificeringeisen voldoet. Daarbij komt dat als gegevens van een patiënt bij een andere zorgverlener zijn opgeslagen in een digitaal dossier, de

zorgverlener die deze gegevens beheerd zijn verantwoordelijkheid naar de patiënt niet meer kan garanderen. Problemen die hierbij kunnen optreden kunnen grote gevolgen met zich meebrengen.

Hoewel het NICTIZ wil doen geloven in hun specificaties dat er geen patiëntinformatie op het LSP wordt opgeslagen, is het tegendeel waar. Deze informatie wordt wel degelijk opgeslagen. Dit is slecht van tijdelijke aard, maar dat betekend dat bij volledige ingebruikname er vele dossiers op het LSP zijn opgeslagen. Na succesvol verzenden worden deze dan wel weer van het LSP verwijderd. Deze opslag is in het nadeel van de integriteit van het LSP die met deze opslag de aanvaller een makkelijk doel geeft om gegevens via een centraal punt te verkrijgen. Waarom heeft het NICTIZ er niet voor gekozen om de patiëntinformatie te versleutelen en door te sturen naar de vragende partij waar vervolgens het dossier wordt gereproduceerd?

Nog een probleem is dat patiëntinformatie nu ook op meerdere plekken is opgeslagen. De verantwoordelijke zorgverleners hebben ieder hun specifieke patiëntinformatie, maar vullen deze aan door ook gegevens van andere zorgverleners eraan toe te voegen waar de patiënt bekend is. Het lokaal opslaan van deze gegevens kan er toe leiden dat men gebruik gaat maken van verouderde informatie. Een oplossing voor dit probleem zou het inzetten van een volledig virtueel patiëntendossier kunnen zijn zoals nu reeds bij het UZORG succesvol gebruik van wordt gemaakt. Met dit virtuele dossier worden gegevens real-time en webbased aan de zorgverlener op het scherm afgeleverd. Deze gegevens kunnen niet op het systeem worden opgeslagen, maar worden alleen vanuit de diverse bronnen bij elkaar gebracht. De verantwoordelijkheid blijft zodoende bij de eigenaren. Privacy is deels gewaarborgd doordat gegevens niet meer opgeslagen kunnen worden. Heeft de verantwoordelijke zorgverlener geen zorgen betreffende de patiëntgegevens en worden altijd de meest actuele patiëntengegevens gebruikt.

"The only truly secure system is one that is powered off,
cast in a block of concrete and sealed in a lead-lined room with armed guards –
and even then I have my doubts."

Dr. Eugene H. Spafford

6. Toegang en de gebruikte technieken

6.1 Inleiding

Om een dossier van een patiënt in te kunnen zien zal een zorgverlener zich toegang moeten verschaffen op het LSP. Met behulp van de verwijsindex worden dan de betreffende gegevens verzameld en aan de zorgverlener verzonden. Echter voordat een zorgverlener deze gegevens kan opvragen zal hij een toegangsprocedure moeten doorlopen om de gegevens via het LSP op te kunnen vragen.

Met behulp van toegangsbeveiliging zullen alleen zorgverleners toegang krijgen tot het LSP die hiervoor gerechtigd zijn. [OVE99] omschrijft toegangsbeveiliging als: "het voorkomen van ongeautoriseerde toegang tot informatie en informatiesystemen ter bescherming van de vertrouwelijkheid van de informatie om zodoende ongeautoriseerde en ongewenste wijzingen, vernieling of vernietiging van informatie of programmatuur te voorkomen, evenals verstoringen van het normale productieproces".

Wanneer de zorgverlener eenmaal toegang heeft gekregen op het LSP, gelden er per zorgverlener bepaalde rechten en beperkingen. Afhankelijk van de functie van de zorgverlener en de goedkeuring van de patiënt zijn er bepaalde LSP functies beschikbaar voor de zorgverlener.

In dit hoofdstuk zullen de belangrijkste technieken nader worden beschreven die toegangsprocedure op het zorgsysteem mogelijk moet maken. Daarbij worden de ook de toegangsprocedures belicht.

6.2 Gebruikte technieken

6.2.1 Minimale beveiligingsniveau

Voor een succesvolle en grootschalige invoering van een landelijk zorgsysteem is het van belang dat zorgaanbieders en zorgverzekeraars die met elkaar communiceren, dit doen op een beveiligingsniveau zodat er veilige informatie-uitwisseling kan plaats hebben.

Om informatiestromen te beveiligen zijn er een aantal diensten die noodzakelijk worden geacht:

- Garanderen van de vertrouwelijkheid van communicatie om ervoor te zorgen dat onbevoegden geen kennis kunnen nemen van de uitgewisselde informatie,
- Identificatie en authenticatie van zorgsystemen, zorgverleners en verzekeraars om er zeker van te zijn dat het systeem en/of de persoon waarmee wordt gecommuniceerd inderdaad degene is die hij beweert te zijn,
- Op basis van een correcte authenticatie kan de autorisatiebevoegdheden van een persoon worden bepaald. Daarmee verwerft de zorgverlener bepaalde rechten waarmee bepaalde acties zijn uit te voeren,
- Handhaven van de integriteit van informatie om onbevoegd wijzigen van informatie te voorkomen,
- Zorgdragen voor de onweerlegbaarheid van opvragen en verzenden van informatie om rechtsgeldige handelingen via elektronische communicatie te kunnen verrichten.

De hierboven genoemde noodzakelijke punten zullen in de onderstaande secties, door middel van het uiteenzetten van de toegepaste technieken, nader worden verduidelijkt.

6.2.2 De UZI-pas

Om veilige elektronische communicatie en raadpleging van vertrouwelijke informatie in het zorgveld mogelijk te maken, is het noodzakelijk om de betrokken partijen uniek te kunnen identificeren. Het UZI-register is hiervoor ingericht. Het UZI-register geeft aan zorgaanbieders een elektronische identiteit uit waarmee zij zich kunnen authenticeren zodat zij de vertrouwelijkheid in de communicatie kunnen waarborgen en een elektronische handtekening kunnen zetten. Die handtekening waarborgt de authenciteit en integriteit. Met behulp van de persoonsgebonden UZI-pas en bijbehorende PIN-code kan de identiteit van een gebruiker worden vastgesteld. Deze elektronische identiteit wordt vastgelegd in certificaten die zich met de behorende cryptografische sleutels op de UZI-pas (figuur 6.1) bevinden. Details over de sleutels en certificaten volgt in secties 6.2.3 en 6.2.4.

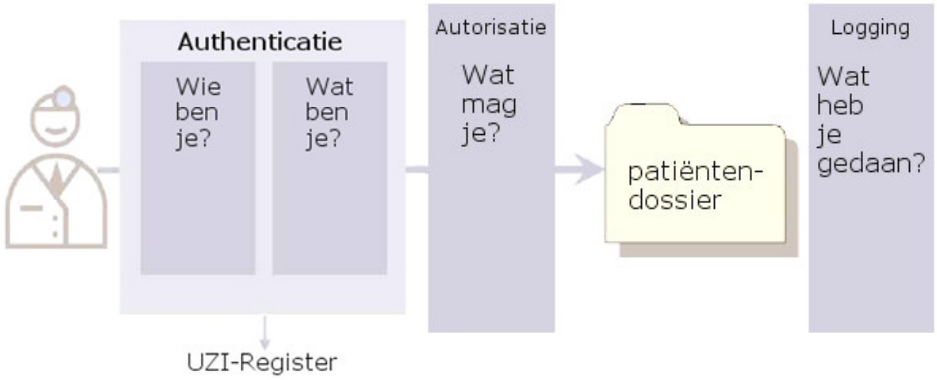
Figuur 6.1: De UZI-pas [UZI05]

De UZI-pas vervult de rol van elektronisch paspoort voor de zorgaanbieders. Zorgverleners kunnen zich met behulp van de UZI-pas authenticeren. Dat wil zeggen dat zij in het elektronische verkeer hun identiteit

kunnen bewijzen. De UZI-pas is daarmee te vergelijken met ons Nederlands paspoort. Een belangrijk individueel “waardedocument”. Daarnaast is de pas te gebruiken om gegevens te versleutelen of een veilig communicatiekanaal te realiseren en kan met behulp van de UZI-pas een elektronische handtekening worden gezet die dezelfde juridische waarde heeft als een handtekening op papier. De verantwoordelijke instelling, het UZI-register, garandeert de juistheid van de gegevens op de UZI-pas alsmede dat pas is uitgegeven aan een zorgverlener.

Functies UZI-pas

Een gebruiker van de UZI-pas kan zichzelf met de pas en unieke gebruikersnaam en wachtwoord identificeren, authenticeren, en een elektronische handtekening te plaatsen voor akkoord. De combinatie zorgt er voor dat de zorgverlener uiteindelijk toegang krijgt tot de voor hem specifiek opengestelde onderdelen van het zorginformatiesysteem.



Figuur 6.2: Afbakening UZI-register [UZI05]

De UZI-pas vervult de volgende basisfuncties (figuur 6.2), om toegang te krijgen tot het systeem, namelijk:

- Wie ben je? Bewijzen van de identiteit,
- Wat ben je? Autoriseren van de toegang,
- Wat mag je? Het zeker stellen van de vertrouwelijkheid van de communicatie,
- Wat heb je gedaan? Vastleggen van acties in een logbestand.

De UZI-pas is te vergelijken met de huidige bankpassen. De pas is voorzien van een magneetstrip én een chip. De magneetstrip wordt gebruikt voor facilitaire zaken bijvoorbeeld voor het parkeren. De magneetstrip bevat onder andere een Persoonlijke Identificatie Nummer (PIN). De chip is verantwoordelijk voor de identificatie van de zorgverlener op het LSP. Voordat een zorgverlener daadwerkelijk met de daarbij behorende bevoegdheden toegang heeft gekregen tot het LSP zijn een aantal technische middelen verantwoordelijk voor de totstandkoming van veilige en betrouwbare communicatie. Deze technieken zullen in de volgende secties aan de orde komen.

6.2.3 PKI Overheid

De Public Key Infrastructure (PKI) voor de overheid (PKIO) is ontworpen om betrouwbare elektronische communicatie binnen en met de Nederlandse overheid mogelijk te maken. Met de certificaten die op de UZI-pas zijn geplaatst, is toegang tot het LSP, in combinatie met een PIN, mogelijk.

Met het inzetten van de PKI-voorziening probeert men invulling te geven aan een aantal belangrijke betrouwbaarheidseisen, te weten:

- Identiteit en authenticiteit: om zeker weten met wie wordt gecommuniceerd,
- Integriteit: om zeker weten dat de informatie niet door derden gewijzigd kan worden,
- Vertrouwelijkheid: om zeker weten dat de informatie niet door derden gelezen kan worden.

Voor elk van deze functies is een certificaat beschikbaar, waarin Het certificaat bevat onder andere informatie over de eigenaar, de uitgever, de periode waarbinnen het certificaat geldig is en voor welke doeleinden het gebruikt mag worden. Zo kan een certificaat ingezet worden ten behoeve van het versleutelen van gegevens, identificatie of het zetten van een elektronische handtekening of het controleren daarvan. Deze certificaten zijn beschikbaar op elke uitgegeven UZI-pas waarmee de UZI-pas een persoonlijk item wordt waarmee vertrouwelijk moet worden omgegaan.

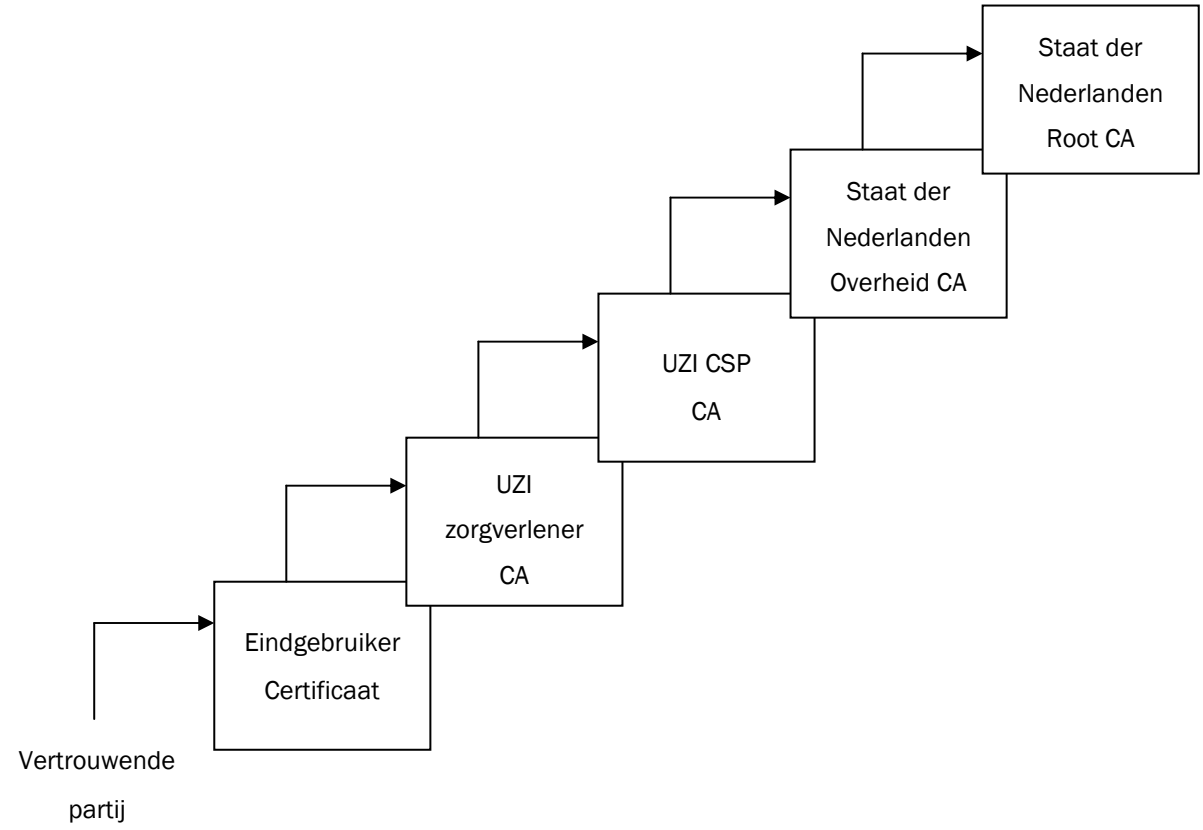
Met de UZI-pas wordt het mogelijk om vanaf een GBZ-systeem betrouwbaar te kunnen communiceren binnen de infrastructuur met het LSP. Ook kan gecontroleerd worden of de geplaatste elektronische handtekening daadwerkelijk klopt. Hiermee wordt onweerlegbaarheid (non-repudiation) aangetoond dat een zorgverlener het document ook daadwerkelijk heeft verzonden of een bepaalde actie ook heeft uitgevoerd.

Certificaten worden altijd in een hiërarchie geplaatst. Op het stamcertificaat na, zijn alle certificaten in de hiërarchie onbetwistbaar gekoppeld aan een hoger liggend certificaat. Dit maakt het mogelijk om een certificaat terug te leiden tot een stamcertificaat, de hoogste in de hiërarchie en daarmee het centrale punt van vertrouwen.

De Nederlandse overheid geeft een dergelijk stamcertificaat uit (figuur 6.3). Door vertrouwen te leggen in dit stamcertificaat, kunnen ook certificaten lager in de hiërarchie worden vertrouwd als deze ondertekend zijn door de Nederlandse CA. Er zijn hoge eisen gesteld aan uitgevers van certificaten binnen de hiërarchie van de overheid, ofwel certificaten die binnen PKI voor de overheid vallen. Hierdoor hebben alle certificaten binnen deze hiërarchie een hoog betrouwbaarheidsgehalte.

Als een vertrouwende partij een certificaat wil controleren dat door het UZI-register is uitgegeven, zal er vast worden gesteld of de handtekening onder het UZI-certificaat klopt. Door de keten te controleren komt men uiteindelijk terecht bij het stamcertificaat. Dit stamcertificaat is bijzonder vanwege dat er geen bovenliggend certificaat is waaraan het vertrouwen kan worden ontleend. Dit certificaat is daardoor zelfgetekend (self-signed).

De uitgever is zowel houder van het certificaat als ondertekenaar van dit certificaat. Voor de hiërarchie van het UZI-register is het stamcertificaat van de Staat der Nederlanden het hoogste vertrouwenspunt.



Figuur 6.3: Hiërarchie van een certificaat naar het stamcertificaat

Hoe werkt PKI

PKI is gebaseerd op asymmetrische encryptie oftewel sleutelparen. Een PKI-sleutelpaar bestaat uit een privé-sleutel en een publieke-sleutel. Deze zijn onlosmakelijk met elkaar verbonden en zijn per gebruiker uniek. Met behulp van de sleutelparen kan een gebruiker zich identificeren, met de privé-sleutel een elektronische handtekening zetten en met de publieke-sleutel informatie coderen.

Om de betrouwbaarheid van een publieke sleutel te kunnen waarborgen, is een neutrale derde partij nodig, de Trusted Third Party (TTP) die door iedereen binnen de gebruikersgroep wordt vertrouwd. In het geval van PKIO is dat de Staat der Nederlanden. De TTP controleert de identiteit van de eigenaar, deelt een privé sleutel uit en koppelt deze aan een bewijs van vertrouwen: het certificaat. Dit certificaat vormt voor andere gebruikers het bewijs dat de uitgegeven privé sleutel bij een persoon of organisatie hoort.

Wijze van ondertekenen en versleutelen

Het proces van ondertekenen en versleutelen van een brief volgens de beginselen van PKI. Ter verduidelijking hiervan wordt het figuur nader toegelicht.

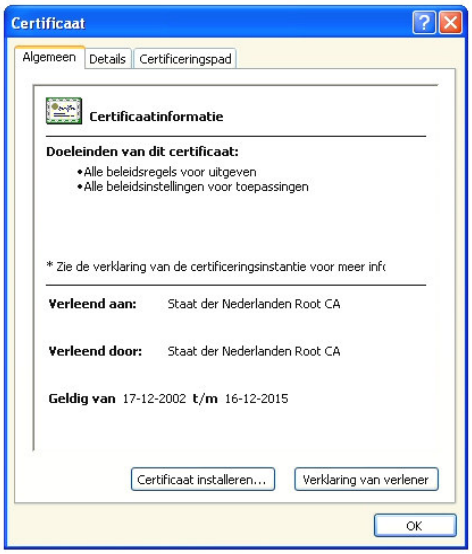
1. Een gebruiker A schrijft een brief en "ondertekent" deze met behulp van zijn privé handtekeningcertificaat. Dit gebeurt dat door een hashwaarde van de brief te berekenen, deze waarde met de privé handtekeningcertificaat te vercijferen en de extra informatie toe te voegen aan de brief.
2. Vervolgens haalt gebruiker A de publieke vertrouwelijkheidcertificaat van gebruiker B op. Met behulp van deze sleutel vercijfert gebruiker A de door hem ondertekende de brief.
3. De brief en de publieke handtekeningcertificaat worden naar gebruiker B verzonden. Gebruiker B weet op zijn beurt zeker dat de brief door gebruiker A is geschreven door de publieke handtekeningcertificaat te gebruiken.
4. Gebruiker B ontvangt de vercijferde brief en de publieke handtekeningcertificaat. Deze gebruiker zal door de inhoud van de vercijferde brief met behulp van zijn privé vertrouwelijkheidcertificaat alleen in staat zijn de brief te decoderen. Door de PKI-techniek weet gebruiker A vervolgens zeker dat alleen gebruiker B, met behulp van zijn privé vertrouwenscertificaat, de brief kan lezen.
5. Tenslotte kan Gebruiker B nagaan of de brief ook daadwerkelijk van de hand van Gebruiker A afkomstig is. Gebruiker B kan dit verifiëren met behulp van de publieke handtekeningcertificaat van gebruiker A. Wanneer de brief in zijn geheel is gedecodeerd is onomstotelijk bewezen dat de brief in ongewijzigde staat is ontvangen en afkomstig is van de juiste gebruiker.

6.2.4 Secure Socket Layer (SSL) en Transport Layer Security (TLS)

Om veilige en betrouwbare internetverbindingen te garanderen maakt de zorginfrastructuur gebruik van een SSL- en TLS-internetverbinding. SSL en TLS kan in combinatie met PKI en de daarbij behorende certificaten gebruikt worden om zowel de server als de client te identificeren en te authenticeren en het dataverkeer daardoor te beveiligen. Middels deze techniek kan men voorkomen dat gebruikers worden geconfronteerd met namaaksites of diefstal van gevoelige informatie door afluisteren van data dat over het toekomstige netwerk zal worden verzonden.

Door gebruik te maken van een SSL-servercertificaat wordt een “unieke zegel” aan een browser toegevoegd dat gebruikers kunnen aanklikken (figuur 6.4). SSL-servercertificaten bieden functies als:

- Garanderen van de identiteit van een site,
- Zorgdragen voor een 'beveiligde verbinding' tussen de bezoeker en website,
- Het stamcertificaat van de Staat der Nederlanden is opgenomen in webbrowsers. Hierdoor hoeven gebruikers geen extra handelingen uit te voeren om te kunnen verifiëren dat overheidssites betrouwbaar zijn.



Figuur 6.4: Een SSL-servercertificaat [WEBMIC]

Een SSL-servercertificaat binnen PKIO kan worden ingezet om de gegevens van een gebruiker te beschermen. Men wil er immers zeker van zijn dat gegevens worden opgehaald bij de juiste bron en niet van een malafide server. Identificatie en authenticatie van systemen en zorgverleners middels SSL-servercertificaat is hiervoor een goede oplossing.

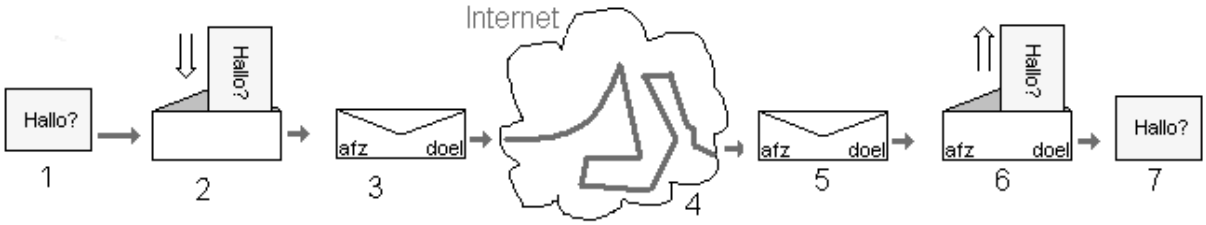
6.2.5 Virtual Private Network

Naast SSL en PKI wordt er ook gebruik gemaakt van een Virtual Private Network (VPN) communicatie-verbinding tussen GBZ en LSP.

Met VPN wordt het mogelijk om op een veilige manier systemen met elkaar belangrijke informatie uit te wisselen via een onbetrouwbare verbinding. Volgens [FER98] is een VPN: “A communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis”. Met behulp van VPN wordt het risico dat onbevoegden of kwaadwillende de communicatie inzien en/of manipuleren aanzienlijke beperkt.

Een normale verbinding

Bij een normale verbinding met het internet wordt een verbinding met het internet tot stand gebracht via pakketjes die via het internet worden verstuurd. Deze pakketjes hebben de vrije keuze om elke route over het internet te nemen, hebben het doel om op de vooraf bepaalde plek bezorgd te worden waar de verzender opdracht voor heeft gegeven.



Figuur 6.5: Versturen van informatie via het internet

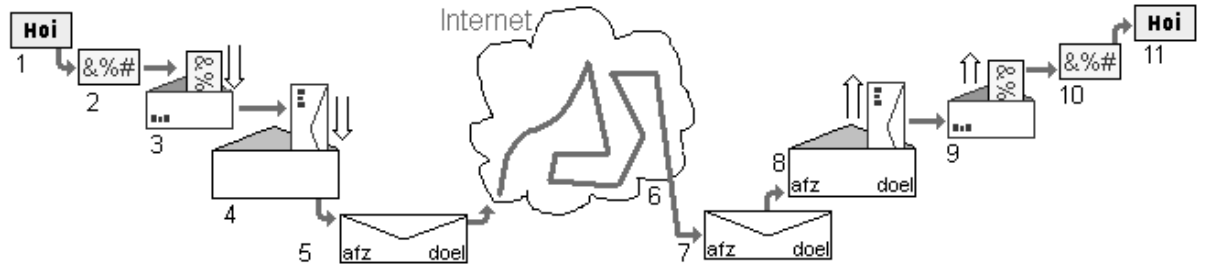
De stappen die genomen moeten worden om informatie via het internet te verzenden gaat als volgt (figuur 6.5):

1. De gegevens worden opgesteld door de verzender,
2. De gegevens post men in een "envelop",
3. Deze envelop wordt door de verzender voorzien van een afzender en de uiteindelijke bestemming,
4. Wanneer de envelop door de verzender wordt verzonden, reist deze over het internet via allerlei wegen richting de afzender. Er is geen vooraf opgestelde routebeschrijving,
5. De envelop komt (onder normale omstandigheden) aan bij de geadresseerde die op de envelop staat beschreven,
6. De geadresseerde opent de envelop en ziet de afkomst,
7. De geadresseerde leest de gegevens.

Een VPN verbinding

Het bovenstaande principe is vanwege het ontbreken van enig beveiliging en controle voor, tijdens en na het versturen niet gegarandeerd veilig. Met een beetje technische kennis en de nodige middelen is het onderscheppen van privacy- en systeemgevoelige informatie mogelijk. Dit potentieel gevaar versterkt doordat een bericht op het internet via diverse knooppunten wordt verzonden waardoor de kans op dat het in handen komt van kwaadwillende groeit.

Om de kans op bovenstaande te beperken is het inzetten van VPN een goede aanvulling. Figuur 6.6 geeft enig inzicht in de werking van VPN.



Figuur 6.6: Versturen van informatie via het internet met een VPN-tunnel

De stappen:

1. De gegevens worden opgesteld door de verzender,
2. De gegevens worden met een beveiligingssleutel veranderd in geheimschrift,
3. De gegevens worden in een geadresseerde gecodeerde envelop gestopt,
4. Deze extra envelop wordt in een normale enveloppe gedaan,
5. De normale envelop wordt voorzien van normale adresgegevens,
6. De normale envelop reist over het internet naar zijn bestemming toe,
7. De normale envelop komt aan op de plaats van bestemming,
8. Bij de bestemming aangekomen wordt de normale envelop uitgepakt,
9. De geadresseerde herkent de VPN envelop en controleert de afzender. Als deze klopt weet de geadresseerde zeker dat de afzender is wie hij zegt dat hij is,
10. Het geheimschrift wordt ontcijferd met de bij de geadresseerde bekende sleutel,
11. De gegevens worden gelezen.

6.2.6 Autorisatieprofiel en autorisatieprotocol

De uitwisseling van informatie in de zorg is alleen toegestaan als de bescherming van de privacy van de patiënt is gewaarborgd. Om de privacy van de patiënt te kunnen beschermen is een autorisatiestructuur ingericht waarin expliciet regels en procedures voor toegang tot een informatie en systeemonderdelen van het LSP zijn vastgelegd.

Voor toegang dient de zorgverlener dan ook te beschikken over een uniek autorisatieprofiel en autorisatieprotocol. Met een dergelijk profiel wordt via elektronische wijze gecontroleerd welke gegevens beschikbaar mogen worden gesteld aan personen op basis van hun functie.

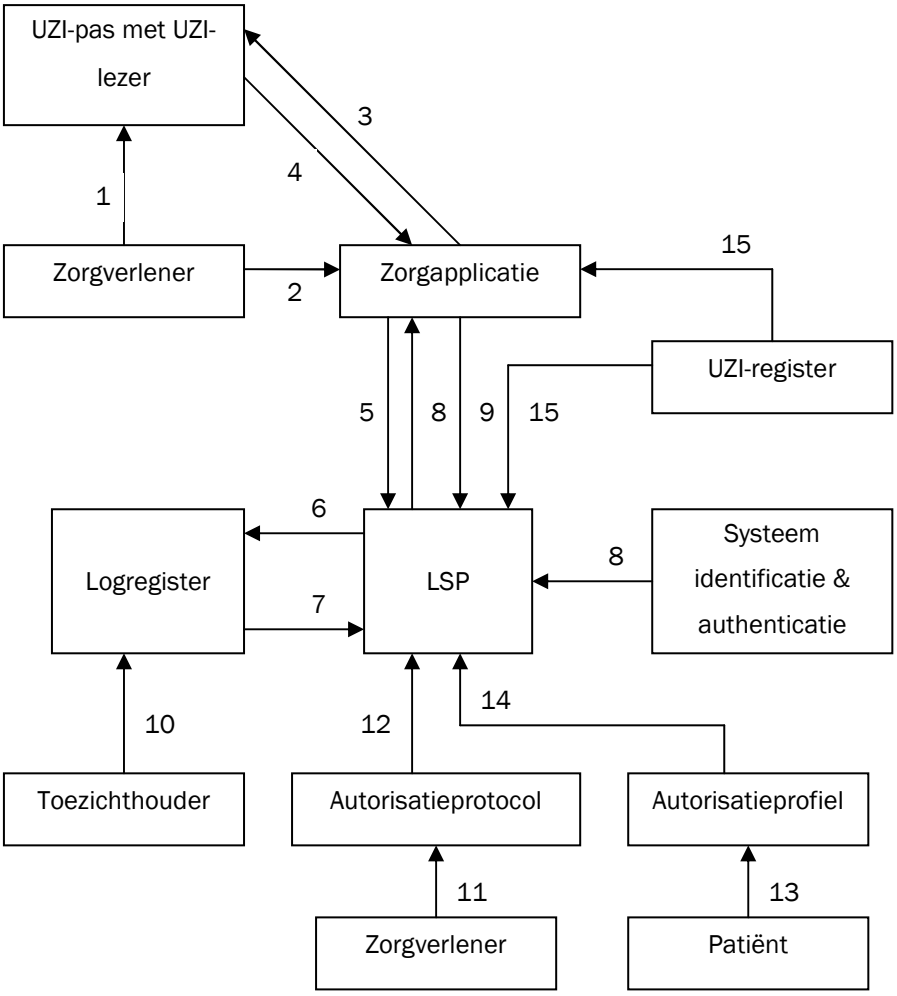
In de huidige situatie geschiedt deze controle veelal handmatig. Echter, in een geautomatiseerde omgeving is dat niet wenselijk en zelfs onmogelijk, vanwege de grote hoeveelheden verwerkingen. De winst van de elektronische zorginfrastructuur zal hierdoor teniet worden gedaan. De vragende zorgverlener zal immers nooit direct antwoord krijgen van de verantwoordelijke zorgverlener als deze niet bereikbaar is of de patiënt nog om toestemming gevraagd moet worden of deze zorgverlener zijn gegevens mag in zien. Het geautomatiseerd controleren wordt mogelijk door gebruik te maken van een autorisatieprotocol waarin is vastgelegd welke soort patiëntgegevens voor welke functies van zorgverleners beschikbaar zijn. Daarnaast bevat het profiel een bevestiging van de patiënt dat deze akkoord gaat met het digitaal uitwisselen van zijn gegevens. Tevens kan hij hiermee beperkingen toekennen aan zijn informatie waardoor deze niet of beperkt is in te zien of op te halen.

6.3 Toegang tot het LSP

De verschillende technieken en de voorgestelde infrastructuur zullen uiteindelijk voor moeten zorgen dat de zorgverleners toegang tot het LSP en de patiëntinformatie kan krijgen. Op basis van de NICTIZ specificatie is getracht deze toegangsprocedure reconstrueren. Helaas worden deze procedures niet vrijgegeven vanwege veiligheidsoverwegingen en kan de procedure daarom afwijken van de werkelijkheid. De toegangsprocedures kunnen er als volgt uit zien (figuur 6.7):

1. De zorgverlener stopt zijn UZI-pas in de UZI-paslezer. De paslezer dient ervoor om gegevens die op de pas staan uit te lezen op het moment dat hierom wordt gevraagd.
2. De zorgverlener die gegevens van een patiënt wenst op te vragen zal via een applicatie op de pc of via het intranet toegang tot het LSP moeten krijgen. De applicatie zal de gebruiker vragen om zijn inloggegevens om zo de zorgverlener te identificeren en authenticeren.
3. Nadat de zorgverlener heeft laten weten dat hij toegang wil, zal de zorgapplicatie enkele gegevens gaan verifiëren door middel van het opvragen van gegevens die op de UZI-pas staan. Deze communicatie tussen applicatie en paslezer verloopt overigens via een PKI versleuteling.
4. De gevraagde gegevens zullen vervolgens desbetreffend worden verzonden naar de applicatie welke de bevestiging heeft gekregen dat de ingevoerde gegevens overeenkomen met de gegevens op de UZI-pas.
5. Via een beveiligde verbinding worden identificatie en authenticatie gecontroleerd en al dan niet toegang tot het LSP en de verwijsindex gegeven, waarbij de gebruiker er vanuit kan gaan dat hij met de correcte LSP is verbonden.
6. Bij elke vraag om informatie vanuit de buitenwereld zal het LSP een logactie wegschrijven in het logregister. Hierdoor kan op een later moment achterhaald worden wie welke informatie heeft opgevraagd en dus alle communicatie in de gaten worden gehouden door de toezichthouder.
7. Indien noodzakelijk kan het LSP gewaarschuwd worden door het logregister of de toezichthouder en bijvoorbeeld een zorgverlener of systeem afgekoppeld worden van het LSP.
8. Door het toepassen van een eigen hardwarematige identificatie token (De UZI-pas) kan het LSP door de gebruiker worden geïdentificeerd en geauthenticeerd, waardoor deze weet dat het LSP betrouwbaar is.
9. De zorgapplicatie krijgt hierna daadwerkelijk toegang tot het LSP. De betreffende zorgverlener zal dan met de zorgapplicatie onder andere een zoekmogelijkheid aangeboden krijgen om daarmee naar verwijzingen van een patiënt te zoeken die zijn opgenomen in de verwijsindex.
10. De toezichthouder zal bij onrechtmatig gebruik van patiëntgegevens actie kunnen ondernemen tegen de in overtreding zijnde zorgverlener of gebruiker. Het LSP kan hiervan op de hoogte worden gesteld en deze zorgverlener de toegang tot het LSP (deels) ontzeggen.
11. De zorgverleners hebben in het autorisatieprotocol vastgelegd welke gegevens voor welke functies van zorgverleners beschikbaar zijn.
12. Het autorisatieprotocol zal bij elke binnenkomende actie van een zorgverlener controleren of de betreffende zorgverlener op basis van zijn functie toegang mag hebben tot de gevraagde gegevens.

13. De patiënt heeft in een autorisatieprofiel vastgelegd welke gegevens hij openbaar en dus toegankelijk wenst te maken op het LSP voor de zorgverleners. De patiënt zal in de nabije toekomst dit vanuit huis kunnen instellen. Dit zal door de verantwoordelijke zorgverlener in overeenstemming met de patiënt dienen te gebeuren.
14. Het autorisatieprofiel controleert elke binnenkomende actie van een zorgverlener aan de hand van de opgestelde regels van de betreffende patiënt. Door deze regels in acht te nemen worden de gevraagde patiëntgegevens al dan niet vrij gegeven en verzonden aan de vragende zorgverlener.
15. De identiteit kan aan de hand van certificaten gecontroleerd worden. Het UZI-register beheert deze certificaten. De betreffende certificaten bevinden zich op de UZI-pas en kunnen bij communicatie tussen zorgverlener en LSP gecontroleerd worden. Het LSP kan op haar beurt de informatie van het UZI-register opvragen en controleren of de gegevens overeenkomen met de gegevens die de zorgapplicatie heeft verzonden naar het LSP.



Figuur 6.7: De LSP toegangsprocedure voor een zorgverlener

6.4 Conclusie

De toegangsprocedure is een belangrijke schakel in het informatiesysteem. Deze zorgt ervoor dat alleen rechtmatige gebruikers de informatie die zij nodig hebben kunnen benaderen en handelingen kunnen uitvoeren waarvoor zij bevoegd zijn. Het toegangsproces waar alleen bevoegde personen normaliter door heen kunnen komen vindt voornamelijk plaats door de inzet van technische middelen.

Door de inzet van middelen en technieken als een UZI-pas, PKI, SSL, Certificaten en VPN, wil het NICTIZ een maximale beveiliging creëren. Hoewel deze middelen en technieken wel enigszins bijdraagt aan een verhoogde beveiliging bevatten ook deze zwakke punten waar een kwaadwillend persoon misbruik van zou kunnen maken. Daarnaast helpt de complexiteit van het systeem niet mee. Hoe groter die wordt de groter de kans dat er problemen ontstaan.

Dat PKI niet veilig is wordt in het artikel [ELL00] duidelijk, hierin worden door Bruce Schneier tien risico's van PKI aangedragen. In een interview [WEBCVI] geeft diezelfde Bruce Schneier aan dat PKI behalve het ondertekenen van een document met een privé-sleutel niet voorziet in of die persoon met de sleutel dat zelf heeft gedaan, welk proces het ondertekenen heeft doorgemaakt, deze persoon het document begreep toen deze door hem werd ondertekend, deze persoon het document wel heeft gezien of dat de computer het document heeft ondertekend zonder toestemming van de persoon en of de identiteit die aan de privé-sleutel verbonden is juist is?

Ook zal met SSL geen veiligheidsgarantie kunnen worden afgegeven. [KO006] beschrijft onder meer dat SSL juist schijnveiligheid in de hand werkt waardoor uiteindelijk niet kan worden gegarandeerd dat de verbinding die is opgezet ook daadwerkelijk met de bedoelde bron is verbonden. Ook [ELL00] toont aan dat SSL, PKI en certificaten geen 100% garantie bieden voor een veilige communicatie. Hoewel deze technieken proberen dat mogelijk te maken kan de veiligheid sterk worden verbeterd door het realiseren van een besloten zorgnetwerk. Door op dit netwerk alleen gecertificeerde zorgsystemen toe te laten, profiteert men van het feit dat de systemen voldoen aan de minimaal gestelde eisen, maar ook dat buitenstaanders geen toegang hebben tot dit netwerk. De betrouwbaarheid en veiligheid wordt aanzienlijk verbeterd en de kans op problemen van buitenaf verminderd.

Naast het afsluiten van systemen en netwerken van de buitenwereld is controle aan de poort ook een essentieel onderdeel van de beveiliging van een informatiesysteem. Daarnaast is het noodzakelijk om controle uit te voeren op de acties die worden uitgevoerd op het LSP systeem. Zowel gedurende het toegangsproces als daarna. In hoofdstuk 7 zal nader in worden gegaan op logging als controlemethode.

"Computerized patient data is bad for privacy.
But it's good for just about everything else,
so it's inevitable."

Bruce Schneier

7. Hoe verloopt de logprocedure?

7.1 Inleiding

Wanneer een zorgverlener eenmaal toegang heeft tot het LSP worden acties die hij op het systeem uitvoert vastgelegd. Met behulp van de opgeslagen gegevens in de logs kan de beheerder onder andere controleren of de uitgevoerde actie rechtmatig was, bekijken of het systeem correct werkt, onregelmatigheden opsporen en na gaan of er ook daadwerkelijk patiëntgegevens zijn opgevraagd. Om meer duidelijkheid te krijgen over het loggen van gegevens op het LSP zal in dit hoofdstuk nader worden ingegaan op het principe van loggen, de momenten van loggen en de problematiek die men kan verwachten bij de massale opslag van deze data.

7.2 Doel van een logfile

7.2.1 Wat is Logging

Loggen in de digitale wereld is: "het vastleggen van informatie over relevante gebeurtenissen binnen een informatiesysteem" [RID98]. En het heeft als doel: Het controleren op naleving van het beveiligingsbeleid van de organisatie en de geldende normen, mede ten behoeve van het voorkomen van schendingen van wettelijke of contractuele beveiligingsvereisten [OVE99]. Maar loggen heeft nog meer voor ogen, namelijk de bevordering van de werking van het zorgsysteem en van het herstel van schade. Daarom is het belangrijk dat de logbestanden continue worden gecontroleerd en geanalyseerd om onjuistheden te signaleren en indien noodzakelijk aan te kunnen pakken.

In organisaties kan loggen gebruikt worden om uitgevoerde acties vast te leggen. Met deze gegevens kan men zien welke situaties zich hebben voorgedaan op het moment van loggen alsmede wie welke acties heeft uitgevoerd. Dit is een goed hulpmiddel om zowel de dataflow in de gaten te houden, problemen op te sporen en controle mogelijk te maken. Een systeembeheerder zonder logfiles is in feite stuurloos, net als een kapitein zonder logboek.

Een logbestand is interessant als deze de onderstaande informatie bevat [BUR04]:

- Wie: een volledige identificatie van de persoon die bepaalde data heeft bekeken of gewijzigd,
- Waar: een logregel laat zien met welke applicatie en methode er is gebruikt om bepaalde data te bekijken,
- Wanneer: een log dient voorzien te zijn van een betrouwbare datum en tijd,
- Wat: een volledige lijst waarin vermeld is welke data is opgevraagd en gewijzigd,
- Waarom: hoe de data is opgevraagd.

Zonder deze criteria in acht te nemen heeft een logbestand geen enkel nut of functie.

7.2.2 Loggen bij het LSP

Bij het LSP hebben de logfiles voornamelijk een controlerende functie. Beheerders kunnen daarmee nagaan of een gebruiker conform de regels gebruik heeft gemaakt van het LSP. Acties die door zorgverleners zijn uitgevoerd worden gelogd en zijn vervolgens opvraagbaar door beheerders en controleurs. Aan de hand van deze opgeslagen informatie kan achteraf onder andere worden bepaald of de actie om patiëntgegevens gerechtvaardigd was en daarbij geen regels zijn geschonden.

Naast een controlerende functie kunnen logbestanden ook fungeren voor het ontdekken van systeemproblemen. Een logbestand dient dan ter identificatie welke condities er voor heeft gezorgd dat het systeem in een bepaalde toestand verkeert. Op deze wijze kan een beheerder ervoor zorgen dat problemen in het systeem kunnen worden verholpen.

Ook het aantonen dat een zorgaanbieder niet gebruik heeft gemaakt van de beschikbare patiëntinformatie kan met logging worden bereikt. Een zorgaanbieder kan namelijk aansprakelijk worden gesteld wanneer hij heeft nagelaten gegevens via het LSP op te vragen. In [NIC05a] wordt gesteld dat: de toezichthouders door de rechter kunnen worden gevraagd de nagelaten opvraag te doen, waarbij de omstandigheden gereconstrueerd moeten worden zoals die waren tijdens de betwiste behandeling. Op deze wijze zou kunnen worden bepaald of de zorgaanbieder door het niet opvragen van gegevens, bepaalde cruciale patiëntinformatie heeft gemist. In dat geval geldt de logfile als bewijsmateriaal en is het van groot belang dat deze bestanden worden beveiligd waardoor verwijderen of overschrijven van deze gegevens niet mogelijk is.

7.2.3 Logmomenten

Een logactie op het zorgsysteem vindt op verschillende momenten plaats. In figuur 7.1 wordt aangetoond hoe logacties plaats vinden. De momenten zijn als volgt:

a) Een gebruiker logt via zijn zorgapplicatie in op het LSP.
b) De actie van de gebruiker zal leiden tot een actie op het LSP waarbij deze de identificatie, authenticatie en autorisatieprocedures uitvoert en al dan niet goedkeurt. De gemaakte acties worden geschreven in het logbestand.

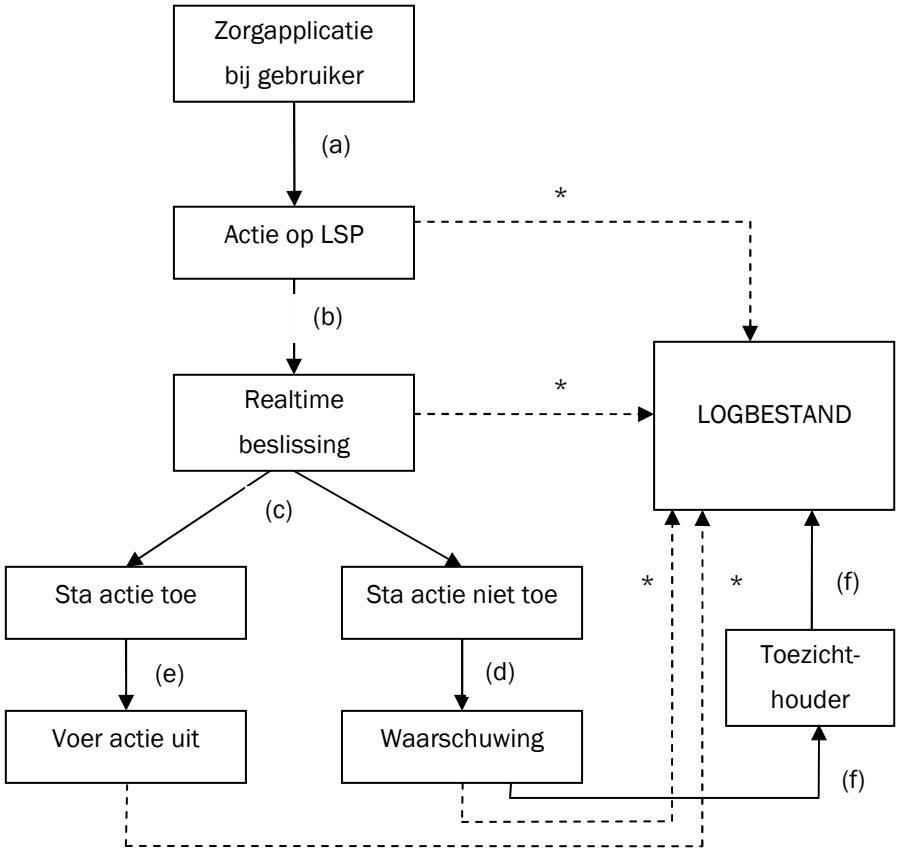
c) Er zal vervolgens, realtime, een beslissing gemaakt worden of de gegevens overeenkomen die de gebruiker heeft ingevoerd en of hij op basis daarvan toegang krijgt tot de LSP. Indien er onrechtmatige gegevens zijn ingevoerd of het LSP ontdekt dat er onrechtmatige dingen zich voltrekken zal deze de gemaakte actie niet toestaan en een waarschuwing afgeven (d). Indien de gegevens wel kloppen wordt de actie toegestaan en wordt de actie uitgevoerd (e). Ook hier geldt dat van de beslissing een actie in het logbestand wordt bijgehouden.

d) Een waarschuwing wordt afgegeven richting de toezichthouder die vervolgens gaat kijken in het logbestand.

e) Tevens zal er een actie worden geschreven in het logbestand met daarin de gegevens van de actie.

f) Indien de actie is toegestaan zal de gebruiker toegang krijgen tot de LSP of het LSP zal de gevraagde actie uitvoeren. Zoals het ophalen van gegevens in de verwijsindex of ophalen van patiëntgegevens.

* Actie wordt weggeschreven in het logbestand.

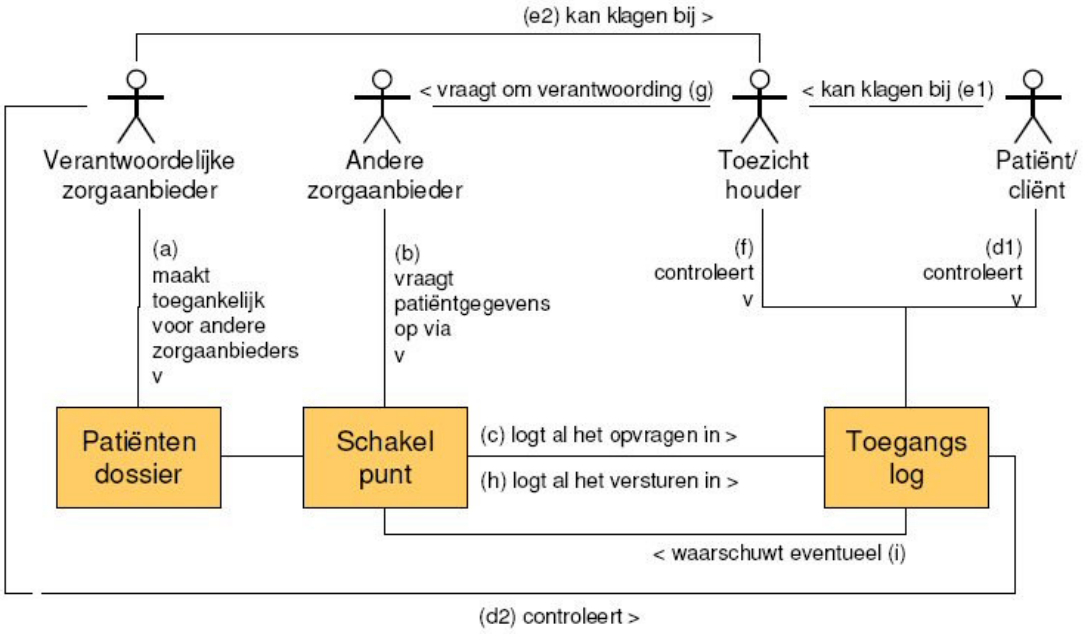


Figuur 7.1: Wegschrijfmomenten van het LSP naar het logbestand

7.2.4 Logfiles bij zoeken naar patiëntgegevens

Wanneer een zorgverlener eenmaal is toegelaten tot het LSP kan de zorgverlener op zoek gaan naar patiëntgegevens. De logfiles worden dan een aantal keren benaderd. Een uiteenzetting is hieronder beschreven en in figuur 7.2 te bekijken [NIC05a]:

a) Een verantwoordelijke zorgaanbieder maakt zijn patiëntendossiers toegankelijk voor andere zorgaanbieders, op voorwaarde dat die daarvan geen misbruik maken. Misbruik wordt afgevangen doordat een zorgaanbieder moet tekenen dat hij zich aan de regels houdt. Met controle doormiddel van logs wordt hierop toegezien.
b) Een andere zorgaanbieder vraagt patiëntgegevens op via het schakelpunt. Hierbij dient hij de reden van opvragen aan te geven.
c) Het schakelpunt houdt bij in een toegangslog welke gegevens er door de zorgaanbieder zijn opgevraagd.
d) Een patiënt of verantwoordelijke zorgaanbieder kan de toegangslog raadplegen dat bij een patiëntdossier hoort om te controleren wie er toegang hebben gehad tot de betreffende dossier,
e) Een patiënt of verantwoordelijke zorgaanbieder die meent dat andere zorgaanbieders onnodig toegang hebben gehad, kan daarover klagen bij de toezichthouder.
f) De toezichthouder kan na klachten en op eigen initiatief het toegangslogs raadplegen om te verifiëren of zorgaanbieders inderdaad onbevoegd toegang hebben gehad tot patiëntgegevens.
g) De toezichthouder zal zonodig de desbetreffende zorgaanbieders om verantwoording vragen en kan in een uiterst geval de zorgaanbieder laten uitsluiten of juridische stappen ondernemen.
h) Het versturen van patiëntgegevens wordt gelogd waardoor patiënt en toezichthouder volledig zicht kunnen hebben op alle uitwisselingen.
i) Het toegangslog zal in geval van verdachte patronen een waarschuwing uitgeven aan de toezichthouder en LSP. Deze kunnen vervolgens een gepaste actie ondernemen.



Figuur 7.2: Verwerken logactie wanneer patiëntinformatie wordt opgevraagd [NIC05a]

7.3 Problematiek bij logfiles

7.3.1 Bewaren van logs

Logging wordt gebruikt om informatie op te slaan aangaande activiteiten die gebruikers op een systeem uitvoeren en daardoor een betere en veilige dienst geleverd kan worden. In sommige gevallen kan de privacy hierbij in het geding komen. De logfiles zullen namelijk persoonsgegevens bevatten welke vanuit twee oogpunten beschermd moeten worden. Ten eerste zullen gebruikers en systeembeheerders de gegevens dienen te respecteren en niet te misbruiken. Ten tweede moet voorkomen worden dat dergelijke gegevens op straat belanden. Daarbij is in artikel 8 van het Europese Verdrag van de rechten van de mens opgenomen dat loggegevens niet langer mogen worden bewaard dan noodzakelijk is. In het geval van de zorginfrastructuur zullen logbestanden voor een periode van minimaal vijftien jaar bewaard worden om terug te kunnen zien wie welke actie heeft uitgevoerd en welke informatie is opgevraagd.

Door de vermeende opslag van acties die uitgevoerd worden zullen de logfiles blijven groeien. Het probleem ontstaat dan dat er flinke opslag capaciteit ingericht moet worden. Dit is te wijten aan het opslagbeleid dat men elke actie die zich op het LSP afspeelt voor lange periode wil vastleggen.

Rekenvoorbeeld

Volgens het [CBS06] blijkt dat in de periode 1981-2005 gemiddeld 70% van de patiënten elk jaar minimaal één keer in contact treedt met zijn huisarts. Wanneer 16 miljoen patiënten in een systeem beschikbaar zijn zou dat resulteren in minimaal 11,2 miljoen opvragingen via het LSP. Volgens de procedure in figuur 6.1 zou in een gemiddelde zoekactie minimaal vijf logacties plaats hebben. Dat betekent minimaal 56 miljoen logacties per jaar. Tel daarbij op dat een patiënt meerdere keren per jaar een huisarts en/of specialist bezoekt alsmede de administratieve en beheersprocedures ook uitgevoerd moet worden en het wordt duidelijk dat de opslag maar ook het beheer van hoog niveau moet zijn.

7.3.2 Beheren van logfiles

Bovenstaand voorbeeld maak duidelijk dat loggen veel dataverkeer genereert, grote opslagbehoeftes met zich meebrengt, de infrastructuur negatief zal beïnvloeden door de constante stroom van logacties én controlemogelijkheden van het logboek zelf aanzienlijk zal bemoeilijken.

Als toezichthouder is het ondoenlijk om handmatig logfiles door te gaan zoeken op onrechtmatigheden. Termen als “auditing” en “monitoring” doen hier hun intrede. Hierbij is noodzakelijk dat men alleen zaken logt die van belang zijn en wanneer aan bepaalde voorwaarden wordt voldaan, alarm wordt geslagen richting de beheerder waarop deze actie kan ondernemen. In dit onderzoek wordt er van uitgegaan dat dit niet in het LSP-infrastructuur is geregeld, omdat hierover niets is vermeld in de NICTIZ documentatie die bepalend zijn voor het creëren van de zorginfrastructuur.

De grote hoeveelheden data die door het loggen zullen worden gegenereerd zijn niet mis. Het is dus van groot belang dat de beheerders alleen gegevens tot zich krijgen die alarmerend zijn voor de gebruiker, de gegevens of het systeem. Immers, de beheerder kan men niet overspoelen met alle informatie die in de logs worden opgeslagen. Hij moet wel de controle hierover kunnen blijven uitvoeren waarbij gegarandeerd moet zijn dat alleen een bevoegde beheerder deze gegevens kan benaderen.

IDS en IPS

Indien een kwaadwillende succesvol het LSP is binnen getreden, zullen zijn acties worden gelogd. Om te voorkomen dat hij zal worden opgemerkt, zal hij proberen de inhoud van de logbestanden te wijzigen. Wanneer de beheerder, al dan niet getriggerd door een melding, op zoek gaat naar de betreffende fout, kan deze door een kwaadwillende zijn gewijzigd waardoor het lijkt alsof er niets aan de hand is. Een kwaadwillende gaat vrij uit en de beheerder weet niet waar het probleem zich heeft voorgedaan. Met als gevolg dat de kwaadwillende gegevens onopgemerkt kan benaderen en vervolgens de logacties kan herschrijven.

Een Intrusion Detection System (IDS) detecteert handelingen van een onbevoegde gebruiker of systeem op het LSP en zou de toezichthouder hier real-time melding van kunnen geven. Klassieke taken van een IDS-systeem zijn het volgen en analyseren van activiteiten van gebruikers en systemen, nakijken van kwetsbaarheden, aanvals- en securitypatronen te herkennen, net als inbreuken door gebruikers van security policies. Een IDS kan gezien worden als een firewall met uitgebreidere mogelijkheden.

Een Intrusion Prevention System (IPS) kan de IDS uitstekend ondersteunen. Een IPS probeert met behulp van patronen en policies gevaar of ongewenste pogingen tot informatie liefst vooraf gedefinieerd nog voordat ze het LSP kunnen bereiken te onderscheppen. Een IPS is een systeem wat proactief mee kan werken het LSP veilig te houden en de toezichthouders veel zorgen uit handen kan nemen. In geval van detectie zal een actie conform de opgestelde policies moeten worden afgehandeld. Dit kan door het direct melden van een probleem aan de toezichthouder en het loggen van de genomen acties. Een IPS-systeem kan zich zowel ophouden in het netwerk als op de host. Voor het LSP zal een combinatie hiervoor moeten worden gebruikt. Een IPS dat geïmplementeerd is op het netwerk heeft dan als taak datapakketten te analyseren en verdachte pakketten nog voordat ze het LSP kunnen bereiken tegen te houden. Een IPS dat op de host is geïnstalleerd en daar zal dienen om kwetsbaarheden op servers te counteren. Ze kunnen een policy opleggen en toepassen, die gebaseerd is op vooraf vastgelegde regels.

Door het gebruik van IDS en IPS zou het mogelijk kunnen worden om een zoektocht in logsystemen aanmerkelijk te verminderen. Gedetecteerde problemen kunnen in een aparte logfile worden weggeschreven. Waardoor de toezichthouder zijn werkzaamheden makkelijker kan overzien dan zonder het gebruik van ondersteunende systemen.

7.4 Conclusie

Logfiles bevat belangrijke informatie over het gebruik van de patiëntendossiers door de gebruikers die hebben plaats gevonden op het LSP. Elke actie die op het LSP wordt uitgevoerd wordt opgeslagen in de logfiles om op een later moment te kunnen achterhalen welke acties een zorgverlener heeft uitgevoerd en onder welke omstandigheden. Dit onuitwisbare geheugen kan op verschillende wijze worden ingezet om het systeem te verbeteren en de gebruikers met hun uitgevoerde acties naderhand te kunnen controleren. Hoewel logging een aantal voordelen heeft, kent een groot loggingsysteem ook problemen. Zo is het beheer ervan niet eenvoudig en dient in dit geval ook gedacht te worden aan hoe men alle logs gaat opslaan. En dan hebben we het niet alleen over fysieke opslag, maar ook over het intelligent opslaan van de logs zodat ze eenvoudig zijn te doorzoeken.

Voor de opslagcapaciteit is aanschaf van kwalitatief snelle en goede servers een vereiste. De techniek die men gebruikt om de logs te kunnen doorspitten opzoek naar de juiste gegevens vergt slimme applicaties en behendige beheerders die op de hoogte zijn van de mogelijkheden van het systeem. De applicaties zullen voornamelijk op de achtergrond constant moeten meedraaien en controles moeten uitvoeren op basis van vooraf vastgelegde regels. Deze applicaties zullen voornamelijk signalerend moeten optreden en de beheerders moeten waarschuwen wanneer dat nodig wordt geacht.

In tegenstelling tot wat men zou verwachten is er tot op heden nog niets bekend over hoe het NICTIZ het systeem rondom het loggen gaat oplossen.

"It's not possible to eliminate all threats."

Bob Small

8. Risicoanalyse van het LSP

8.1 Inleiding

Het staat vast dat kwaadwillenden zullen proberen het LSP aan te vallen en zo toegang willen krijgen tot de infrastructuur. Welke mogelijkheden een kwaadwillende heeft om toegang te verkrijgen tot het LSP zonder hierbij rechtmatig de beschikking te hebben over de twee autorisatiemiddelen, de UZI-pas en het bijbehorende wachtwoord, dat wordt in dit hoofdstuk met behulp van de risicoanalyse in kaart gebracht.

Zoals reeds in figuur 4.2 naar voren is gekomen, zijn er een aantal opeenvolgende activiteiten die er voor moet zorgen dat risico's worden weggenomen of verlaagd. Met behulp van de attack tree methode [SCH00] zullen in eerste instantie de mogelijkheden die een kwaadwillende heeft om het LSP te betreden worden geïdentificeerd. Per zogenaamde attack zal vervolgens een reële kans en omvangsfactor van de schade worden toegekend wanneer de attack zich voordoet. Tevens zal per attack het effect met betrekking tot de CIA-aspecten worden bepaald. Tezamen levert dit een uiteindelijk indexfactor per geïdentificeerde risico op. Met behulp met deze indexfactor kan de urgentie bepaald worden dat de risico weggenomen moet worden omdat hierdoor het LSP en dus de gegevens gevaar dreigen te lopen. Per geïdentificeerde risico zal ook een aantal maatregelen worden gegeven om zo het risico weg te nemen of zo klein mogelijk te maken.

8.2 Beweegredenen aanval op het LSP

De in dit onderzoek opgestelde attack tree brengt de mogelijkheden in kaart om toegang te verkrijgen tot het LSP via methodes anders dan het NICTIZ heeft beschreven. Deze attack tree kan van belang zijn om nieuwe inzichten te krijgen in en heeft eveneens tot doel om de betrouwbaarheid en de beveiliging van het LSP te verbeteren.

Het onderzoeken hoe toegang kan worden verkregen tot het LSP is een interessant doel om te onderzoeken. Dit vanwege het feit dat informatie die toegankelijk wordt wanneer eenmaal toegang is verkregen voor verschillende partijen van grote waarde kan zijn. Enkele van die partijen en hun voordelen kunnen zijn:

- Een zorgverzekeraar; vanwege de zorggeschiedenis van zijn patiënten,
- Een werkgever; omdat hij graag wil vermijden een probleempatiënt aan te nemen,
- Een patiënt; omdat hij graag wil weten welke informatie er over hem bekend is,
- De veiligheidsexpert; om het zorgsysteem te testen en problemen boven tafel te krijgen,
- De scriptkiddies en crackers; om het zorgsysteem plat te leggen en hiermee aan te tonen hoe goed je bent,

- Commerciële bedrijven; om gericht informatie te versturen naar hun doelgroep,
- Derden; het verkopen van medische en persoonlijke gegevens aan iedereen die er interesse in heeft.

8.4 Toegang krijgen tot het LSP

8.4.1 Gemaakte keuzes

De attack trees zullen inzicht geven in de mogelijke dreigingen op het LSP. Om enige structuur te krijgen is de attack tree opgedeeld in een aantal niveaus. De verfijning heeft uiteindelijk geleid tot vijf niveaus: een logisch, een systeem, een fysiek, een informatie niveau en een niveau met onvoorzienbare attacks (zie figuur 8.1).

De attacks zijn gevonden door de literatuur erop na te slaan, door het internet af te speuren naar nieuwe, effectieve en veel gebruikte methodes alsmede door enige voorkennis op dit gebied van de auteur zelf. Deze mogelijkheden zijn vooral in de eerste lagen van elke attack tree terug te vinden. De daaronder gelegen subattacks zijn een gevolg en een verfijning van de mogelijkheden om het bovenliggende hoofddoel mogelijk te maken. Hoewel er vele attacks zijn opgenomen is het nooit mogelijk om alle attacks in een attack tree op te nemen. Daarvoor zijn er teveel mogelijkheden.

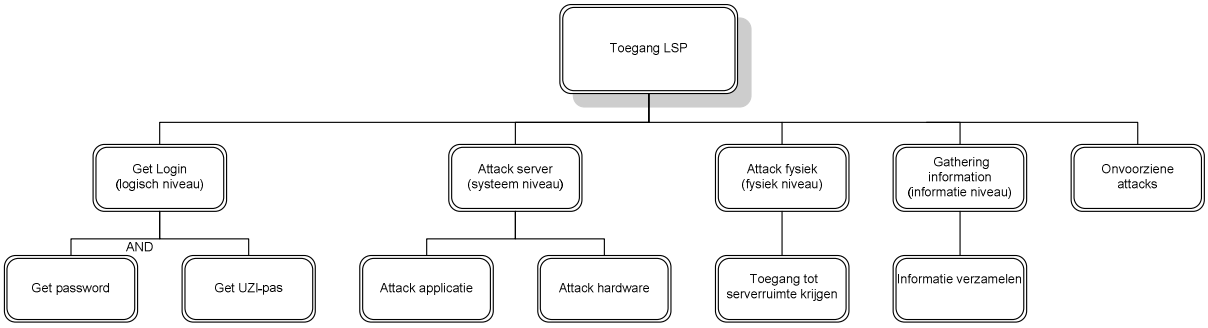
De attack trees in dit onderzoek zijn ook niet tot in detail beschreven. Veelal worden maximaal de eerste twee niveaus beschreven in de analyses. De onderliggende attacks zijn daarmee niet minder belangrijk, maar geven een te gedetailleerd beeld wat de leesbaarheid negatief beïnvloed. Daarnaast is de invloed op de uiteindelijke attack in de eerste laag zeer beperkt.

Gekozen is om de attack trees, anders dan de naam doet vermoeden, te tekenen als wortels. Normaliter kunnen “trees” niet in elkaar opgaan, maar bij wortels is dat wel mogelijk. De hiërarchie kan hierdoor minder snel duidelijk worden (zie figuren 8.10 en 8.11) omdat de wortels weer in elkaar opgaan of een laag kunnen omzeilen. Dit is te wijten dat enkele subattacks vaker in een attack tree voorkomen. Het gebruik van diezelfde subattack is volgens deze tekenmethode eenvoudiger. Tevens wordt er zo voor gezorgd de grote van de attack tree beperkt blijft en redundante informatie niet voorkomt. Natuurlijk wordt door deze aanpassing de feitelijke bedoeling en structuur enigszins aangetast waardoor het overzicht mogelijkerwijs wat onduidelijk wordt omdat lijnen naar onderliggende subattacks door elkaar lopen. Desondanks is dit de enige manier om een attack tree volgens deze tekenmethode qua omvang beperkt te houden.

Uiteindelijk zullen de gevonden attacks worden geclassificeerd door er een CIA-factor en risicofactor aan toe te kennen. Door deze factoren met elkaar te vermenigvuldigen ontstaat een uitslag waarmee bepaald kan worden welke prioriteit een attack heeft om te worden aangepakt. De CIA-factor is in een aantal gevallen voorzien van een extra score. Deze score geeft de hoogte van de betreffende factor aan wanneer aan een bepaalde voorwaarde wordt voldaan. Deze is te herkennen aan de haakjes om de toegekende score.

8.4.2 Structuur attack tree

Onderstaande attack tree (figuur 8.1) toont een vijftal niveaus met in ieder niveau eenzelfde categorie attacks waarmee men mogelijkerwijs toegang wil verschaffen tot het LSP.



Figuur 8.1: Attack tree met het hoofddoel en alle niveaus

De vijf niveaus zijn als volgt gedefinieerd:

- **Logisch niveau: 1. Get login**
  Niveau waarin attacks zich richten op het verkrijgen van toegang tot het LSP door het wachtwoord en de UZI-pas in bezit te krijgen zonder dat de aanvaller hiervoor bevoegdheden heeft.
- **Systeem niveau: 2. Attack server**
  Niveau dat zich kenmerkt doordat een aantal attacks hierin zijn verzameld waarmee getracht wordt toegang te krijgen tot het LSP door gebruik te maken van de mogelijkheden die de geïmplementeerde hardware of geïnstalleerde software een kwaadwillende kan bieden.
- **Fysiek niveau: 3. Attack fysiek**
  Met fysieke attacks wordt getracht om direct toegang te krijgen tot het LSP.
- **Fysiek niveau: 4. Gathering information**
  Kenmerkend voor dit niveau is dat een kwaadwillende probeert informatie te verzamelen of toegang tot bruikbare informatie te krijgen waarmee vervolgens, via nog niet genoemde wegen, deze toegang tot het LSP krijgt en zo belangrijke informatie kan onderscheppen.
- **Fysiek niveau: 5. Onvoorziene attacks**
  Onbekende attacks.

8.4.3 Structuur per subdoel

Per niveau zijn er een of meerdere attacks mogelijk. Voor de consistentie zal per attack een vaste beschrijving worden gegeven die bestaat uit de volgende onderdelen:

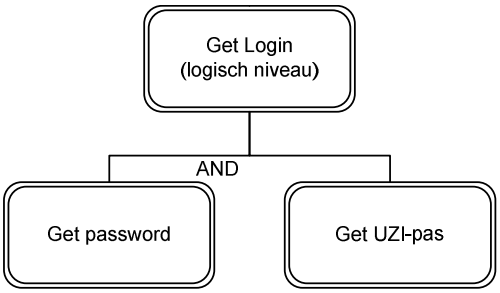
- **Dreigingen en gevolgen**: beschrijving van de attack, de daaruit voortvloeiende dreiging en de gevolgen die hieruit kan ontstaan voor het LSP.
- **Belang van bescherming**: waarom een dreiging moet worden weg genomen. Het belang van bescherming wordt verduidelijkt aan de hand van de hoogte van de risicofactor en de CIA-classificatie.
- **Risicofactor**: de kans dat het risico zich zou kunnen voordoen. De hoogte van deze kans wordt uitgedrukt in een score. Deze eerder voorgestelde risicofactor wordt bepaald door de kansfactor maal de omvangfactor. De kansfactor kan worden gezien als de kans dat de attack zich mogelijkerwijs voor zal doen. Met de omvangsfactor wordt bedoeld de grootte van de mogelijke schade aangericht door het succesvol uitvoeren van de genoemde attack. De kans alsmede de omvang variëren van score één tot en met drie. Risicofactor 1 staat voor vrijwel geen kans en op een verwaarloosbare omvang op schade. Risicofactor 3 daarentegen duidt op veel kans en een grote omvang op schade. Zowel de kans als de omvangscores zijn gebaseerd op schattingen.
- **CIA-classificatie**: de score van de C, I en A kan liggen tussen de 1 wat staat voor minimaal effect op het aspect en 3 wat staat voor een maximaal effect op het betreffende aspect.
    - De C staat voor Confidentiality (vertrouwelijkheid) wordt bedoeld dat een gegeven alleen te benaderen is door iemand die gerechtigd is het gegeven te benaderen.
    - De I staat voor Integrity (betrouwbaarheid) wat inhoudt of de informatie wel correct en volledig is.
    - De A staat voor Availability (beschikbaarheid) wat inhoudt of de gebruiker wel de gegevens kan inzien of bewerken op elke moment dat hem dit uitkomt.

  Net zoals bij de risicofactor zijn ook de scores schattingen.
- **Urgentie**: Op basis van de score van de risicofactor en de CIA-aspecten kan men schatten welke attacks “zeer noodzakelijk”, “noodzakelijk” en “niet noodzakelijk” zijn om te verhelpen. Een attack met een lagere urgentie hoeft niet direct te worden verholpen omdat verwacht wordt dat kans en/of schade van en door de attack geringer zijn geschat. In geval van een hoge urgentie is dat natuurlijk wel noodzakelijk.
- **Aanbevelingen**; beschrijving van de wijze waarop een dreiging mogelijkerwijs te niet kan worden gedaan of zo goed mogelijk kan worden ontzenuwd.

8.5 Logisch niveau: get login

8.5.1 Inleiding

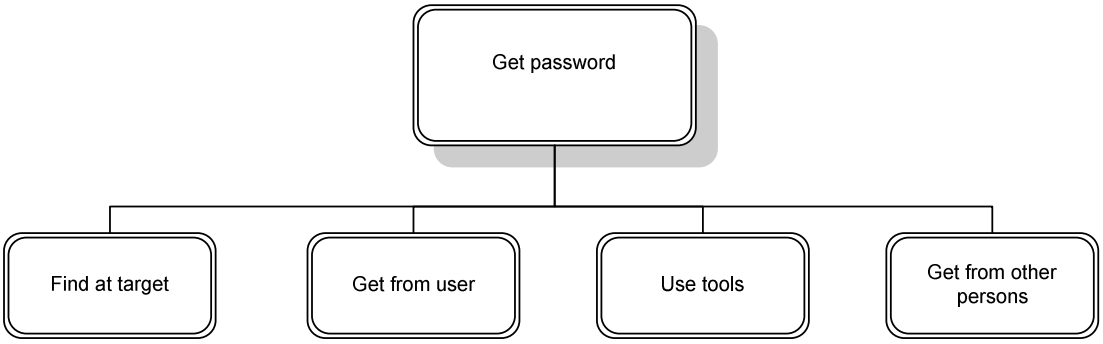
De eerste attack tree op logisch niveau, zal in kaart brengen welke attacks er mogelijk zijn om een UZI-pas en het wachtwoord van een zorgverlener (gebruiker) te bemachtigen om vervolgens daarmee het LSP te kunnen betreden.



Figuur 8.2: Attack tree met AND-vertakking op logisch niveau

Het risico op dit niveau wordt gekenmerkt doordat de aanvaller probeert logingegevens én de UZI-pas te verkrijgen om zodoende toegang te verkrijgen tot het LSP. De combinatie van beide onderdelen is noodzakelijk en wordt daarom aangeduid met een “AND” (figuur 8.2). Indien niet aan de “AND” voorwaarde wordt voldaan, kan er geen succesvolle attack plaats vinden op dit niveau.

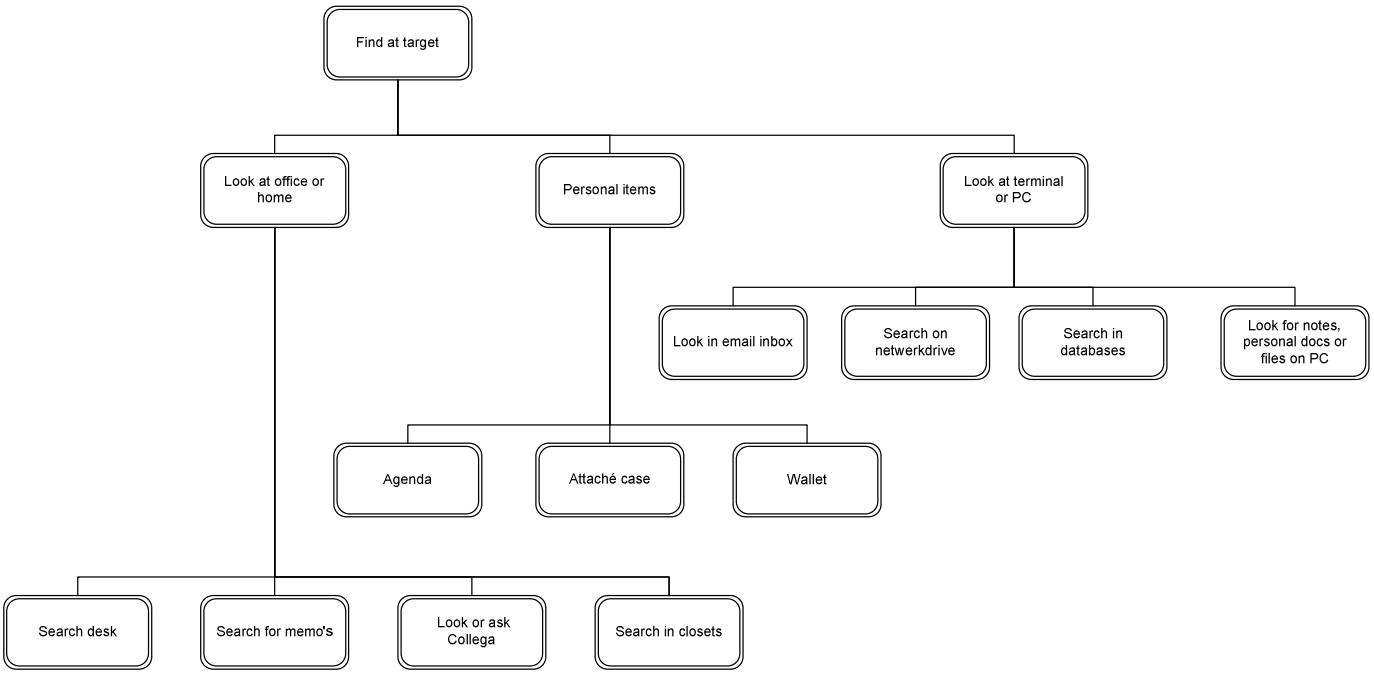
8.5.2 Get password



Figuur 8.3: Attack tree “get password”

De attack tree “Get password” (figuur 8.3) kent een aantal onderkende attacks die in de secties 8.5.3, 8.5.4 en 8.5.5 nader worden uitgewerkt. De scores van zowel de risicofactor en CIA zijn hoger wanneer een kwaadwillende al beschikt over een geldige UZI-pas. Immers, met al een pas op zak is een kwaadwillende dichter bij zijn uiteindelijke doel. Een lagere score wordt toegekend wanneer dat niet het geval is.

8.5.3 Get password - Find at target



Figuur 8.4: Attack tree "find at target"

Dreiging en gevolg

Look at office or home/ personal items/look at terminal or pc

De dreiging van deze attack zit in het feit dat deze eenvoudig is uit te voeren, een kwaadwillende geen specialistische kennis behoeft te hebben alsmede de kosten voor de uitvoering laag zijn waarbij de kans op een succes net zo groot is als de gevolgen.

Het eenvoudig uitvoeren is te danken aan het feit dat het zoeken naar inloggegevens een eenvoudige maar wel een tijdrovende klus is. Veelal bewaren gebruikers deze gegevens op een logische plaats, zoals in een agenda, memo's, telefoons, op de pc, of rondom het bureau of kantoor van een gebruiker. Het succes van deze attack is afhankelijk van de aan te vallen gebruiker en hoe deze omgaat met dergelijke gegevens. Wanneer gegevens niet bij een gebruiker zijn te achterhalen, kan een kwaadwillende het eenvoudig bij een andere gebruiker proberen. Er zijn immers voldoende gebruikers.

Belang van bescherming

Look at office or home/ personal items/look at terminal or pc

Wanneer een kwaadwillende deze methode kiest, dan zijn attacks waarbij logingegevens en de UZI-pas moeten worden verkregen makkelijk uit te voeren. Het belang van bescherming van de gegevens en de pas is, ook wanneer regels consequent worden gevolgd door de gebruikers, nog steeds noodzakelijk. Wanneer een gebruiker onzorgvuldig omgaat met zijn persoonlijke voorwerpen (pas of inloggegevens) neemt de kans op misbruik echter toe. Desondanks zijn veel zorgverleners bewust van het feit dat met persoonsgebonden

items vertrouwelijke patiëntinformatie is te benaderen. Daarbij realiseert men zich dat bij laks gedrag dit gevolgen kan hebben voor de uitoefening van het beroep.

Het risico dat logingegevens bij de target gevonden worden is groot. Dit is vooral te wijten aan onverantwoordelijk gedrag of toch door onwetendheid. Omdat de zorgverlener met vertrouwelijke gegevens werkt mag men er van uitgaan dat de zorgverlener op de hoogte is van eventuele risico's die hij door onzorgvuldig gedrag riskeert. Hun reputatie voor wat betreft de patiëntinformatie, komt in het geding wanneer men niet zorgvuldig omgaat met de persoonsgebonden toegangsmiddelen.

Risicofactor

De risicofactor voor deze attack wordt geschat op: 3 (kansfactor) x 3 (omvangfactor) = 9 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA gelden de cijfers van tabel 8.1. Het cijfer tussen de haakjes geeft de effecten aan wanneer een kwaadwillende reeds in het bezit is van een geldige UZI-pas. Dat zorgt namelijk voor een verhoogde kans op het slagen van de attack. Het andere cijfer impliceert wanneer dat niet het geval is.

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Inloggegevens verkregen door deze te zoeken in en rondom kantoor of huis, verkregen door persoonlijke items te doorzoeken of door deze van de pc of netwerk te halen.	1 (3)	1 (3)	1 (1)

Tabel 8.1: Effecten attack "find at target" op de CIA

De effecten op de aspecten confidentiallity, integrity en availability zijn in eerste instantie laag, omdat een kwaadwillende moet beschikken over een UZI-pas wil de attack succesvol zijn. Heeft hij deze niet, dan is inloggen op het LSP niet mogelijk. Indien een kwaadwillende wél de beschikking heeft over een UZI-pas is de kans zeer groot op misbruik door een kwaadwillende. Immers, hij heeft een van beide persoonlijke items al in handen.

Urgentie

Wanneer gekeken wordt naar de risicofactor van de attack en dat in relatie wordt gebracht met de CIA wordt duidelijk dat het voor gebruikers noodzakelijk is dat zij op een verantwoordelijke wijze hun persoonlijke inlogtools gebruiken en misbruik proberen te voorkomen. Een zorgverlener zou net zo met deze inlogtools moeten omgaan als met zijn PIN-code en bankpas. Door de gestelde (bank-) procedures op te volgen wordt het risico aanzienlijk verkleind. Desondanks blijven kwaadwillende proberen zich toegang te verschaffen tot andermans rekening.

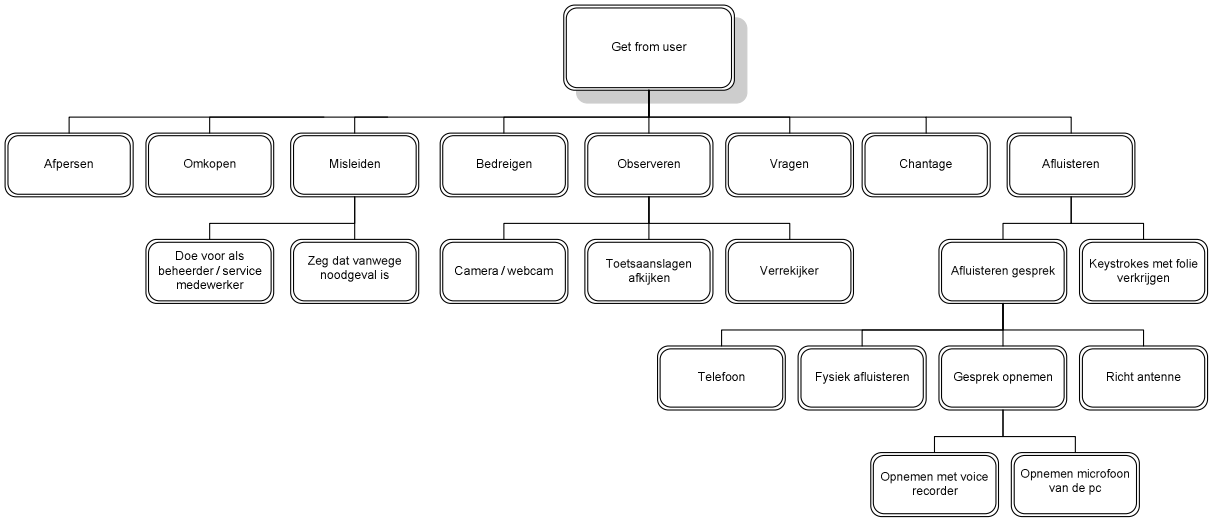
De onderzochte attack scoort bij de risicofactor de maximale kans- en omvangsfactor, waardoor de risicoscore ook maximaal is. Bij de CIA-aspecten is de score minimaal, wanneer de kwaadwillende niet de beschikking heeft over een UZI-pas, en maximaal wanneer een kwaadwillende wél de beschikking heeft over de UZI-pas. Omdat er van uit moet worden gegaan dat een kwaadwillende reeds alle informatie tot zich heeft is het “zeer noodzakelijk” om maatregelen te nemen tegen een eventuele attack.

Aanbevelingen

Look at office or home/ personal items/look at terminal or pc

Mogelijkheden om te voorkomen dat inloggegevens niet verkregen kunnen worden is een zaak waar de gebruiker goed op zal moeten letten. De gebruiker zal gewezen moeten worden op de vertrouwelijkheid van het gebruik van het account evenals het risico dat hij loopt wanneer nonchalant met deze gegevens wordt omgesprongen. Het is daarom noodzakelijk om gebruikers bewust te maken van deze verantwoordelijkheid en trachten te voorkomen dat deze gegevens te verkrijgen zijn. Indien een gebruiker hierin faalt, zou men kunnen overwegen sancties op te leggen tegen de betreffende gebruiker, zoals beperkt (of geen) toegang tot het LSP of permanente controle.

8.5.4 Get password - Get from user



Figuur 8.5: Attack tree “get from user”

Dreigingen en gevolgen

Get from user

“[..] Security is only as good as its weakest link, and people are the weakest link in the chain” [SCH00]. Een constatering die ook zeer zeker bekend is bij de aanvaller. Indien hij toegang tot het LSP wil krijgen kan hij proberen de gebruiker te benaderen om zo de benodigde inloggegevens te verkrijgen. Het risico dat de aanvaller bij deze methode loopt is dat hij zich bekend moet maken waardoor men mogelijk op de hoogte is van de identiteit en mogelijke intenties van de aanvaller [KIE06].

De methoden of technieken die hiervoor gebruikt kunnen worden zijn er genoeg. Attacks als het bieden van geld, bedreigingen, misleiding, of het misleiden van de gebruiker door zich voor te doen als beheerder of medewerker die de hulp van de gebruiker nodig heeft om succesvol zijn taken te kunnen afronden. Vanwege de bereidheid om andere mensen te helpen zullen veel gebruikers zonder daarvan kwade bedoelingen van in te zien, het gevraagde overhandigen aan de aanvaller.

Belang van bescherming

Get from user

De aanvaller heeft de mogelijkheid te kiezen tussen twee aanvalstactieken. Enerzijds door direct de confrontatie aan te gaan met de gebruiker en anderzijds door contact met de gebruiker juist te vermijden en zo onopgemerkt informatie van deze te verkrijgen. De risicofactoren zijn voor beide aanvallen hoog, omdat ze relatief eenvoudig uit te voeren zijn, geen grote kennis vereisen van de aanvaller en er snel resultaat geboekt kan worden zonder hierbij afhankelijk te hoeven zijn van andere partijen. Dat snelle resultaat is mede ook afhankelijk van het feit dat er meerdere potentiële gebruikers benaderd kunnen worden, zodat er bij problemen bij een gebruiker er altijd andere gebruikers kunnen worden benaderd. De kans dat men een gebruiker zijn gegevens afgeeft is niet groot. Dit vanwege het feit dat veel gebruikers realiseren dat men persoonlijke gegevens goed moet beschermen. Desondanks is er een kans dat dergelijke informatie in handen valt van een aanvaller zeer zeker aanwezig.

Risicofactor

Get from user (afpersen, omkopen, misleiden, bedreigen, chanteren of vragen)

De risicofactor voor deze attack wordt geschat op: 2 (kansfactor) x 3 (omvangfactor) = 6 (risicofactor).

Get from user (observeren of afluisteren)

De risicofactor voor deze attack wordt geschat op: 3 (kansfactor) x 3 (omvangfactor) = 9 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA gelden de cijfers van tabel 8.2. Het cijfer tussen de haakjes geeft de effecten aan wanneer een kwaadwillende reeds in het bezit is van een geldige UZI-pas. Dat zorgt namelijk voor een verhoogde kans op het slagen van de attack. Het andere cijfer impliceert wanneer dat niet het geval is.

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Gebruikers afpersen, omkopen, misleiden, bedreigen, chanteren of vragen de inloggegevens af te geven.	1 (3)	1 (3)	1 (1)
• Gebruikers observeren of afluisteren om zodoende de inloggegevens te verkrijgen.	1 (3)	1 (3)	1 (1)

Tabel 8.2: Effecten attack “get from user” op de CIA

Net zoals bij de attack in sectie 8.5.2 gelden hier dezelfde constateringen. De dreigingen oefenen ook hier vrijwel geen druk uit op de aspecten confidentiallity, integrity en availability. Dit is anders wanneer de kwaadwillende in het bezit is van een geldige UZI-pas en daarmee met deze attacks een reëel gevaar voor het systeem wordt.

Urgentie

De eerste attack scoort een zes bij de risicofactor. De tweede attack de hoogst haalbare score, een negen. De CIA-aspecten zijn voor beide, wanneer de kwaadwillende niet de beschikking heeft over een UZI-pas, zeer laag. Wanneer deze juist wel daarover weet te beschikken is de CIA op twee van de drie aspecten zeer hoog. Omdat uiteraard niet op voorhand is te bepalen of een kwaadwillende de beschikking heeft over de UZI-pas is het verstandig uit te gaan van het slechtste scenario. Het is dus daarom “noodzakelijk” dat men probeert dat men praktijken als afpersing, omkoping, misleiding e.d. van gebruikers voorkomt. En “zeer noodzakelijk” om te voorkomen dat men diezelfde gebruiker door observeren of afluisteren persoonlijke informatie afhandig maakt.

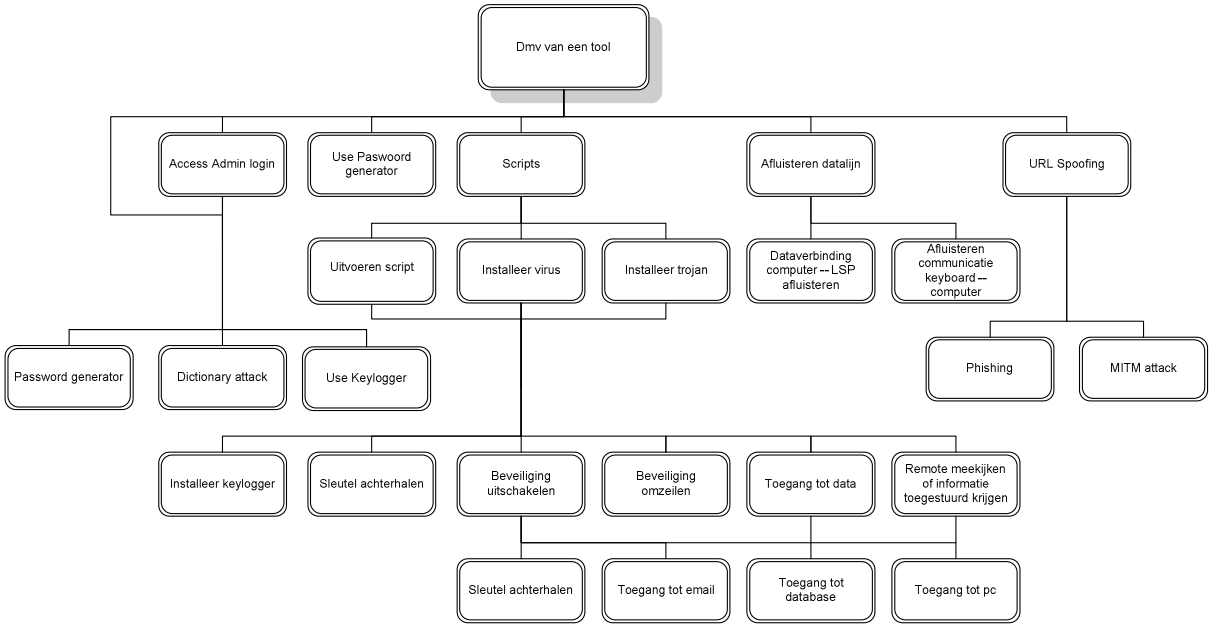
Aanbevelingen

Get from user

De bescherming tegen dit soort attacks is relatief eenvoudig te bewerkstelligen door het opstellen van richtlijnen waar gebruikers zich aan dienen te houden. Hierin kan bijvoorbeeld staan dat de persoonlijk voorwerpen onder geen beding aan derden mogen worden verstrekt. Wanneer is gebleken dat er niet aan de vastgestelde gebruikersvoorwaarden kan worden voldaan zou men de gebruiker een sanctie moeten opleggen. Dit om bijvoorbeeld te voorkomen dat gebruikers op het LSP onder elkaars identiteit zijn ingelogd, wat tot nu toe vooral bij verwerken van gegevens veel gebeurd.

In het tweede geval (afluisteren en observeren) is beveiliging en bescherming een stuk lastiger omdat afluisteren van een gebruiker, met de juiste middelen en methodes, succesvol is uit te voeren. Observeren of afluisteren kan niet direct worden tegen gegaan, vooral ook doordat de technische mogelijkheden steeds slimmer, kleiner, makkelijker en eenvoudiger zijn te verkrijgen. Ook hier zouden richtlijnen grote risico’s kunnen wegnemen, door gebruikers verstandig om te laten gaan met hun gegevens en deze discreet en met enige terughoudendheid te gebruiken.

8.5.4 Get password - Use tools



Figuur 8.6: Attack tree "dmv tools of technische middelen"

Dreigingen en gevolgen

Get password dmv een tool

Een tool kan zowel een hard- als softwarematige methode zijn waarmee het mogelijk is een doel te bereiken dat zonder gebruik hiervan niet is te realiseren. Deze attack tree laat een aantal mogelijkheden zien die zijn te gebruiken om een paswoord te achterhalen. Het gebruik van softwarematige methodes verdient hierbij de voorkeur vooral ook omdat deze vrij eenvoudig via het internet zijn te verkrijgen. De snelheid waarmee er vernieuwende aanpassingen worden gedaan zorgt er voor dat deze nieuwe software moeilijk is te stoppen. Aan de andere kant laat dit wel zien waarom softwarematige methodes de voorkeur genieten.

De attack tree belicht voornamelijk de softwarematige zijde. Keyloggers, toegang verkrijgen met behulp van het admin account, paswoord generators, scripting, het af luisteren van de communicatie en URL spoofing behoren tot veel gebruikte methoden. De inzet en gebruik van deze methodes zijn relatief vrij eenvoudig betaalbaar en bieden een grote kans van slagen.

- **Keyloggers***:* Zowel hard- als softwarematig toepassing mogelijk waarbij toetsaanslagen die een gebruiker invoert via het toetsenbord ongemerkt doorstuurt naar een kwaadwillende.
- **Toegang via admin**: Door gebruik te maken van het administrator account van het LSP is een belangrijke en bruikbare methode om toegang te verkrijgen tot dit systeem. De middelen die gebruikt worden om succesvol toegang te krijgen zonder het systeem te beschadigen zijn een keylogger, paswoordgenerator, dictionary attack, guessing, vragen, afluisteren of afkijken.

- **Scripts**: kunnen op allerlei wijzen worden ingezet. Er zijn scripts bij die een extra functie hebben die normaal niet aanwezig is. Er zijn ook scripts die mis- of gebruik maken van bepaalde mogelijkheden van een ander stuk soft- of hardware door het script te installeren of te activeren.
- **Afluisteren datalijn**: Naast het gebruik van softwarematige attacks behoort het afluisteren van de communicatie tot de mogelijkheden. Het betreft hier het afluisteren van de communicatie tijdens bijvoorbeeld een inlogprocedure waarbij cruciale en belangrijke informatie door de gebruiker wordt verstuurd naar het systeem. De tool die men hierbij zou kunnen gebruiken is programmatuur dat de communicatie afluistert en doorstuurt naar een kwaadwillende (het principe van een keylogger).
- **URL-spoofing**: een veel gebruikte methode bij banken om via een internetsite dat sprekend lijkt op het origineel probeert een kwaadwillende de logingegevens van de bankrelaties op onrechtmatige wijze te bemachtigen. Het effect van deze attack is groot maar zal in geval van het LSP pas echt effect hebben wanneer er gebruik wordt gemaakt van URL based pagina's of patiënten vanuit huis kunnen inloggen om hun persoonlijke dossier op te vragen.

Belang van bescherming

Get password dmv tool

De kans dat een kwaadwillende een tool gebruikt is voornamelijk groter doordat er via het internet genoeg resources voorhanden zijn waar potentieel gezien genoeg software en broncode vrij is te verkrijgen om systemen kwaad te doen. Het probleem daarbij is dat door het internet, zoals bij virussen, vele varianten opduiken. Bescherming daartegen is zeer noodzakelijk en hoort bij de basis van beveiliging. Het zou geen goed signaal afgeven als blijkt dat men informatie heeft weten te bemachtigen (in dit geval informatie om het LSP te kunnen betreden), door gebruik te maken van software van het internet. De betrouwbaarheid van het systeem zou daardoor een deuk oplopen, waardoor het gebruik van het informatiesysteem wel eens onder druk kan komen te staan.

Risicofactor

Get password dmv tool (door installatie software als bijvoorbeeld een keylogger)

De risicofactor voor deze attack wordt geschat op: 3 (kansfactor) x 3 (omvangfactor) = 9 (risicofactor).

Get password dmv tool (door afluisteren communicatie met software)

De risicofactor voor deze attack wordt geschat op: 2 (kansfactor) x 3 (omvangfactor) = 6 (risicofactor).

Get password dmv tool (door gebruik van nepsite/voorziening)

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA gelden de cijfers van tabel 8.3. Het cijfer tussen de haakjes geeft de effecten aan wanneer een kwaadwillende reeds in het bezit is van een geldige UZI-pas. Dat zorgt namelijk voor een verhoogde kans op het slagen van de attack. Het andere cijfer impliceert wanneer dat niet het geval is.

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Inloggegevens verkregen doordat een kwaadwillende software gebruikt of installeert waarmee vervolgens de inloggegevens worden verkregen	1(3)	1(3)	1(1)
• Inloggegevens verkregen door softwarematig afluisteren van verbindingen	1(3)	1(3)	1(1)
• Inloggegevens verkregen door opzetten van een nep-site waardoor gebruiker denkt dat deze originele site bezoekt, maar feitelijk gebruik maakt van een malafide website	1(3)	1(3)	1(1)

Tabel 8.3: Effecten attack “dmv een tool” op de CIA

Ook hier scoren de drie aspecten laag wanneer de kwaadwillende niet de beschikking heeft over de verplichte UZI-pas. Wanneer hij hier wel over beschikt én de attacks succesvol weet uit te voeren veranderd de score voor de eerste twee aspecten. De score wordt dan hoog, waardoor confidentiality en integrity niet meer zijn te garanderen. De beschikbaarheid van de informatie is niet in het geding omdat met deze attacks de informatie ondanks de attack beschikbaar blijft.

Urgentie

De drie attacks verschillen in hun geschatte risicoscores van hoog (negen), naar gemiddeld (zes) en laag (drie). De CIA-aspecten leveren voor alle drie eenzelfde resultaat, waarbij ook nu weer de availability in alle gevallen laag is. De attack waarbij gebruik wordt gemaakt van software die, in dit geval, belangrijke gegevens weet door te spelen naar een kwaadwillende kent een zeer hoge risicofactor. De classificatie “zeer noodzakelijk” om te worden opgelost is deze attack meer dan waardig. Het risico dat men loopt wanneer dergelijke software actief is blijft mogelijk.

De attack waarmee met behulp van software wordt geprobeerd om belangrijke inloggegevens direct van af te luisteren van een verbinding en niet vanaf een computer blijft een specialistische aanval, dat waarschijnlijk niet direct een grote kans van slagen heeft. De noodzaak om hier dan ook iets tegen te doen neemt daardoor af tot “noodzakelijk”.
De attack waarin een kwaadwillende probeert met behulp van een malafide internetsite de zorgverlener te misleiden om daarmee de inloggegevens afhandig te maken van de zorgverlener. Hoewel deze toepassing zeer effectief is en veel wordt toegepast in bijvoorbeeld de bancaire sector, scoort de attack er niet hoog op omdat de zorgverlener lokaal inlogt en daarna geautomatiseerd contact wordt gemaakt met het LSP. Het is in dat opzicht daarom “minder noodzakelijk” om hier op korte termijn extra maatregelen tegen te nemen.

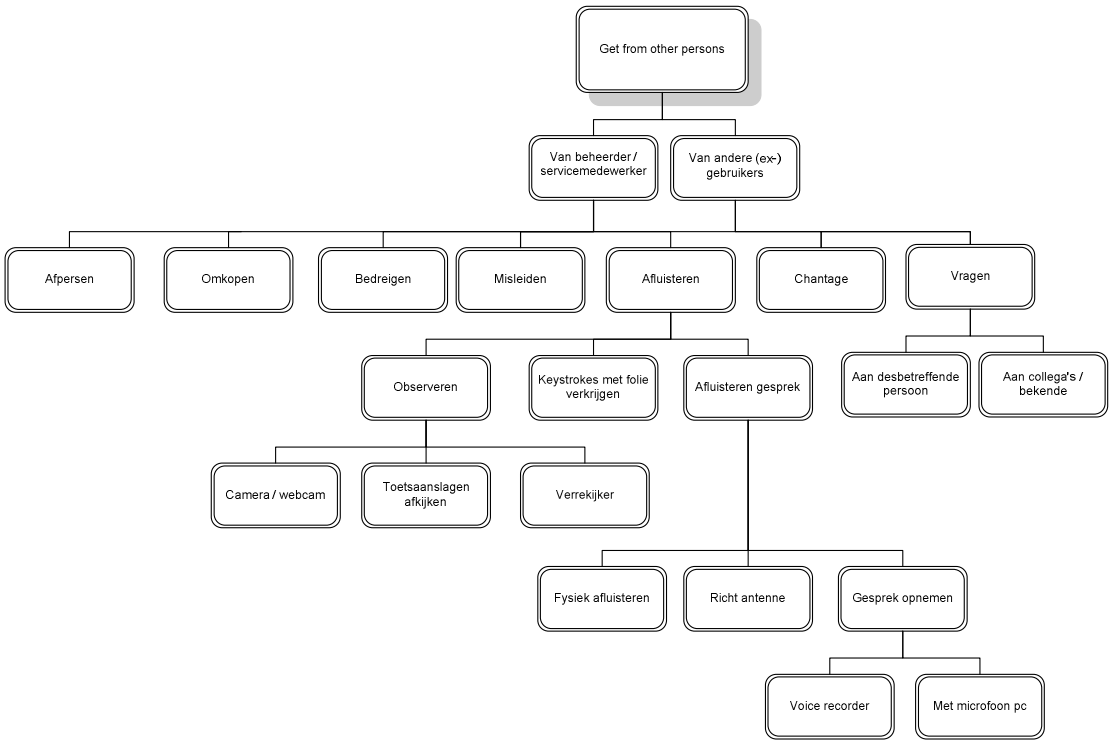
Aanbevelingen

Get password dmv tool

Het risico dat men loopt doordat een aanvaller zal proberen met behulp van softwarematige oplossingen informatie te verkrijgen is een constante en reële dreiging. Probleem is de grote beschikbaarheid op het internet van software die eerder genoemde attacks mogelijk maken. Men zal moeten voorkomen dat het verkrijgen van het wachtwoord zo moeilijk mogelijk word. Keyloggers en scripts moeten daarom alvorens men deze kan installeren detecteren op ongewenste inhoud. Wachtwoorden moeten zodanig worden uitgevoerd dat het gebruik van dictionairy attacks wordt bemoeilijkt. Afluisteren moet men bemoeilijken door communicatie te versleutelen en mogen gebruikers alleen van het systeem gebruik maken wanneer ze aanwezig zijn op een bepaald domein met identificerende gegevens over waar een gebruiker zich bevindt.

Probleem wat betreft attacks van softwarematige aard is dat deze onderhevig zijn aan snelle wijzigingen en mutaties. Virussen en scripts komen in vele vormen voor en vormen zodoende alsnog een bedreiging waarbij ze een catastrofale uitwerking kunnen hebben.

8.5.5 Get password - Get from other persons



Figuur 8.7: Attack tree “get from other persons”

Dreigingen en gevolgen

Van beheerder/servicemedewerker

Niet alleen bij de gebruiker zelf zijn gegevens te verkrijgen. Ook systeembeheerders of andere personen die onderdeel zijn van het beheersysteem kunnen al dan niet via legitieme wijze toegang krijgen tot het systeem en de privacy gevoelige informatie. De gevolgen die een dergelijke attack kan veroorzaken kan gevolgen hebben voor de beheerders omdat zij veelal ongecontroleerd toegang hebben tot alle systeemresources. Zij vormen een belangrijke schakel waar de beveiliging nauwlettend in de gaten moet worden gehouden. Voornamelijk ook vanwege het feit dat beheerders vrij spel hebben in hun werkzaamheden en hij of anderen misbruik zouden kunnen maken van die rechten.

Van andere (ex-) medewerkers

Ook medewerkers behoren tot de risicogroep. Medewerkers zijn vaak op de hoogte van specifieke informatie of kunnen vaak zonder al te veel moeite de beschikking hebben over allerlei bedrijfsgevoelige informatie die interessant kan zijn voor derden. Een kwaadwillende kan wanneer hij in de organisatie werkzaam is, dit voorrecht misbruiken en te gelde maken. Ook ex-medewerkers beschikken, nadat zij de organisatie hebben verlaten, nog altijd over gevoelige informatie die voor een kwaadwillende van belang kan zijn om een attack succesvol te kunnen uitvoeren. Hierbij kan het dus gaan om zowel personen die zich reeds in de organisatie bevinden, maar ook kwaadwillenden die zich extern bevinden en gebruik willen maken van de kennis van de medewerker.

Het risico dat een medewerker daadwerkelijk mee zal werken aan een dergelijk initiatief is uiteraard ook afhankelijk van het feit of hij op een al dan niet prettige wijze afscheid heeft genomen van de organisatie. Wanneer dat niet het geval is, zal deze vatbaarder zijn voor eventuele wraakgevoelens en eerder ingaan op een voorstel van een kwaadwillende om mee te werken bepaalde bedrijfsinformatie los te laten in ruil voor financiële genoegdoening.

Belang van bescherming

Hoewel men veelal op de hoogte is dat dergelijke situaties kunnen ontstaan wordt er niet heel veel prioriteit geboden om dit tegen te gaan. Vooral in kleinere organisaties neemt men het niet zo nauw met de preventie tegen dit soort acties. Dit is vooral te wijten aan onwetendheid, voorgestelde hoge preventiekosten, gebrek aan tijd en vertrouwen in het personeel.

Desondanks is de kans dat een dergelijke attack zich voordoet waarschijnlijk groter dan men zou verwachten. In een doorsnee organisatie komt het vaak voor dat mensen wisselend op elkaars account werken. Vaak ook omdat het vertrouwen groot is en het vaak net even wat makkelijker uit komt. Men raakt op de hoogte van elkaars inloggegevens en kan wanneer de ander bijvoorbeeld bij ziekte toch de administratie verwerken. Het risico dat hierin schuilt, is dat het vertrouwen geen grenzen meer kent en anderen geheel zonder dat de rechtmatige gebruiker er van op de hoogte is, toegang hebben tot niet voor hem bedoelde informatie.

Risicofactor

Get from other persons (van beheerder/servicemedewerker)

De risicofactor voor deze attack wordt geschat op: 2 (kansfactor) x 3 (omvangfactor) = 6 (risicofactor).

Get from other persons (van andere (ex-) medewerkers)

De risicofactor voor deze attack wordt geschat op: 3 (kansfactor) x 3 (omvangfactor) = 9 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA gelden de cijfers van tabel 8.4. Het cijfer tussen de haakjes geeft de effecten aan wanneer een kwaadwillende reeds in het bezit is van een geldige UZI-pas. Dat zorgt namelijk voor een verhoogde kans op het slagen van de attack. Het andere cijfer impliceert wanneer dat niet het geval is.

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Beheerder of (ex-) medewerker/gebruiker afpersen, omkopen, bedreigen, misleiden, chanteren of vragen inloggegevens van een gebruiker waarover de betreffende gebruiker beschikt.	1(3)	1(3)	1(1)
• Beheerders of andere (ex-) medewerkers/ gebruikers observeren of afluisteren om zo inloggegevens te verkrijgen van een andere gebruiker waarover deze gebruiker beschikt.	1(3)	1(3)	1(1)

Tabel 8.4: Effecten attack “dmv andere personen” op de CIA

In vergelijking met sectie 8.5.4 scoren ook hier de drie CIA-aspecten laag wanneer de kwaadwillende niet de beschikking heeft over een UZI-pas. Echter, wanneer hij die wel heeft en zijn attack succesvol kan uitvoeren zullen de CIA-scores veranderen. Voornamelijk de aspecten confidentiality en integrity ondervinden hiervan de nodige effecten. De score wordt voor beide aspecten dan dus hoog. Zowel de confidentiality als de integrity zijn dan niet meer te garanderen. De availability van de informatie komt hierdoor niet in het geding omdat de informatie ondanks de attack beschikbaar blijft.

Urgentie

Net als het risico dat men loopt doordat inloggegevens afhandig worden gemaakt door kwaadwillenden bij een gebruiker zo kan men ook deze gegevens afhandig proberen te maken van beheerders of zelfs ex-medewerkers die misschien deze gegevens nog in bezit hebben waardoor de kwaadwillende succesvol kan inloggen. Wat de reden ook mogen zijn, een kwaadwillende is bij de beheerder aan het goede adres als het gaat om het verkrijgen van ieder gewenst, in dit geval, inloggegeven. De CIA toont geen veranderingen ten

opzichte van eerdere attacks, is het “noodzakelijk” om dergelijke attacks tegen te gaan. Immers, wanneer een kwaadwillende een beheerder zover heeft gekregen, is het hek van de dam en kan deze diverse vervolg attacks uitvoeren. Het risico dat men loopt dat een ex-medewerker hier medewerking aan verleent is even zo zeer een punt van aandacht waarmee voorkomen moet worden dat zij nog de mogelijkheid hebben om van invloed te zijn op de veiligheid van het systeem. Ook hiervoor geldt dat het volgen van procedures door alle gebruikers een hoge prioriteit heeft en dat daar niet van af mag worden geweken om zodoende het systeem niet in gevaar te brengen.

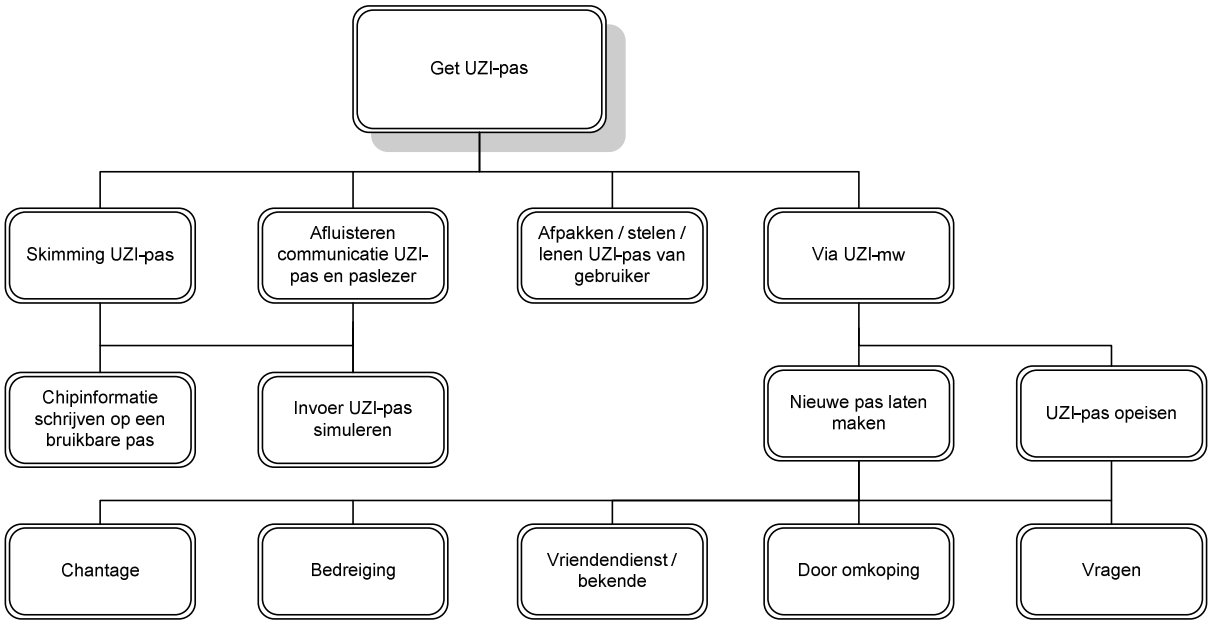
De attack waarbij de kwaadwillende tracht de voor hem belangrijke informatie door middel van afluisteren of observaties te verkrijgen biedt meer potentie, vooral vanwege de eenvoudige uitvoering. Ondanks de CIA-aspecten is het sowieso aan te raden hier extra alert op te zijn. Daarom is het “zeer noodzakelijk” om hier de nodige aandacht aan te blijven besteden. Wanneer men over deze persoonlijke informatie beschikt, is alleen het verkrijgen van de UZI-pas de laatst te nemen horde.

Aanbevelingen

Bescherming kan worden gerealiseerd door reglementen op te stellen en procedurele maatregelen te nemen. Gebruikers van het zorgsysteem mogen alleen dit systeem gebruiken wanneer zij zich van te voren conformeren aan de geldende regels. Wanneer misbruik plaats vindt kan men reglementair gezien sancties op leggen. Uiteraard betreft het hier wel een actie die pas achteraf, dus wanneer het kwaad al is geschiedt en onrechtmatigheid is geconstateerd, tegen kan worden opgetreden. Hier toe behoort bijvoorbeeld het onrechtmatig verspreiden van persoonlijke inloggegevens onder collega’s en andere gebruikers bedoeld om hen onder het persoonlijke account van een ander te laten werken.

Procedureel gezien kan men vooraf ook een aantal zaken regelen, zoals het screenen van beheerders en/of met belangrijke functies binnen de zorgapplicatie. Dit om ongeschikte personen op voorhand zo goed mogelijk te filteren van de goede personen. Wanneer gebruikers van functie veranderen of de zorginstelling verlaten moet hun account direct na afscheid worden opgeheven en wordt daarmee voorkomen dat zij nog toegang hebben tot het zorgsysteem.

8.5.6 Get UZI-pas



Figuur 8.8: Attack tree "get UZI-pas"

Dreigingen en gevolgen

Wanneer een kwaadwillende in bezit is van de inloggegevens, dient hij volgens de attack tree, nog in bezit te komen van de UZI-pas om het systeem op een rechtmatige wijze te kunnen betreden. Hieronder worden een aantal opties gegeven op welke wijze dat is te realiseren (zie figuur 8.8).

Skimming

Een op dit moment populaire methode is de skimming-methode en wordt vooral gebruikt om de magneetstrip van een bankpas te lezen en vervolgens te kopiëren op een nieuwe blanco pas met eenzelfde magneetstrip. Op het internet is genoeg informatie te vinden om hard- en software aan te schaffen waarmee het mogelijk wordt om kaarten te kunnen dupliceren. Ook het kopiëren van een chip zal niet lang op zich laten wachten. Het is wel zaak dat men er voor zorgt dat de pas niet in handen komt van anderen of kan worden uitgelezen om de informatie te dupliceren.

Afluisteren communicatie UZI-paslezer en UZI-pas

Naast skimming beschrijft de attack tree ook de mogelijkheid van het afluisteren van de communicatie tussen de UZI-pas en de UZI-paslezer oftewel sniffen. Data die wordt verzonden tussen beide kan door een kwaadwillende worden afluistert en in het slechtste geval door hem worden gebruikt.

Afpakken / stelen / lenen UZI-pas van gebruiker

een kwaadwillende kan ook de directe benadering kiezen om zo de UZI-pas proberen in bezit te krijgen. Dit kan heel simpel door af te wachten wanneer een gebruiker zijn UZI-pas heeft verloren of wanneer deze de pas zelfs wil geven. Ook opties zijn om de pas van de rechtmatige eigenaar te stelen, af te pakken of te lenen. Hoewel de gebruiker in de laatste gevallen veelal direct op de hoogte is dat iemand anders de pas in bezit heeft, kan een kwaadwillende er wel (tijdelijk) gebruik van maken. Wanneer een kwaadwillende de pas kopieert en het origineel teruggeeft aan de eigenaar hoeft dat in eerste instantie niet direct tot problemen te leiden.

Via UZI-medewerker

Bij de laatst onderzochte attack wend een kwaadwillende zich bij de uitgifte-instantie voor UZI-pasjes tot het UZI-register. Wanneer uitgifteprocedures niet door medewerkers van het UZI-register consequent worden opgevolgd, kan de aanvaller proberen met een valse identiteit een pas (via een al dan niet bevriende medewerker) aan te vragen of te eisen. Hij kan dan de beschikking krijgen over een pas met de daarbij behorende gewenste rechten.

Belang van bescherming

Skimming

De kans dat de informatie op de chip wordt uitgelezen en door een kwaadwillende wordt gekopieerd op een blanco pas is misschien nog niet mogelijk. De kans dat dit ooit wel het geval zal zijn wordt groter naar mate het gebruik ervan stijgt en de toepassingen interessant worden om de chip te gaan dupliceren, bijvoorbeeld bij access control als voor het LSP noodzakelijk is. Hoewel het risico nu dus nog niet groot is, zal deze naarmate de technische ontwikkelingen vorderen er vast en zeker een moment komen dat het risico en dus het belang van bescherming groter is dan nu.

Afluisteren communicatie UZI-paslezer en UZI-pas

Sniffen is, op enkele uitzonderingen na, verboden door de wet. Dat is niet voor niets, omdat het sniffen betrekkelijk eenvoudig is uit te voeren. Hoewel er door een kwaadwillende vrijwel zeker “een bijzondere inspanning” geleverd dient te worden, worden vele gebruikers van het internet constant gesnift en afgeluisterd. Het belang van bescherming zit voornamelijk in het feit dat met “digitaal luistervinken” de aanvaller informatie in handen kan krijgen zonder dat de eigenaar van deze informatie hiervan op de hoogte is. Met ernstige gevolgen, wanneer blijkt dat de communicatie tussen de UZI-paslezer en de UZI-pas of welke andere communicatie dan ook niet beschermt is tegen privacy en door derden kan worden gevolgd en mogelijkerwijs ook kan worden gebruikt.

Afpakken / stelen / lenen UZI-pas van gebruiker

Een zorgverlener met UZI-pas wordt verplicht om zorgvuldig met zijn pas om te gaan, deze niet aan derden uit te lenen en alleen te gebruiken waarvoor het is bedoeld. De kans dat een pas wordt afgepakt of gestolen is net zoals bij de bankpas, aannemelijk. Maar goed te beveiligen mits de rechtmatige eigenaar van de pas consequent handelt wanneer hij zijn pas door onrechtmatige toe-eigening bij iemand anders in gebruik is. Het uitlenen van een UZI-pas aan een collega is, hoewel het vooral bij administratieve taken of

bij afwezigheid van een collega veel zou kunnen voorkomen, niet wenselijk. Elke zorgverlener is feitelijk aansprakelijk voor het waarborgen dat de pas alleen door hem kan worden gebruikt zodat daarmee de privacy van zijn patiënten gewaarborgd blijft.

Via UZI-pas medewerker

Deze attack zal niet tot een verhoogd risico leiden indien de uitgifteprocedures worden opgevolgd. De dreiging dat een pas wordt vervaardigd zonder dat dit wordt opgemerkt is vrijwel uitgesloten.

Risicofactor

Skimming

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

Afluisteren communicatie UZI-paslezer en UZI-pas

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

Afpakken / stelen / lenen UZI-pas van gebruiker

De risicofactor voor deze attack wordt geschat op: 3 (kansfactor) x 3 (omvangfactor) = 9 (risicofactor).

Via UZI-pas medewerker

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA gelden de cijfers van tabel 8.5. Het cijfer tussen de haakjes geeft de effecten aan wanneer een kwaadwillende reeds in het bezit is van de correcte inloggegevens. Dat zorgt namelijk voor een verhoogde kans op het slagen van de attack. Het andere cijfer impliceert wanneer dat niet het geval is.

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Skimming: chipinformatie van de UZI-pas wordt gelezen en gekopieerd op een blanco kaart of ander medium opgeslagen om toegang te verkrijgen tot het LSP.	1(3)	1(3)	1(1)
Sniffen: Communicatie tussen UZI-pas en paslezer wordt afgeluisterd en gebruikt om hiermee vervolgens toegang te verkrijgen tot het LSP.	1(3)	1(3)	1(1)
• De UZI-pas wordt gestolen of geleend van de rechtmatige gebruiker om vervolgens toegang tot het LSP te verkrijgen.	1(3)	1(3)	1(1)

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Via het UZI-register, al dan niet via een (malafide) medewerker, wordt getracht een UZI-pas te verkrijgen om hier vervolgens toegang mee te verkrijgen tot het LSP.	1(3)	1(3)	1(1)

Tabel 8.5: Effecten attack "get UZI-pas" op de CIA

Hier geldt dat de confidentaility en integrity in geval van het in bezit hebben van beide persoonlijke items tot grote problemen zouden kunnen leiden. De hoogte van de CIA tabel 8.5 toont dit aan. Voor het effect op de availability geldt deze in geval van skimming en afluisteren laag blijft. Immers, de gebruiker kan van de LSP diensten gebruik blijven maken. In de andere twee gevallen, UZI-pas gestolen/uitgeleend of UZI-pas verkregen via medewerking van het UZI-register.

Urgentie

Skimming

De kans dat een kwaadwillende gegevens van een UZI-pas wil lezen en kopiëren op een andere pas is iets waar zeer specialistische kennis voor benodigd is. Daardoor is de kans zeer laag. De omvang is echter groot wanneer men dit wel voor elkaar heeft gekregen. Dit levert een lage risicofactor op. De CIA voorziet een hoge score wanneer over de inloggegevens wordt beschikt voor de aspecten confidentiality en integrity, waarbij privacy en juist- en volledigheid in gevaar komen. De beschikbaarheid blijft ongewijzigd. Vanwege de ontwikkelingen om informatie van een chip te dupliceren, de hoge omvang bij een succesvolle attack en de beïnvloeding van de twee aspecten wordt het "noodzakelijk" geacht extra aandacht te besteden aan het voorkomen van een dergelijke attack.

Afluisteren communicatie UZI-paslezer en UZI-pas

Hoewel ook hier de kans laag is omdat het wat inspanning, tijd, specialisme en vooral de juiste informatie vereist om daarmee vervolgens het systeem te kunnen betreden (met of zonder de persoonlijke inlogitems) staat een succesvolle attack wel in voor een grote omvang. Eenmaal gevonden welke informatie verantwoordelijk is voor de verificatie kan er voor zorgen dat ook andere zorgverleners zonder dat zij het weten slachtoffer worden. Ook hier geldt dat de availability geen schade zal ondervinden van dit alles. De confidentialily en integrity wel wanneer men al over de inloggegevens van de zorgverlener de beschikking heeft. Immers heeft men al een deel van de inlogprocedure in handen. De encryptie en andere beveiligingsmaatregelen storen in dit principe het succes. Desondanks is het verstandig "noodzakelijk" om er toch zeker van te zijn dat een dergelijke kwaadwillende actie niet kan worden uitgevoerd.

Afpakken / stelen / lenen UZI-pas van gebruiker

Deze attack kenmerkt zich door de eenvoud van de aanval. Zowel de risicofactoren als de CIA-aspecten scoren beide hoog. De effectiviteit wordt nog eens versterkt wanneer de kwaadwillende ook over de inloggegevens beschikt die bij de UZI-pas horen. Het wordt dan uitermate eenvoudig om toegang te krijgen tot het LSP en informatie van patiënten die bij de bevoegdheden horen van de houder van de pas. Het is “meer dan noodzakelijk” om te zorgen dat zorgverleners zich bewust zijn van de mogelijkheid tot het hanteren van deze aanval en dat uiteindelijk ook zij verantwoordelijk zijn voor hun gedrag en de correctheid van de informatie die zij beheren.

Via UZI-pas medewerker

Een kwaadwillende die via een medewerker van het UZI probeert op welke wijze dan ook een UZI-pas te verkrijgen, al dan niet met bijbehorende toegangscode, is een attack die wanneer de procedures worden gevolgd zich niet mag voordoen. De kans dat dit ook daadwerkelijk zal gebeuren is klein omdat bij het verkrijgen van een UZI-pas meerdere afdelingen zijn betrokken die hun goedkeuring moeten geven. De kans dat dit zich zal voltrekken is klein, omdat er vanuit mag worden gegaan dat bij het UZI-register iedereen zich aan de procedures gaat houden. De omvang is uiteraard heel hoog, wanneer het toch mogelijk mocht zijn dat een UZI-pas onterecht wordt uitgereikt. De effecten op de CIA aspecten vormen op de gebieden confidentiality en integrity een groot risico, terwijl ook nu weer de availability ook hier niet negatief wordt beïnvloed. Het is daarom “niet direct noodzakelijk” om hier tegen actie te ondernemen.

Aanbevelingen

Skimming

Dat skimming een ernstig probleem is bewijst de problemen die banken hebben. Ook pasjes met een chip zullen steeds vaker worden geconfronteerd met dergelijke praktijken om informatie die op de chip staat te verkrijgen. Tot op heden is de chip en het gebruik veilig doordat communicatie is versleuteld en verkrijgen van informatie specialistische apparatuur vereist. Mocht desondanks een pas succesvol gedupliceerd worden dan zal het systeem moeten detecteren dat het een valse UZI-pas betreft dat niet door de officiële instanties is uitgegeven. De pas wordt door deze controle onbruikbaar. Wanneer ook dit probleem kan worden verholpen, is men aangewezen op de logs.

Afluisteren communicatie UZI-paslezer en UZI-pas of afpakken / stelen / lenen UZI-pas van gebruiker

Om kopiëren, afluisteren, stelen etc. van een pas door een kwaadwillende tegen te gaan moeten de gebruikers bewust worden gemaakt van het feit dat de UZI-pas een persoonlijk voorwerp is waarvoor zij persoonlijk de verantwoordelijkheid dragen en bij misbruik hier op kunnen worden aangesproken. De gebruikersverklaring die aan de zorgverleners worden aangeboden biedt juridische mogelijkheden om, hoewel achteraf, maatregelen te nemen tegen het onverantwoordelijke gedrag van de zorgverlener en het nalaten van het nemen van actie. Het afluisteren van de communicatie kan deels worden voorkomen door de apparatuur goed te controleren voor deze in gebruik te nemen en het systeem waarop men werkt met enige regelmaat te inspecteren op de aanwezigheid van software dat daar niet op thuis hoort.

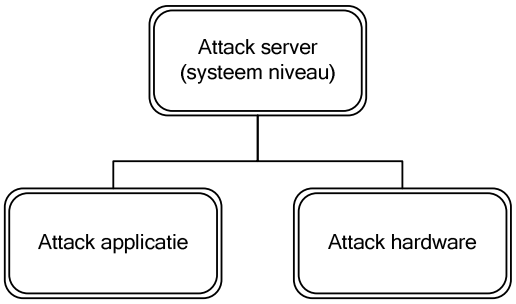
Via UZI-medewerker

Om misbruik tegen te gaan rondom de uitgifteprocedures van een UZI-pas zal men controlepunten moeten in bouwen die er voor moeten zorgen dat het onmogelijk is voor een UZI-medewerker een pas zelfstandig uit te geven. Datzelfde principe hanteren de Nederlandse gemeentes nu bij de aanvraag van een nieuw Nederlandse paspoort. Een paspoort wordt pas uitgegeven nadat deze het gehele traject heeft doorlopen wat over diverse schijven in de organisatie plaats heeft.

8.6 Systeem niveau: attack server

8.6.1 Inleiding

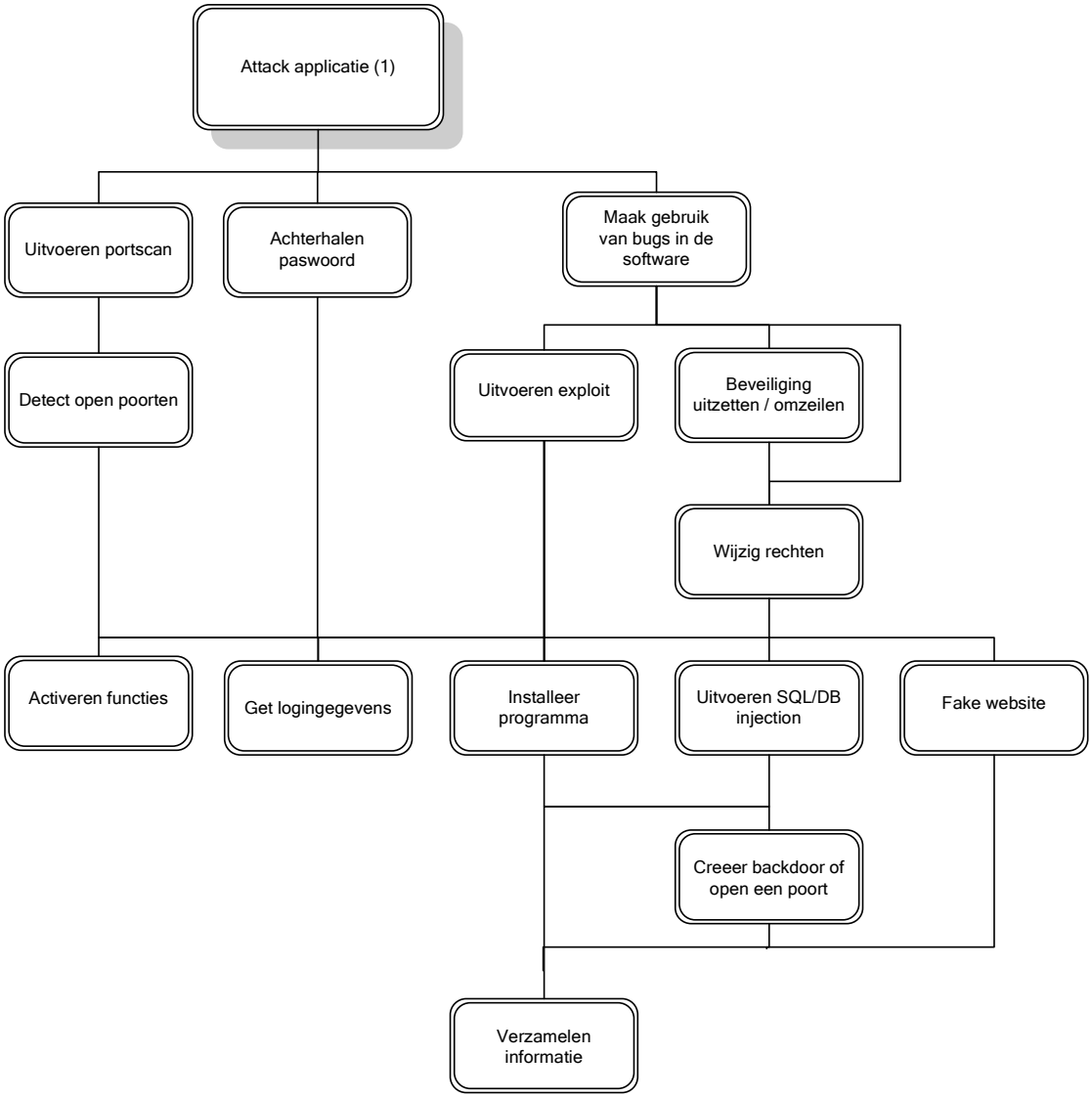
Risico's welke in dit niveau voorkomen hebben betrekking op mogelijke aanvallen welke voortvloeien uit zwakke plekken die een kwaadwillende kan gebruiken rondom de hard- en software van het LSP.



Figuur 8.9: Attack tree op systeem niveau

Attack tree "attack applicatie" is vanwege de enorme omvang opgedeeld in drie bomen en komen respectievelijk gedetailleerd aan bod in secties 8.6.2, 8.6.3 en 8.6.4. In de secties 8.6.5 en 8.6.6 wordt uitvoerig aandacht besteed aan de attacks op hardwarematig niveau.

8.6.2 Attack applicatie (1)



Figuur 8.10: Attack tree "attack applicatie 1"

Dreigingen en gevolgen

Portscan

Een poortscan wordt veelal gebruikt om een overzicht te krijgen van de poorten op een computersysteem die niet zijn beveiligd. Een systeem bevat vele duizenden zogenaamde communicatiepoorten het computersysteem bepaalde diensten als FTP, Email, HTTP of P2P kan uitvoeren. Een open poort hoeft geen probleem te zijn, echter een aanvaller kan wanneer deze hiervan op de hoogte misbruik maken van deze poort door daar opdrachten over te versturen die het systeem bereiken waardoor er nieuwe attack mogelijkheden voor hem ontstaan. Wanneer een kwaadwillende zich eenmaal toegang heeft verschaft kunnen de er nieuwe attacks op het systeem worden losgelaten.

Het scannen van poorten van een systeem is toegestaan en mag door iedereen worden uitgevoerd. Dit omdat een poortscan niet altijd de bedoeling heeft om kwaadwillend te zijn. Er zijn namelijk software-applicaites die het portscanprincipe gebruiken om netwerkproblemen op te kunnen sporen.
Ondanks dat een poortscan niet een bedreiging is, wordt deze veelal wel gezien als een voorbode op een mogelijke inbraakpoging op het systeem. Het risico wordt aanzienlijk vergroot wanneer deze met het internet is verbonden. Het systeem krijgt dan vele keren per dag te maken met het dergelijke verzoeken.

Achterhalen password
Om de applicatie te kunnen gebruiken kan het zijn dat er specifieke gegevens, zoals een wachtwoord, benodigd is. De attackmethodes en de daaruit voortvloeiende dreiging zijn besproken in de secties 8.5.2 tot en met 8.5.5.

Maak gebruik van bugs
Een bug is een error, flaw, mistake, failure of fault in een computerprogramma dat er voor zorgt dat het programma niet meer werkt zoals het bedoeld is of een resultaat oplevert wat niet de bedoeling van de programmeur was. Bugs worden veroorzaakt door fouten in de programmacode of het ontwerp gemaakt door de ontwerpers. Veel bugs worden door het uitvoeren van tests gevonden nog voordat de software wordt vrijgegeven voor gebruik. Ondanks die vele tests kan het toch voorkomen dat er fouten in de applicatie onopgemerkt blijven. Deze kunnen zich tijdens het gebruik van de software tot problemen ontpoppen die in het geval van levensafhankelijke systemen vergaande gevolgen teweeg kunnen brengen. Indien een kwaadwillende op de hoogte is van een onopgemerkte bug en daarvan gebruik maakt, is de betrouwbaarheid van het systeem in het geding en kan niet meer met zekerheid gesteld worden of de toegankelijke informatie juist is.

Belang van bescherming

Uitvoeren portscan
Wanneer niet wordt over gegaan tot bescherming tegen poortscans hoeft wil dat niet direct zeggen dat het systeem gevaar loopt. Immers niet elke poortscan hoeft een attack te betekenen. Wel maakt een poortscan veelal deel uit van een groter geheel en wordt het gezien als een op handen zijnde aanval. Wanneer eenmaal een “open poort” gevonden en kwaadwillende gebruik kunnen maken van deze mogelijkheid in het systeem, zal het slechts een kwestie van tijd zijn voordat er een aanval wordt uitgevoerd. De gevolgen laten zich niet voorspellen.

Achterhalen password
Wachtwoorden en inloggegevens moeten te alle tijden beschermd worden. Voor details zie de secties 8.5.2 tot en met 8.5.5.

Maak gebruik van bugs
Fouten in applicaties vormen een reëel risico. Wanneer een aanvaller eenmaal op de hoogte is dat er een fout in de software aanwezig is, kan hij deze op allerlei manieren misbruiken. Een aantal opties zijn al in

diverse attack trees beschreven. Bescherming is van belang omdat het de betrouwbaarheid van de infrastructuur die de gebruikers in grote mate beïnvloed.

Risicofactor

Uitvoeren portscan

De risicofactor voor deze attack wordt geschat op: 3 (kansfactor) x 1 (omvangfactor) = 3 (risicofactor).

Achterhalen password

De risicofactor voor deze attack wordt geschat op: 2 (kansfactor) x 3 (omvangfactor) = 6 (risicofactor).

Maak gebruik van bugs

De risicofactor voor deze attack wordt geschat op: 2 (kansfactor) x 3 (omvangfactor) = 6 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA zijn de volgende cijfers beraamd:

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Doormiddel van het uitvoeren van een portscan probeert een kwaadwillende er achter te komen welke poorten open staan om vervolgens te trachten toegang tot het systeem te krijgen om instellingen te wijzigen.	1	1	1
• Door het achterhalen van wachtwoord of inloggegevens van een applicatie krijgt men toegang tot de applicatie waardoor instellingen gewijzigd kunnen worden, extra rechten kunnen worden toegekend aan een gebruiker of logs kunnen worden verwijderd.	3	3	3
• Kwaadwillenden maken gebruik van fouten in de software, de dreiging die hiermee ontstaat, kan grote gevolgen hebben voor een systeem omdat de bugs soms niet bekend zijn waardoor het systeem risico's loopt.	3	3	3

Tabel 8.6: Effecten attack "attack applicatie 1" op de CIA

Poortscan

Attacks uitvoeren met behulp van applicaties herbergt vele mogelijkheden. Het effect op de aspecten door het uitvoeren van een poortscan heeft geen effecten op de CIA. Er mag vanuit worden gegaan dat alle poorten zodoende dicht zijn getimmerd dat er geen “open poorten” kunnen worden ontdekt die mogelijkerwijs toegang tot het LSP kan worden gerealiseerd. De risicofactor is de enige score die in dit geval maximaal scoort vanwege de eenvoud tot uitvoeren daarvan maar desondanks dat bruikbare informatie oplevert waarmee de kwaadwillende vervolgstappen kan ondernemen.

Achterhalen wachtwoord

Toegang tot applicaties die direct invloed hebben op het LSP en dus ook indirect invloed hebben op de patiëntinformatie en de betrouwbaarheid daarvan beïnvloeden zowel de CIA-aspecten in negatieve zin alsmede de omvangsfactor. De risicofactor echter is heel laag waardoor de prioriteit slechts geclassificeerd wordt op “noodzakelijk” om tegen dit soort aanvallen iets te doen.

Maak gebruik van bugs

Deze attack maakt gebruik van fouten in de software die door de diversie tests zijn geslopen of simpelweg niet zijn ontdekt. Bugs geven een dermate hoge risico dat de beveiliging hiermee zodanig geconfronteerd wordt dat het een risico vormt voor zowel het systeem als de informatie die daarop wordt gedeeld.

Indien een systeem of programma niet naar behoren is gepatched of bestanden of functies door een virus zijn aangetast, kan het voorkomen dat een kwaadwillende misbruik kan proberen te maken van de ontdekte fout. Omdat we het hier hebben over een systeem dat afhankelijk van meerdere applicaties en systemen is het niet onwaarschijnlijk dat er na ingebruikname ervan, ondanks de nodige tests, er fouten worden ontdekt en zelfs worden misbruikt. De kansfactor, de risicofactor alsmede de CIA-aspecten tonen aan dat het risico zeer groot is en daarom is het “zeer noodzakelijk” dat hier direct extra aandacht aan wordt besteed om zowel de kans als de omvang zo klein mogelijk te maken en houden. Dit om eventuele grote gevolgen uit te sluiten, waardoor het imago van het LSP geen deuk zal oplopen.

Urgentie

Poortscan

Deze attack laat in de CIA zien dat uitvoering ervan geen directe gevolgen hoeft te hebben op de aspecten beschikbaarheid en integrity. Het beïnvloed in lichte mate de vertrouwelijkheid. Maar, ook hier is het effect niet extreem hoog. Dit vanwege het feit dat de attack voornamelijk wordt gebruikt om informatie in te winnen en niet direct een attack mee uit te oefenen. Echter, het resultaat daarvan kan wel een intentie zijn om een (doelgerichte) attack uit te voeren. Vanwege de beperkte risicofactor en de classificatie wordt deze attack als “minder noodzakelijk” geschat. Dit ook vanwege het feit dat de huidige systemen veelal standaard zijn voorzien van hardwarematige oplossingen om dit soort attacks heel goed kunnen verwerken.

Achterhalen wachtwoord
Voor details zie sectie 8.5.2 tot en met 8.5.5.

Maak gebruik van bugs
De kans en de omvang dat deze attack teweeg kan brengen is niet voorspellen en vooral afhankelijk van het type fout dat wordt gevonden en gebruikt om het uiteindelijke doel te bereiken. De risicofactor laat dit ook zien, net zoals de CIA-classificatie die op alle fronten hoog scoort. Wat vooral te wijten is aan de grote diversiteit aan mogelijke fouten. Want dat er fouten in de applicatie gaandeweg worden gevonden is vrijwel gegarandeerd, vooral ook vanwege de omvang van dit project de belangen die er mee gemoeid zijn. Alleen daarom is het aan te raden extra aandacht te besteden om fouten zoveel mogelijk eruit te halen en houden. Dit komt de betrouwbaarheid van de gebruikers en patiënten in het project, de applicatie en de zorg alleen maar ten goede.

Aanbevelingen
Uitvoeren portscan
Hoewel poortscans zelf niet gevaarlijk zijn, kan de kennis die een kwaadwillende hiermee vergaart wel degelijk enig effect op het systeem hebben.

Om te voorkomen dat een kwaadwillende een poort vindt waarvan deze misbruik kan maken is het verstandig een firewall en een IDS in het netwerk op te nemen. De firewall kan verzoeken tegen houden en poorten beschermen en zelfs onzichtbaar voor detectie maken. Een IDS kan detecteren vanwaar de scan poging afkomstig is, detecteert kwaadwillend netwerkverkeer dat niet door een firewall kan worden gedetecteerd, kan gegevens van event vastleggen.

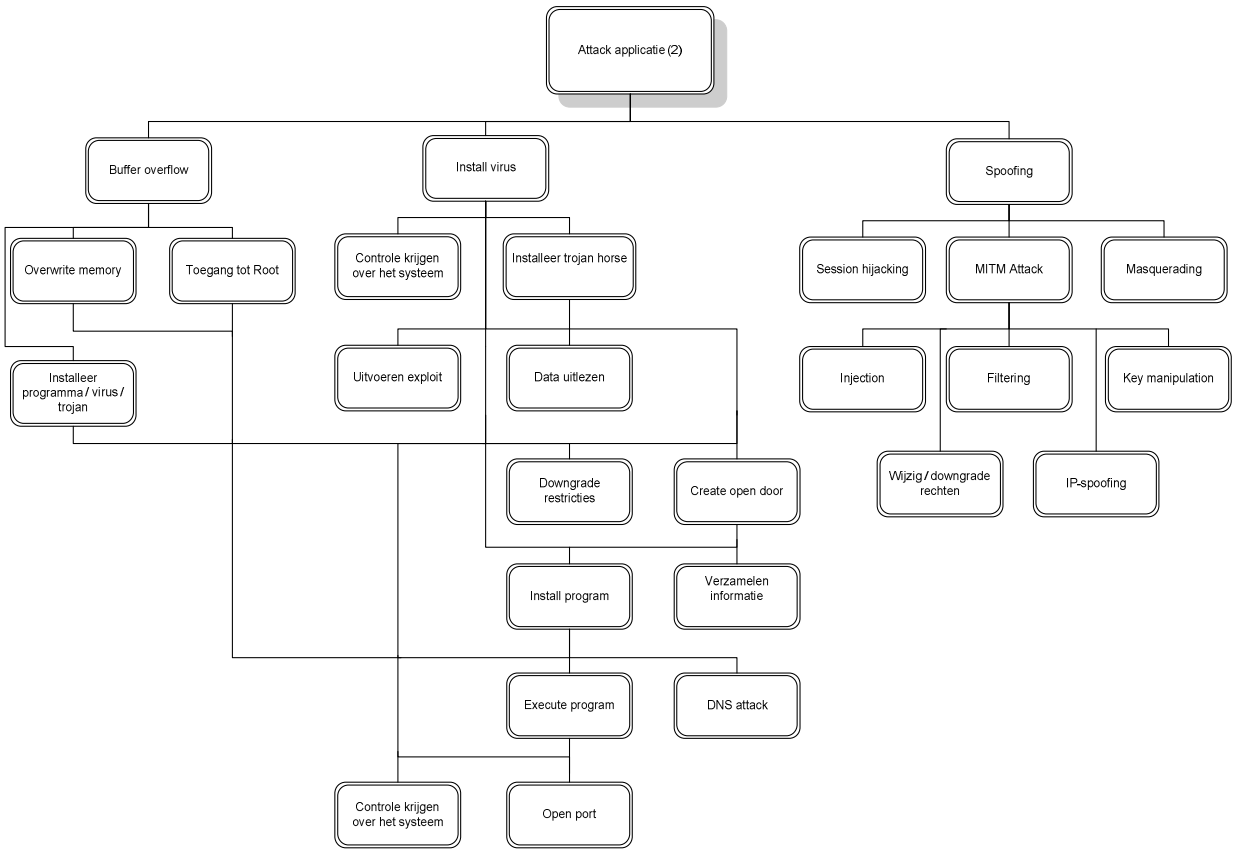
Achterhalen password
Voor details zie sectie 8.5.2 tot en met 8.5.5.

Maak gebruik van bugs
Hoewel fouten in de software ook nog na vele tests voor zullen blijven komen is een feit. Vooral het feit dat er meerdere applicaties bij de zorgverleners van diverse zorginstanties gebruik maken kan betekenen dat er fouten kunnen optreden tijdens bijvoorbeeld het uitwisselen van bepaalde informatie of verzoeken. Uiteraard hebben beheerders er baat bij dat deze fouten zo snel mogelijk worden opgelost, al is het maar om de onrust weg te nemen en de betrouwbaarheid van de applicatie, door het oplossen van de fout(-en), in ieder geval te houden zoals die is en zelfs te verbeteren.

Een veel gebruikte methode om fouten vroegtijdig op te sporen is om de applicatie en de systemen afzonderlijk maar ook samen grondig te testen. Door middel van regressietests kan men het systeem logischerwijs uitbreiden met nieuwe modules die foutloos functioneren. Naast het testen is het gebruik van formele methoden, waarmee wordt bewezen of onderdelen van software en het geheel ook daadwerkelijk voldoen aan de vooraf gestelde eisen. Samen met de technische kwaliteitscontrole en de systeemtests kan men een systeem opleveren dat vrijwel foutloos kan functioneren.

Desondanks de vele bewijzen en tests veroorzaken, om welke reden dan ook, fouten in de software regelmatig problemen. Ingeval van een ontdekking is het noodzakelijk de software zodanig snel en constructief te verbeteren dat de gebruiker er zo min mogelijk hinder van ondervind, de informatie daarna nog altijd is te vertrouwen en de daardoor betrouwbaarheid blijft gewaarborgd.

8.6.3 Attack application (2)



Figuur 8.11: Attack tree “attack applicatie 2”

Dreigingen en gevolgen

Buffer overflow

Door méér data weg te schrijven in een (tijdelijke) buffer van de computer dan daar ruimte voor is gereserveerd kan er een buffer overflow optreden. Met een dergelijke overflow kan men misbruik maken van een slechte controle van de input van data en overschrijft data die normaliter niet overschreven mag worden. Dit heeft als gevolg dat een procedure, applicatie of server incorrecte resultaten geeft, crasht of dat een kwaadwillende zelf specifieke “opdrachten” en procedures kan uitvoeren die onder normale omstandigheden niet (door hem) uit te voeren zijn.

Install virus

Een virus is een kwaadwillend stuk software dat zich verbind aan een computerbestand, zich zelfstandig kan verspreiden en zelfs muteren. Virussen zijn een grote bedreiging voor organisaties en hun informatie. Zij kunnen veel schade aan zowel op het systeem als in de bedrijfsvoering aanrichten. Niet geheel onterecht dat er daarom ook een hele beveiligingsindustrie hieromheen is ontstaan. Een kwaadwillende die een virus heeft geschreven kan deze de meest uiteenlopende opdrachten meegeven waardoor bestanden niet meer toegankelijk zijn, worden verwijderd of gebruikt worden om juist nog meer schade aan te richten. Virussen als trojan horses hebben daarnaast zelfs de functie om zichzelf voor te doen als een “onverdacht” stukje software dat zichzelf ook nog eens over het netwerk kan verspreiden en daardoor meerdere computers kan besmetten.

Met een virus kan een kwaadwillende, wanneer voordat deze zijn destructieve toepassing uitvoert worden gedetecteerd, taken of functies uitvoeren die normaliter niet mogelijk zijn. Dat dit onherstelbare schade met zich mee kan brengen is vast en zeker voor te stellen.

Spoofing

Spoofen is afkomstig van het Engelse werkwoord “to spoof” wat zoveel als “voor de gek houden” betekent. Met deze attack probeert men de identiteit, via het internet, van een persoon aan te nemen zonder dat voor andere partijen duidelijk is dat ze niet communiceren met de persoon die zegt dat hij is. Dit is handig om zo informatie te weten te komen die normaal alleen met de rechtmatige persoon wordt uitgewisseld.

Spoofing kan op meerdere manieren worden uitgevoerd. Drie veel voorkomende technieken zijn:

- **Masquerading**: Wordt gebruikt om informatie van de onoplettende gebruiker te verkrijgen doordat deze identificerende informatie invoert omdat deze het verschil niet opmerkt tussen de originele applicatie en de nagemaakte applicatie en er zodoende vanuit gaat dat hij met de correcte applicatie communiceert. Een kwaadwillende kan door gebruik te maken van deze methode belangrijke informatie te weten komen.
- **Session hijacking**: Bij session hijacking zal een kwaadwillende proberen een sessie tussen rechtmatige gebruiker en LSP te onderscheppen om zo alsnog toegang te verkrijgen tot het systeem. De kwaadwillende zal dan proberen de onderschepte sessie met de rechten van de rechtmatige gebruiker voort proberen te zetten zonder dat de gebruiker als het systeem hiervan op de hoogte zijn.
- **Man-in-the-middle-attack**: Bij een man-in-the-middle-attack participeert de aanvaller, in tegenstelling bij een session hijacking, al vanaf de start van een sessie mee [SCH00]. Waarbij uiteindelijk zowel de rechtmatige gebruiker als het systeem denken dat ze met elkaar praten maar dat beide doen via de aanvaller. Indien er waardevolle informatie tussen beide wordt verzonden kan vervolgens de aanvaller hier van profiteren en de informatie verkrijgen waarmee deze vervolgacties kan uitvoeren.

Belang van bescherming

Buffer overflow

De gevolgen die een buffer overflow kan genereren is moeilijk in te schatten vanwege het feit dat een buffer overflow niet direct tot problemen hoeft te leiden. Desondanks is er een aannemelijk belang om het systeem te beschermen tegen dit risico omdat het systeem hierdoor ontregeld kan raken, de kwaadwillende wijzigingen kan uitvoeren, functies activeren of informatie kan opvragen die normaliter beveiligd zijn met de nodige gebruikers- en systeemrechten.

Install virus

Een populaire wijze om een virus te verspreiden is via email. Elk systeem dat aan een netwerk is aangesloten kent een verhoogd risico wat betreft het ontvangen van virussen. Veelal door de onwetendheid van de gebruiker wordt het virus geactiveerd en verspreid. Wat de gebruiker zich veelal niet realiseert is het risico en de kans op schade die hij en de organisatie loopt door het onprofessioneel gebruiken van email maar ook van het internet. Wanneer een systeem eenmaal is geïnfecteerd is, vooral bij organisaties die gebruik maken van netwerken, de kans zeer groot dat andere systemen ook besmet raken met het virus. Wanneer eenmaal een virus actief is kan dit grote problemen veroorzaken op diverse gebieden zoals vertraging in het netwerk, bestanden onherstelbaar beschadigen of informatie wordt verminkt. Wat vrijwel altijd resulteert in fikse schade.

Spoofing

Het risico van spoofing is dat iemand de identiteit van een ander probeert over te nemen, zonder dat een derde partij hiervan op de hoogte is. Welke techniek ook wordt gebruikt, het blijft een uiterst effectieve methode om te gebruiken en duid er veelal op dat er iets groots staat te gebeuren. Veelal wordt spoofing gebruikt om een achterdeur in het systeem in te bouwen waarna misbruik van het systeem voor een kwaadwillende eenvoudiger wordt.

De kans dat men dit deze methode gaat proberen uit te voeren is meer dan reëel. Deze kan echter nog groter worden wanneer in een later stadium geplande patiëntendossier ook voor de patiënt zelf beschikbaar komt. Immers, zij communiceren wel met het LSP via een onbetrouwbare computer en verbinding.

Risicofactor

Buffer overflow

De risicofactor voor deze attack wordt daarom geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

Install virus

De risicofactor voor deze attack wordt daarom geschat op: 3 (kansfactor) x 3 (omvangfactor) = 9 (risicofactor).

Spoofing

De risicofactor voor deze attack wordt daarom nu geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA zijn de volgende cijfers beraamd:

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Door het uitvoeren van een buffer overflow probeert een kwaadwillende het systeem binnen te treden anders dan via de inlogprocedure, hij tracht daarbij mogelijkerwijs taken uit te voeren die normaliter niet zijn uit te voeren.	3	3	3
• Door het installeren van een virus op een pc probeert een kwaadwillende toegang te krijgen tot de besmette pc en via deze pc verder in het netwerk binnen te dringen, de pc af te luisteren of gegevens te bemachtigen.	3	3	3
• Door spoofing te gebruiken probeert een kwaadwillende de gebruiker te misleiden en zodoende zijn inloggegevens te verkrijgen, de communicatie af te luisteren en zich voor te doen als een andere partij en daardoor voor hem belangrijke informatie te verkrijgen.	3	3	1

Tabel 8.7: Effecten attack “attack application 2” op de CIA

De drie attacks worden de effecten op de aspecten gemiddeld tot hoog gewaardeerd. De vertrouwelijkheid is gemiddeld omdat door een buffer overflow, virus of spoofing het risico toch aanwezig is dat een dergelijke attack ingezet kan worden. Immers door inzet van een van deze technieken behoort het tot de mogelijkheden om bij de informatie te kunnen inzien. Tevens kan de informatie ook worden gewijzigd. De lees- of wijzigopdracht verschillen in dat opzicht niet veel, zodat wijzigen van gegevens ook mogelijk zou kunnen zijn. In geval van de buffer overflow en virus attacks zou het mogelijk kunnen zijn dat de beschikbaarheid in het gedrang komt. Dat dit kan gebeuren is aannemelijk. De beschikbaarheid bij de attack spoofing is ook redelijk hoog omdat door middel van spoofing niet gegarandeerd kan worden dat de gebruiker het systeem nog kan benaderen, omdat een attack mogelijk herleid naar een andere, onjuiste, locatie. De effecten van de dreigingen op de CIA-aspecten zijn niet alarmerend hoog omdat de technieken

die worden gebruikt in alle gevallen, bij een GBZ niet mogelijk zouden moeten zijn. Virussen mogen niet mogelijk zijn, omdat anders er geen sprake is van een GBZ en spoofing is te vermijden door bijvoorbeeld te kiezen voor een gesloten netwerk. Meer methodes om deze attack tegen te gaan in de volgende sectie.

Urgentie

Buffer overflow

Hoewel de kansfactor laag wordt geschat kan de eventuele omvang grote gevolgen hebben voor het systeem en de informatievoorziening daarvan. Vandaar ook de hoge score hierop. De effecten op de CIA-aspecten zijn zeer hoog omdat nadat de buffer overflow succesvol heeft plaats gevonden de kwaadwillende feitelijk en afhankelijk van de mogelijkheden alles kan doen in het systeem. De informatie kan hierdoor onbetrouwbaar worden, of onjuist, privacy kan worden geschonden, logbestanden kan worden gewijzigd e.d. Ondanks de lage geschatte kans is het desondanks “noodzakelijk” aandacht te besteden aan deze vorm van misbruik door de kwaadwillende.

Install virus

Het gebruik van een virus is een methode waarop een hele industrie van profiteert met het leveren van virusdefinities om de virus onschadelijk te maken. Ondanks dat alle systemen zeer waarschijnlijk zijn uitgevoerd met dergelijke scanners zorgt dat niet ervoor dat virussen niet meer voor zouden kunnen komen en schade kunnen aanrichten. De kans op het krijgen van een virus is desondanks nog steeds hoog, maar ook de omvang die een virus kan hebben is ook, ondanks de genomen maatregelen nog steeds hoog. Dit is te wijten aan het feit aan de constante ontwikkelingen die ook in virusland nog steeds doordendert. Gevolgen die een eventuele virus zou kunnen veroorzaken heeft daardoor ook effecten op de CiA-aspecten. Deze zijn vanwege de hoge kans en hun onbekende invloed hoog geschat. Dit zorgt ervoor dat het voor deze attack “zeer noodzakelijk” is om hier extra aandacht en maatregelen tegen te nemen waardoor een eventuele uitbraak voortijdig kan worden onderschept de geschatte omvang niet realiteit wordt.

Spoofing

Bij spoofing probeert de kwaadwillende onder valse voorwenselen de zorgverlener te doen geloven dat hij te maken heeft met het contact, persoon, computer, applicatie waarvan hij verwacht dat deze te vertrouwen is maar dat niet is. De kwaadwillende zal zo proberen voor hem belangrijke informatie te verkrijgen waardoor hij vervolgens misbruik kan maken van deze informatie door deze te gebruiken op het systeem waarvoor het wel bedoeld is. De kwaadwillende kan dan onder het account van de zorgverlener inloggen. Het risico dat zich op het LSP zal afspelen is niet groot, vooral vanwege het feit dat zorgverleners zonder een UZI-pas geen toegang hebben tot het systeem. Mocht een kwaadwillende dus de beschikking hebben over een UZI-pas en op een slimme manier de inloggegevens weet te verkrijgen via spoofing zonder dat de zorgverlener hiervan op de hoogte is, is dit een aanval die zeer effectief is. Vooral gebruikers die het niet zo nauw nemen met de beveiligingsmaatregelen of niet op de hoogte zijn van deze mogelijkheden is het een effectieve methode. De omvang van deze attack kan dan ook zeer groot zijn. De CIA-aspecten tonen aan dat behalve voor de beschikbaarheid de een hoge score geldt. Immers de privacy als de juistheid valt wanneer een kwaadwillende is toegetreden, niet meer te garanderen. Doordat deze attack is pas effectief wanneer de kwaadwillende ook daadwerkelijk al over de UZI-pas beschikt. Zonder pas wordt het

een moeilijk verhaal waardoor de kans op een dergelijke aanval zeer klein wordt en niet de moeite is. Vanuit deze achterliggende gedachte is het ondanks de hoge CIA en omvangsfactor “minder noodzakelijk” om aandacht te besteden aan deze attack. De prioriteit is daarom laag.

Aanbevelingen

Buffer overflow

Een buffer overflow is relatief eenvoudig op te lossen door in de buffer de mogelijkheid om executeerbare code uit te voeren, te blokkeren. Dergelijke code genereert namelijk extra data in de buffer waardoor deze kan overlopen en de pointer in een gedeelte van de buffer terecht komt waardoor opdrachten in het systeem mogelijk worden die normaliter alleen door specifieke gebruikers zijn te activeren of niet mogelijk zijn.

Naast het blokkeren van executeerbare code zal men ook de broncode secuur moeten controleren en testen op gevaarlijke condities die een buffer overflow kunnen veroorzaken. Het afvangen van veel voorkomende fouten die al reeds bekend zijn beperkt de mogelijkheden van een kwaadwillende.

Ook het controleren van de grote van de array die wordt gelezen of weggeschreven naar de buffers is een effectieve methode. Omdat de data wordt gecontroleerd grootte kan er geen overflow optreden. Data die over het maximale bereik van de buffer gaan, kan niet worden opgeslagen. Op deze methode zal zeer waarschijnlijk wel ten koste gaan van de performance, maar biedt een effectieve bescherming.

Install virus

Met behulp van een virusscanner is kwaadwillende software te ontdekken. Hiermee is de bedoeling om dergelijke software voordat deze schade kan aanrichten aan het systeem, af te vangen. Om goede detectie mogelijk te maken zijn de recente virusdefinities benodigd. Desalniettemin dienen beveiligingsmechanismes dan wel up-to-date zijn, anders is effect en de bescherming te verwaarlozen en is er sprake van schijnveiligheid waarop de gebruiker vertrouwd. Door de inzet van detectiepunten als een IDS, backup- en rollbacksysteem kan men de data in de gaten houden, veilig opslaan en wanneer dat noodzakelijk is terughalen.

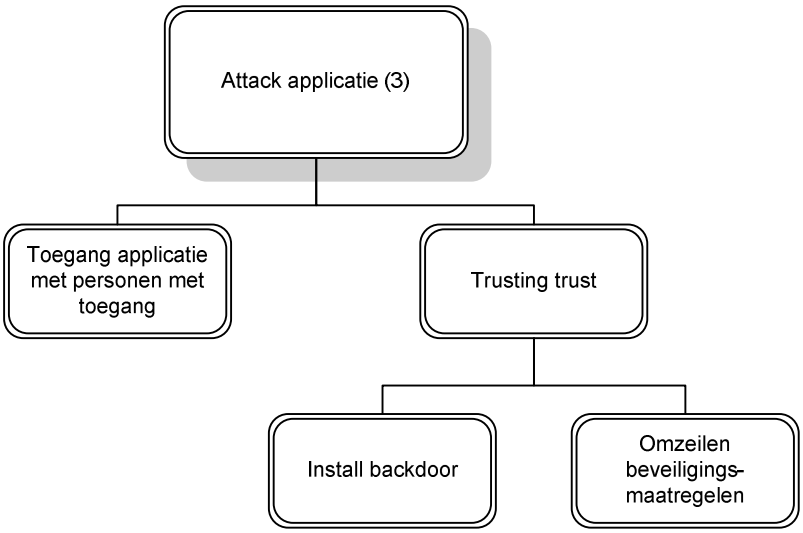
Naast technische oplossingen kunnen ook de gebruikers en beheerders aanzienlijk bijdragen aan een goede bescherming tegen het verspreiden en gebruik van kwaadwillende software. Men zal de gebruikers richtlijnen moeten geven waaraan zij zich dienen te houden tijdens het gebruik van hun systeem. Daarnaast moeten zij geïnformeerd worden over de mogelijkheden wat te doen als er onverhoopt toch een virus op hun pc staat. De systeembeheerders hebben de verantwoordelijkheid om de systemen up-to-date als virusvrij te houden.

Spoofing

Door gebruik te maken van netwerkfirewalls kan men regels opstellen waarin is vastgelegd welke ip-adressen en protocollen in verbinding mogen treden met het LSP systeem. Alleen zo is te garanderen dat alleen verbindingen die op voorhand zijn goedgekeurd contact kan maken met het LSP. Met behulp van

technieken als onder andere Network Adress Translation (NAT) zijn interne netwerkadressen te camoufleren en voor de “buitenwereld” niet zijn te traceren.

8.6.4 Attack application (3)



Figuur 8.12: Attack tree “attack applicatie 3”

Dreigingen en gevolgen

Toegang applicatie met personen met toegang

Details over deze attack zijn reeds beschreven vanaf sectie 8.6.2 tot en met 8.6.5.

Trusting trust

Trusting trust staat voor dat een kwaadwillende aanpassingen of toevoegingen aan de programmacode toevoegt zonder dat andere hiervan op de hoogte zijn en de aanwezigheid opmerken om op een later moment hiermee bepaalde acties mogelijk te maken. De kwaadwillende kan via deze achterdeur het systeem betreden zonder dat dit op deze manier mogelijk mag zijn en hiervan andere weet van hebben om bijvoorbeeld informatie te verzamelen of te manipuleren. De kwaadwillende heeft hiermee de beschikking over een informatiekanaal waarmee hij kan doen wat hij wil, wat veel schade kan veroorzaken. Eventuele gevolgen zou, zonder dat men op de hoogte is van dat er een attack plaats heeft gevonden, grote gevolgen hebben die voornamelijk de betrouwbaarheid zowel in de uitgewisselde informatie als de infrastructuur ernstig schade .

Belang van bescherming

Toegang applicatie met personen met toegang

Details over deze attack zijn reeds beschreven vanaf sectie 8.5.2 tot en met 8.5.5.

Trusting trust

Het belang van bescherming hierbij is dat voorkomen moet worden dat kwaadwillenden onopgemerkt wijzigingen of uitbreidingen aan het systeem doen. Dit zorgt voor een betrouwbaarder systeem welke overeenkomt met de vooraf opgestelde eisen en zorgt er voor dat informatie alleen toegankelijk is voor gebruikers met de juiste rechten. Wanneer blijkt dat er toch ernstige problemen als gevolg van het implementeren van ongecontroleerde ingangen zal het vertrouwen van de patiënt en de gebruikers worden geschaad in zowel het systeem als de beschikbare informatie. Het is daarom in het belang van de patiënt, de gebruikers en de zorgsector dat men de garantie kan geven dat de applicatie geen verborgen functies bevat.

Risicofactor

Toegang applicatie met personen met toegang

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

Trusting trust

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA zijn de volgende cijfers beraamd:

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Toegang tot de applicatie krijgen door gebruik te maken van kennis, het wachtwoord of de diensten van personen met rechtmatige toegang tot de applicatie.	3	3	3
• Doormiddel van trusting trust probeert de aanvaller toegang tot de applicatie te krijgen.	3	3	3

Tabel 8.8: Effecten attack “attack application 3” op de CIA

De effecten op de CIA-aspecten zijn gemiddel tot hoog. Betreffende de attack “*Toegang applicatie met personen met toegang*” krijgen ondervinden de aspecten vertrouwelijkheid en betrouwbaarheid een verhoogd effect omdat de vertrouwelijkheid wordt beïnvloed door het feit dat informatie ook door een kwaadwillende kan worden ingezien. De betrouwbaarheid komt daarmee ook in het geding, omdat wanneer een kwaadwillende via zijn trusting trust methode een achterdeur in het systeem heeft ingebouwd de gegevens van een patiënt eenvoudig kan inzien of zelfs wijzigen waardoor de betrouwbaarheid in het geding komt. En als er gewijzigd kan worden, kan dat misschien ook betekenen dat gegevens niet meer beschikbaar zijn voor de rechtmatige zorgverlener, waardoor de availability ook wordt beïnvloed.

Voor de trusting trust attack geldt dat alle drie de aspecten zeer hoog wordt geschat. Omdat men geen aanwijzingen heeft dat zich al in de realisatiefase een attack heeft plaats gevonden, kan de informatie in principe onvertrouwelijk, onbetrouwbaar en onbeschikbaar zijn of worden voor de zorgverleners en dus de informatievoorziening rondom een patiënt verstoord.

Urgentie

Toegang applicatie met personen met toegang

Details over deze attack zijn reeds beschreven vanaf sectie 8.5.2 tot en met 8.5.5.

Trusting trust

Deze attack biedt een kwaadwillende zeer veel macht en kracht waardoor hij feitelijk de regie kan voeren over een systeem of een applicatie. Vanuit dit perspectief zijn de CIA-aspecten dan ook zeer hoog geschat, vooral vanwege de eventuele gevaren die er kleven aan het feit dat je niet weet of de broncode die wordt geschreven of gecompiled ook te vertrouwen en veilig is. Een eventuele attack middels trusting trust zal een geweldige klap betekenen voor de veiligheid van het systeem, de omvangsfactor is daarom zo hoog geschat. De kans dat zich echter een dergelijk vooraf opgesteld plan daadwerkelijk in een applicatie of systeem wordt ingebouwd, alle tests weet te doorstaan, niet opvalt bij diverse betrokken partijen en de kwaadwillende gebruik kan maken van het door hem gecreëerde mogelijkheden is echter laag. Ondanks de lage kans is het toch noodzakelijk aandacht te besteden dat er desondanks programma's worden opgeleverd die ook daadwerkelijk doen wat ze achten te doen en voldoen aan de vooraf gestelde eisen.

Aanbevelingen

Toegang applicatie met personen met toegang

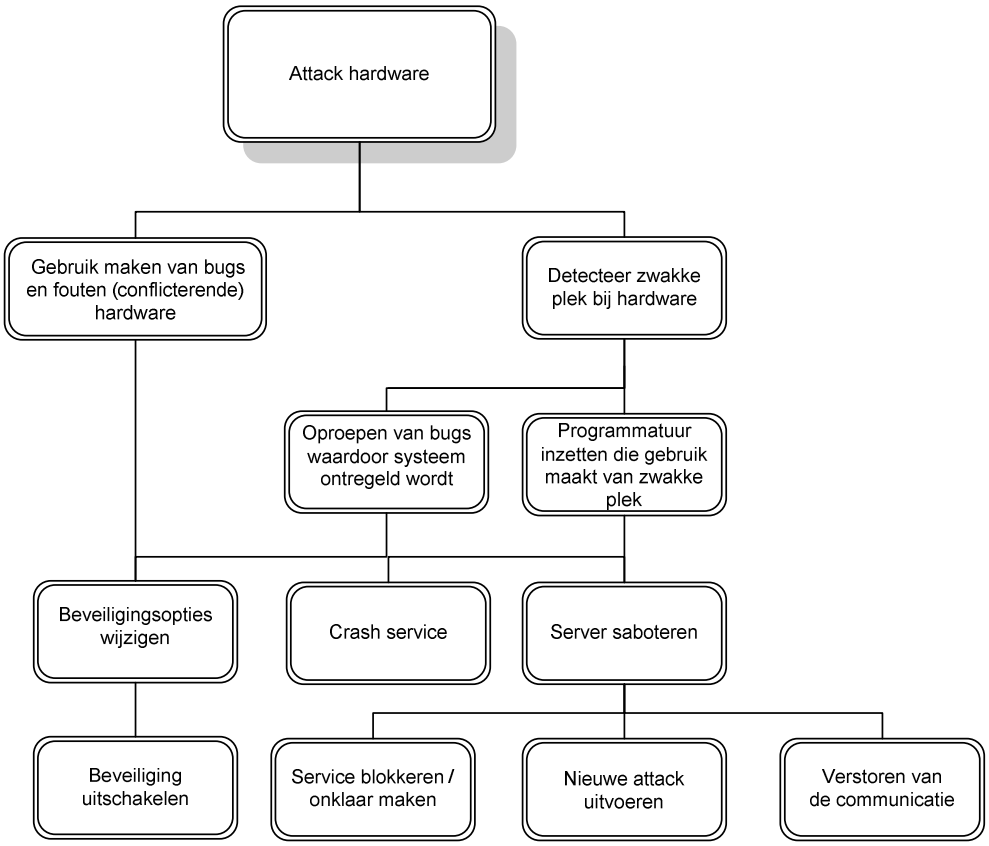
Details over deze attack zijn reeds beschreven vanaf sectie 8.5.2 tot en met 8.5.5.

Trusting trust

Door zowel de broncode als de uiteindelijke gecompileerde code te reviewen, kan men de onbedoelde functies of programmagedeeltes die niet in de applicatie thuis hoort, verwijderen. Een kwaadwillende heeft zo niet de mogelijkheid om deze op een willekeurig moment alsnog te gebruiken.

Door de broncode voor als na het compilen te controleren kan geprobeerd worden te bewijzen dat de software ook doet wat het moet doen en niet meer dan dat. Dit gecontroleerd compilen kan uitgevoerd worden door een techniek dat "Diverse Double-Compiling" [WHE05] wordt genoemd. Aan de hand van deze correctheid kan men aantonen dat de software voldoet aan de vooraf gestelde eisen. Wanneer zowel de broncode áls de uiteindelijk gecompileerde code correct zijn bevonden, mag over worden gegaan tot het testen en uiteindelijk het implementeren van het systeem.

8.6.5 Attack hardware



Figuur 8.12: Attack tree "attack hardware"

Dreigingen en gevolgen

Gebruik maken van bugs en fouten van (conflicterende) hardware

Om toegang te krijgen tot een systeem via de niet vastgestelde wijze heeft een kwaadwillende vele opties. Een daarvan is dat de aanvaller gebruik maakt van fouten die hardware bevatten doordat ze in het systeem aanwezig zijn om de noodzakelijke taken uit te voeren, maar op een aantal toestanden een fout produceren of zelfs in combinatie met elkaar voor problemen zorgen. Beide situaties kunnen ontstaan door slechte configuratie bij installatie of als gevolg van een productie- of ontwerpfout van de fabrikant. De gevolgen bij het niet 100% correct functioneren van de hardware betekent dat men niet er van uit kan gaan dat deze zich onder alle omstandigheden aan de gestelde en verwachte eisen voldoet. Dat kan riskant zijn voor de beschikbaarheid van de systemen en dus de informatie.

Detecteer zwakke plek bij hardware

Wanneer een kwaadwillende gebruik wil gaan maken van bugs in de hardware maar niet op de hoogte is óf deze er zijn en in dat geval waar, kan deze de hardware scannen op mogelijke fouten in de gebruikte hardware. Eenmaal een fout of bug gevonden kan een kwaadwillende vervolgens bepalen of een vervolg attack mogelijk is om zijn uiteindelijke doel te kunnen bereiken en dus het systeem binnen te dringen. Om dergelijke bugs of fouten te vinden is het gebruik van een vulnerability scanner een handig hulpmiddel die

het speurwerk enigszins kan verlichten. Desondanks zijn de gevolgen voor deze attack niet groot vanwege het feit dat het in dit geval alleen het detecteren van de zwakke plekken betreft en niet het daadwerkelijk aanvallen van het LSP.

Belang van bescherming

Gebruik maken van bugs en fouten van (conflicterende) hardware

Hardware in kritische systemen als waarin het LSP zich bevindt zal moeten voldoen aan hoge kwaliteitseisen. Dit om te voorkomen dat er regelmatig fouten of conflicten optreden binnen de systemen waardoor deze niet meer is te benaderen of juist mogelijkheden biedt die normaliter niet aan de orde mogen zijn. Dergelijke problematiek zal men daarom dienen uit te sluiten om er in ieder geval voor te zorgen dat systemen in dit geval systemen niet zijn te benaderen op een wijze zoals dat niet bedoeld is. Immers, het risico mag niet gelopen worden wanneer blijkt dat kwaadwillende door een fout of conflict juist wel toegang tot het systeem heeft gekregen.

Detecteer zwakke plek bij hardware

Wanneer met behulp van een vulnerability scanner een zwakke plek wordt gevonden is er nog geen verhoogd risico. Immers, het betreft hier juist alleen het signaleren van een zwakke plek en niet het profiteren van deze zwakke plek. Uiteraard kan men er van uit gaan dat, net zoals bij de poortscan attack, dit een voorbode is op een mogelijk vervolgattack.

Risicofactor

Gebruik maken van bugs en fouten van (conflicterende) hardware

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

Detecteer zwakke plek bij hardware

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 1 (omvangfactor) = 1 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA zijn de volgende cijfers beraamd:

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Gebruik maken van bugs en fouten van (conflicterende) hardware.	3	3	3
• Detecteer zwakke plek bij hardware.	1	1	1

Tabel 8.9: Effecten attack “attack hardware” op de CIA

De effecten op de aspecten voor de eerste attack zijn de hoogst haalbare score toebedeeld. Dit omdat niet is te bepalen welke bugs of fouten er worden gevonden, men kan gebruiken en welke problemen hieruit zullen ontstaat. Problemen zijn vanwege hun diversiteit moeilijk in te schatten en vanwege de diversiteit aan hardware is het niet onlogisch om een hoge score vast te stellen.
Bij de attack waarbij het doel is een zwakke plek te detecteren, zijn de effecten op de CIA laag. Dit omdat het hier alleen het detecteren van een zwak punt betreft. Verdere actie kan op basis van het gevonden zwakke punt plaats vinden. Echter zal de kwaadwillende hiervoor een vervolg attack moeten uitvoeren dat aansluit bij de gevonden zwakte.

Urgentie

Gebruik maken van bugs en fouten van (conflicterende) hardware

Hoe goed men de code controleert, alle systemen probeert en uittest, fouten blijven desondanks grote voorzorg bestaan en ontstaan. De risicofactor laat voor beide attacks een tweedeling zien. Terwijl de attack, “gebruik maken van bugs en fouten van (conflicterende) hardware”, in de risicofactor een hoge score laat zien is de tweede attack beduidend minder effectief. Echter is het detecteren van een zwakke plek wel een mogelijke voorbode van eventueel op komst zijnd onheil. Immers met de gevonden informatie kan de kwaadwillende gebruik maken van een door hem gevonden fout of minder goed beveiligd onderdeel.

Door eventuele grote gevolgen van onbekende bugs, fouten etc. veroorzaakt door hardware die fouten bevatten of doordat ze niet effectief samen kunnen werken en daardoor enige conflicten veroorzaken levert een CIA classificatie op waarbij de effecten op de aspecten hoog moeten worden geschat. Hoewel vanuit mag worden gegaan dat men vooraf goed heeft bekeken welke hardware er wordt gebruikt, systemen niet zomaar gecertificeerd worden en eventuele problemen snel worden gesignaleerd en verholpen is er een betrekkelijk lage kans op dat kwaadwillenden ook daadwerkelijk misbruik kunnen maken. De omvang wanneer dit wel gebeurd is echter hoog. Voornamelijk als gevolg van de vele mogelijkheden die een eventueel conflict met hardware op kan leveren. Op basis van de CIA-score en de geschatte omvang is geconcludeerd dat het “zeer noodzakelijk” is om te zorgen dat dergelijke problemen niet kunnen voorkomen of anders zeer snel worden opgelost om vooral de betrouwbaarheid te garanderen.

Detecteer zwakke plek bij hardware

Voordat een kwaadwillende daadwerkelijk gebruik kan maken van eventuele bugs, fouten etc. zal hij hiervan wel op de hoogte moeten zijn. Hij zal, wanneer hij hiervoor kiest, opzoek kunnen gaan naar zwakke plekken in het te onderzoeken systeem. Het blijft bij deze attack dus alleen bij het detecteren van eventuele fouten. De volgende stap is het feitelijk uitvoeren van een attack op de gevonden zwakke plek.

Omdat het hier alleen om detectie gaat, dat systeembeheerders ook moeten uitvoeren om te bekijken of er ergens iets niet volgens planning verloopt, zorgt dit voor een lage CIA-score, kans- en omvangsfactor. Mocht een dergelijke detectie worden uitgevoerd door andere dan de hiervoor bevoegde personen, dan mag dit opgevat worden als een eerste inventarisatie waaraan, bij een mogelijke positieve uitslag, een vervolg aan wordt gegeven waarbij de gevonden zwakke plek(-ken) wordt aangevallen. Het is daarom “minder noodzakelijk” om extra aandacht te vragen voor deze attack.

Aanbevelingen

Gebruik maken van bugs en fouten van (conflicterende) hardware / Detecteer zwakke plek bij hardware

Voorkomen dat dergelijke attacks succes heeft is lastig, vooral vanwege de complexiteit van de gehele infrastructuur blijft het moeilijk om het bugvrij en foutloos te maken. Daarbij is altijd een functie, component of code de zwakste in de schakel van het systeem dat eventueel is te gebruiken om het systeem binnen te kunnen dringen. Dat wil echter niet zeggen dat er niets tegen kan doen om dit risico weg te nemen of anders tot het minimale te beperken.

Zo is het verstandig de hard- en software apart als in combinatie met elkaar doorlopend te testen en dit ook te doen wanneer er wijzigingen plaats vinden in de structuur op beide gebieden. Vele problemen kunnen door het uitvoeren hiervan worden voorkomen. De regressie-, systeem- en applicatietests zorgen uiteindelijk voor een hogere betrouwbaarheid van het systeem alsmede een kleiner kans op het ontstaan van fouten, het ontdekken en misbruik daarvan.

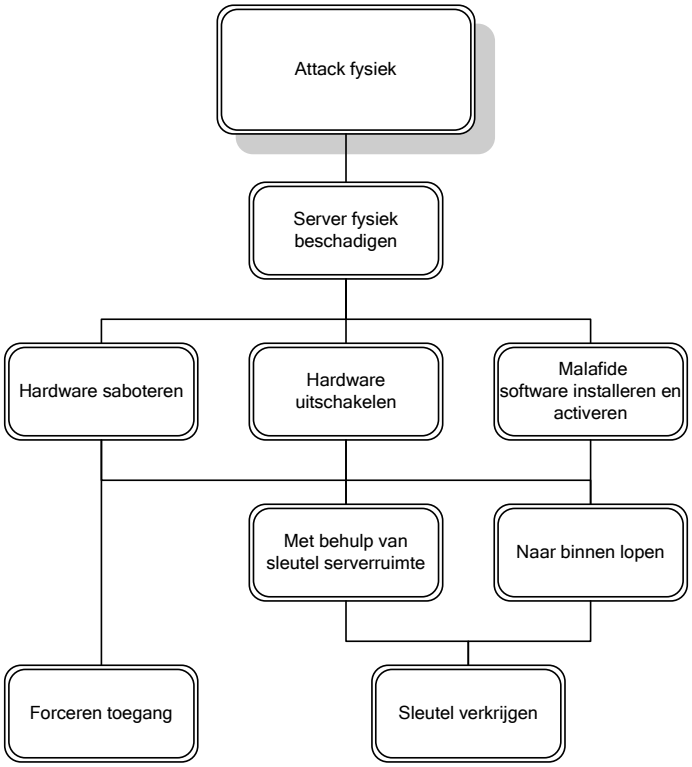
Wanneer zich onverhoopt toch een attack succesvol wordt uitgevoerd en men heeft dit gedetecteerd is het belangrijk het probleem zo snel mogelijk te repareren en de attack in het vervolg onmogelijk te maken. Hierbij is het van belang dat de gebruikers zo min mogelijk last hebben van de ontstane problemen en hun werkzaamheden kunnen blijven uitvoeren met nog steeds betrouwbare informatie. De detectie van een attack valt of staat bij de paraatheid van de beheerders en de toegepaste detectietoepassingen.

8.7 Fysiek niveau: attack fysiek

8.7.1 Inleiding

Dit niveau kenmerkt zich door de attack tree in kaart te brengen die een aanvaller kan uitoefenen op het LSP door fysiek schade aan te richten met als doel het systeem op onrechtmatige wijze te kunnen betreden.

8.7.2 Server fysiek beschadigen



Figuur 8.13: Attack tree “server fysiek beschadigen”

Dreigingen en gevolgen

Server fysiek beschadigen

De dreiging in deze attack bestaat uit het fysiek beschadigen van de server met als uiteindelijke doel daarmee toegang te verkrijgen tot het LSP. Dat toegang krijgen tot de afgesloten serverruimte kan op diverse manieren: door gebruik te maken van een sleutel of andere geldige token (zoals een UZI-pas) al dan niet op rechtmatige wijze verkregen, of door de toegang te forceren.

De wijze waarop een kwaadwillende binnenkomt, is voor deze attack van ondergeschikt belang, omdat het hier betrekking heeft op het fysiek aanvallen van de server en niet het toegang krijgen tot de ruimte.

Wanneer een kwaadwillende zich eenmaal fysiek in de buurt van de server bevindt, kan deze de nodige schade aanrichten en zelfs het systeem of delen daarvan onbruikbaar maken om toegang tot het systeem mogelijk te maken. Gevolgen die dit teweeg zal brengen bij een succesvol uitgevoerde attack zijn niet te overzien, omdat het systeem op dat moment afhankelijk is van de bedoelingen van de kwaadwillende. Desondanks mag duidelijk zijn dat men zich op het ergste moet zijn voorbereid en het systeem zelfs in zijn geheel onbruikbaar kan worden gemaakt. Daarvoor is geen specifieke kennis nodig, maar slechts kwade bedoelingen en brute kracht.

Belang van bescherming

Server fysiek beschadigen

Het mag duidelijk zijn dat het belang is om de bescherming van de servers en de toegang daar naar toe groot zijn. Immers de gehele infrastructuur is afhankelijk van het goed werken van alle benodigde systemen, waardoor het uitwisselen van informatie juist mogelijk wordt gemaakt. Toegang mag alleen mogelijk zijn voor hen die daarvoor zijn bevoegd. Wanneer zich, ondanks alle beveiligingsmaatregelen, er echter een onbevoegde met kwaadwillende bedoelingen zichzelf toegang heeft verschaft tot de serverruimte kan deze het systeem schade toe brengen en/of met behulp van eerder besproken attacks zichzelf toegang verlenen tot het LSP en de informatie wijzigen, vernietigen, het systeem ontregelen of zonder dat andere dit weten er informatie ophalen of er juist een systeem tussen plaatsen waardoor afluisteren mogelijk wordt gemaakt. Wat het doel van een kwaadwillende ook mogen zijn, men moet proberen te voorkomen dat de server en de daarop draaiende processen ongestoord kunnen draaien.

Risicofactor

Server fysiek beschadigen

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA zijn de volgende cijfers beraamd:

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Een kwaadwillende probeert toegang te verkrijgen tot de serverruimte om vervolgens daar door fysiek toe doen het LSP te kunnen betreden.	3	3	3

Tabel 8.10: Effecten attack “server fysiek beschadigen” op de CIA

Alle drie de CIA-aspecten zijn hierbij in het geding en worden zeer hoog geschat. Immers wanneer een kwaadwillende zich bij het systeem bevindt kan deze doelgericht proberen toegang te krijgen tot het systeem om vervolgens te doen wat er in die situatie mogelijk is. Uiteraard hangt de aard van de attack af van het risico, en de omvang, maar een onbevoegde kwaadwillende in de serverruimte betekent veelal niet

dat deze een betrouwbare update komt uitvoeren. Voor de CIA zou het in het meest extreme geval kunnen betekenen dat wanneer een kwaadwillende zichzelf toegang heeft verschaft tot het LSP de informatie door een kwaadwillende kan worden benaderd, kan worden gewijzigd of zelfs worden verwijderd.

Urgentie

Server fysiek beschadigen

De kans dat een onbevoegd persoon een serverruimte fysiek zal kunnen betreden is niet uit te sluiten. Wanneer een kwaadwillende zich eenmaal toegang heeft verschaft en kwade bedoelingen heeft, is echter de kans op schade en de omvang van de schade erg groot. Onderdelen in de infrastructuur kunnen daardoor niet meer volledig functioneren waardoor het vertrouwen in de beschikbare informatie wordt ondermijnd. Daarbij komt dat met als eis heeft gesteld dat het backupsysteem pas binnen 24 uur actief dient te zijn, wat er toe kan leiden dat in deze periode, door zorgverleners, onterechte beslissingen kunnen worden genomen als gevolg van een onvolledig functionerende infrastructuur. Dat uiteraard risico's voor de behandelen patiënt teweeg kan brengen. De prioriteit om aan deze attack aandacht te besteden wordt om deze reden dan ook geschat op "zeer noodzakelijk".

Aanbevelingen

Server fysiek beschadigen

Over het algemeen is men zich bewust dat zenuwcentra's van deze orde van grootte en belangrijkheid een maximale beveiliging dienen te genieten. Getroffen maatregelen dienen dan ook van een hoogstaand niveau zijn. Bescherming van deze ruimte zal daarom veel investeringen op diverse vlakken vergen.

Om te voorkomen dat de hierboven beschreven dreiging realiteit wordt zijn een aantal doeltreffende maatregelen benodigd waardoor de ruimte minder eenvoudig voor indringers zijn te betreden. Een van de mogelijkheden is om de serverruimte in het pand te isoleren, dat biedt extra fysieke beveiliging tegen ramkraken maar ook praktisch gezien voordelen waardoor maatregelen maar een keer hoeven te worden geregeld en de aanpak kan worden gefocused.

Een van die maatregelen is dat deze ruimte alleen toegankelijk is voor personen met bijbehorende bevoegdheden om beheertaken uit te kunnen voeren. Toegang krijgen is alleen mogelijk door het invoeren van meerdere controlepunten. Dit gebeurd al bij de sollicitatieprocedure waarbij screening van kandidaat systeembeheerders plaats moet vinden. Daarnaast is toegangscontrole bij betreden van het pand alsmede van toegangscontrole bij de ruimte zelf noodzakelijk. Eenmaal in de ruimte zal met behulp van detectieapparatuur en systeemlogs de situatie gedurende de aanwezigheid blijvend worden gecontroleerd.

Door systeemkast extra te beveiligen waardoor directe toegang niet mogelijk is zal het voor de kwaadwillende moeilijker worden om bijvoorbeeld de harddisks te verwijderen. Maar ook het wijzigen van de BIOS of het gebruik van opslagmedia als USB-sticks, tapes of cd's verdient de nodige aandacht. Tevens is het verstandig backuptapes e.d. niet in dezelfde, beveiligde ruimte, te bewaren.

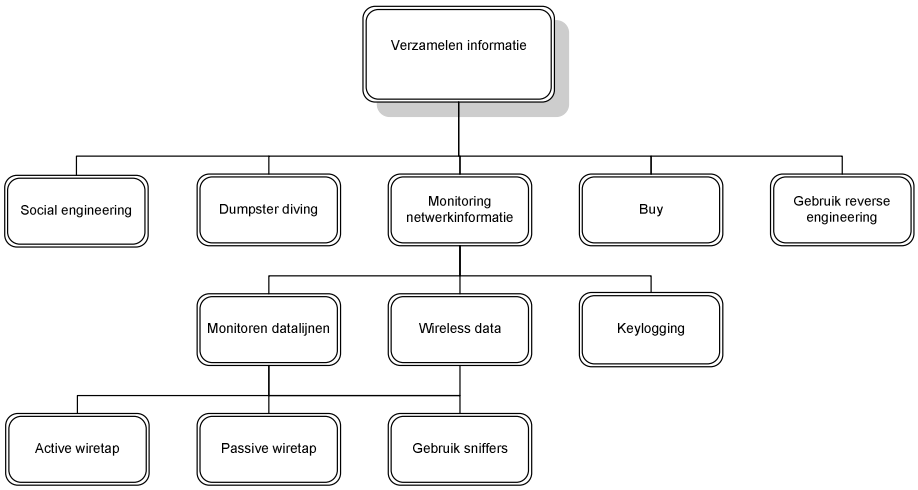
8.8 Fysiek niveau: verzamelen informatie

8.8.1 Inleiding

Veel interessante informatie is op een vrij eenvoudige wijze via de gebruikers, systeemontwerpers, beheerders of andere partijen die in relatie staan met het LSP, te verkrijgen. Wanneer men onzorgvuldig omgaat met de informatie aangaande het LSP biedt dat een kwaadwillende een kans om het LSP succesvol te kunnen aan vallen.

Deze sectie gaat dan ook in op mogelijke attacks die zich openbaren wanneer een kwaadwillende met behulp van deze informatie het LSP kan betreden.

8.8.2 Verzamelen informatie



Figuur 8.14: Attack tree “verzamelen informatie”

Dreigingen en gevolgen

Social engineering

Hierbij maakt de aanvaller bewust misbruik van de goedheid, bereidheid of onwetendheid van de mens. Veelal omdat zij niet in de gaten hebben dat ze worden misleid of niet op de hoogte zijn van de wijze waarop een kwaadwillende misbruik van hen probeert te maken. Social engineering maakt gebruik van sociale kundigheid en persoonlijke interactie om beveiligingsrelevante informatie te verkrijgen of om er voor te zorgen dat een succesvolle attack mogelijk wordt [PLF03]. Het voordeel voor een kwaadwillende is dat de attack zowel goedkoop als doeltreffend is.

Zolang de gebruiker niet sceptisch tegenover de gestelde vraag en het gewenste doel staat zal deze proberen de kwaadwillende te helpen. De gebruiker zal zich, meestal achteraf, pas realiseren waaraan hij zojuist medewerking aan heeft verleend. Tegenmaatregelen komen dan ook te laat, omdat veelal de kwaadwillende al heeft toegeslagen.

Dumpster diving

Veel belangrijke informatie, zoals systeeminstellingen, wachtwoorden, handelingen is vastgelegd in procedures- en instructiehandboeken of andere rapportages. Vaak verdwijnen deze gegevens als gevolg van onzorgvuldig handelen in de prullenbak. Voor een kwaadwillende dus een meer dan interessante informatiebron dat ondanks dat deze de nodige geluk moet hebben dat er nuttige informatie wordt gevonden wel zeer effectief kan zijn.

Monitoring netwerkinformatie

Een andere methode is om data dat op het netwerk wordt verzonden te verzamelen. Door het afluisteren van het netwerk kan de kwaadwillende belangrijke stukken informatie onderscheppen en op basis van de verkregen informatie de bijpassende attack activeren. Het afluisteren vindt onder andere plaats door de inzet van “sniffers”. Desondanks blijft het een vooral tijdrovende klus om de correcte data uit de berg met nutteloze data te filteren. Desalniettemin wordt met name door het gebruik van slimme applicaties het dit proces steeds efficiënter en kan deze zonder dat de kwaadwillende zich bekend hoeft te maken worden uitgevoerd.

Buy

Betaal voor de informatie die je wilt hebben. Zeer effectief mits de bron betrouwbaar is. Daarentegen loopt een kwaadwillende uiteraard wel een verhoogd risico als het gaat om betrouwbaarheid van zijn bron, de geleverde informatie en zijn positie.

Gebruik maken van reverse engineering

De laatste methode binnen deze attack heeft als kern het achterhalen van de precieze werking van de applicatie. Hierdoor krijgt een kwaadwillende een beeld van hoe het systeem in elkaar zit, taken worden uitgevoerd, welke bronnen worden aangesproken alsmede hoe de gegevens worden verwerkt. Feitelijk wordt een blauwdruk door een kwaadwillende gemaakt van de applicatie of systeem. Daarbij is het dan mogelijk om de gemaakte beslissingen van de ontwerper te begrijpen. Met behulp van deze informatie kan de kwaadwillende een succesvolle attack initiëren. Wanneer hij daar toe in staat is kan deze zelfs de applicatiesoftware voorzien van fault injection (in kwade zin de broncode bewust voorzien van slechte code waardoor een kwaadwillende mogelijkheden heeft om te doen wat hij wil doen).

Belang van bescherming

Social engineering

Deze vorm van aanvallen blinkt uit in haar eenvoud. Men is veelal bereid om andere mensen te helpen, vooral ook omdat de zorgsector een nog hogere graad van behulpzaamheid kent dan andere in sectoren. Deze bereidheid bepaald daardoor uiteindelijk ook het succes van deze attack, waarbij een kwaadwillende handig inspeelt op de onwetendheid bij gebruikers omdat ze hier zich nooit van bewust zijn gemaakt. Het is daarom aan te raden dat men ook na invoering van een UZI-pas, waarbij de identificatie van een zorgverlener wordt regelt, niet een waterdicht systeem maakt. De zwakste schakel in de beveiliging blijft ondanks alle beveiligingsmechanismen de mens [JAN05], waarbij een succesvolle attack wel eens grote gevolgen kan hebben.

Dumpster diving

Bedrijfsgevoelige informatie dat niet effectief wordt vernietigd past binnen het beeld dat bestaat over hoe men met informatie omgaat, onzorgvuldig namelijk. Hoewel er steeds meer informatie zorgvuldig wordt vernietigd, geldt dat niet voor alle niet meer te gebruiken informatie. Het niet vernietigen van belangrijke informatie maakt de overige beveiligingsmaatregelen overbodig en dus ineffectief.

Monitoring netwerkinformatie

Voor het monitoren van data zijn steeds meer methodes beschikbaar en dus dient het netwerk daardoor ook van een steeds betere beveiliging te worden voorzien. In een iedere computerzaak zijn tegenwoordig keyloggers te kopen die je tussen pc en keyboard plaatst. Datzelfde kan ook op het netwerk, zoals in de serverruimte. Deze ontwikkelingen zorgen er voor dat informatie dat over het netwerk wordt verzonden niet per direct veilig zijn voor kwaadwillende. Wanneer zij een techniek hebben gevonden waarmee zijn de communicatie kunnen afluisteren is niet direct de informatie niet meer betrouwbaar, maar loopt deze wel het risico dat het door uitvoeren van een vervolgaanval niet meer correct en dus betrouwbaar is.

Buy

Het belang van bescherming bij een aanval als deze is niet eenvoudig. Immers, alles en iedereen heeft zijn prijs. Van belang is om proberen te voorkomen dat gebruikers toegang hebben tot veel informatie en daarmee een interessant object zijn voor een kwaadwillende.

Gebruik maken van reverse engineering

Reverse engineering vergt kennis van de te onderzoeken hard- of software alsmede toegang tot deze bronnen. Hoewel het veel tijd kost om met behulp van reverse engineering succesvol een attack op het LSP te realiseren mag dit niet is uit te sluiten. Het is tevens ook lastig om dergelijke attacks tegen te gaan, omdat wanneer de broncode in handen is van een kwaadwillende de reverse engineering methode feitelijk onomkeerbaar is en alleen nog afhankelijk is van kennis die een kwaadwillende heeft of inkoopt om de broncode te kunnen reconstrueren.

Risicofactor

Social engineering

De risicofactor voor deze attack wordt geschat op: 3 (kansfactor) x 3 (omvangfactor) = 9 (risicofactor).

Dumpster diving

De risicofactor voor deze attack wordt geschat op: 3 (kansfactor) x 3 (omvangfactor) = 9 (risicofactor).

Monitoring netwerkinformatie

De risicofactor voor deze attack wordt geschat op: 2 (kansfactor) x 3 (omvangfactor) = 6 (risicofactor).

Buy

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

Gebruik maken van reverse engineering

De risicofactor voor deze attack wordt geschat op: 1 (kansfactor) x 3 (omvangfactor) = 3 (risicofactor).

CIA-classificatie

Voor de mogelijke effecten op de CIA zijn de volgende cijfers beraamd.

Aspecten / Dreigingen	Confidentiality	Integrity	Availability
• Door gebruik te maken van de bereidheid van mensen alsmede de onwetendheid kan een kwaadwillende proberen informatie te verkrijgen die niet vrijgegeven zouden mogen worden aan derden.	3	3	3
• Met dumpster diving probeert een kwaadwillende voor hem interessante informatie te achterhalen die door gebruikers worden weggegooid zonder deze te vernietigen.	2	2	1
• Informatie dat over het netwerk wordt verzonden kan van grote waarde zijn vooral wanneer dit mogelijk is zonder dat men hiervan op de hoogte is.	3	1	1
• Informatie verkrijgen via gebruikers van het LSP door het bieden van geld als tegenprestatie.	3	3	3
• Het ontrafelen van de werking van de applicatie en te leren van de beslissingen die de ontwerper heeft gemaakt met als uiteindelijke doel een gerichte attack op het LSP mogelijk te maken.	2	2	2

Tabel 8.11: Effecten attack “verzamelen informatie” op de CIA

Social engineering

Uit de effecten op de CIA-aspecten is op maken dat alle aspecten door deze attack ernstig worden aangetast. De vertrouwelijkheid van informatie is niet te waarborgen doordat niet is na te gaan of een kwaadwillende toegang tot de patiëntinformatie heeft gehad. De betrouwbaarheid is niet te garanderen vanwege de onwetendheid over de correctheid en volledigheid van deze informatie. Daarnaast kan er geen uitspraken gedaan worden over de beschikbaarheid. Immers, wanneer een kwaadwillende zich toegang heeft verschaft tot het LSP is alle informatie onbetrouwbaar tenzij vaststaat dat dit niet het geval is. Het

grote risico van deze attack is dat een kwaadwillende zijn doel op een zodanige wijze probeert te bereiken en dat de gebruiker meestal niet op de hoogte is van het feit dat hij slachtoffer is geworden.

Dumpster diving

De attack dumpster diving is een gevaarlijke attack omdat dit net zoals bij social engineering eenvoudig is uit te voeren en goedkoop is. Vanwege het feit dat veel informatie, ondanks de gestelde voorwaarde om privacygevoelige informatie gecontroleerd te vernietigen alvorens te dumpen in de papiercontainer, wordt er toch veel informatie zomaar weggegooid. Dit verhoogd de kans op succes voor een kwaadwillende, ondanks dat hij veel moeite en tijd moet investeren of er voor hem interessante informatie is te vinden. De effecten op de CIA-aspecten zijn niet heel hoog, omdat het desondanks moeilijk zal zijn informatie te verkrijgen waarmee hij ook daadwerkelijk iets kan uitvoeren.

Monitoring netwerkinformatie

In het verlengde van de attack dumpster diving ligt het vinden van informatie op het netwerk. Feitelijk is dit dezelfde attack alleen de bron en de gehanteerde methode verschilt. In dit geval is niet de prullenbak het doel maar het netwerk. De CIA-aspecten is niet hoog. Wanneer attack toch slaagt zal om de informatie te verkrijgen een vervolgstap moeten plaats vinden om daadwerkelijk toegang te krijgen tot het LSP.

Buy

De effecten op de CIA-aspecten zijn maximaal. Een kwaadwillende heeft alle mogelijkheden als het gaat om het kopen van informatie die nodig is om daarmee toegang tot het LSP mogelijk te kunnen maken. Dat de attack risicovol is in dit geval van ondergeschikt belang.

Gebruik maken van reverse engineering

De kans als de schade die op en door de reverse engineering attack is afhankelijk van het succes van de ontdekkingen die gedaan zijn tijdens het onderzoek. Indien daar nuttige informatie is vergaard, men de applicatie heeft kunnen reconstrueren en daaruit de nodige bevindingen heeft weten te halen waarmee een attack succesvol kan worden uitgevoerd, heeft dat zeker zijn invloed op de CIA-aspecten. Desondanks is dit risico niet extreem hoog omdat het zeker niet eenvoudig zal zijn vanwege het feit dat het LSP en de software die het gebruikt alleen voor een zeer beperkte groep beschikbaar is. Het risico wordt daardoor beperkt.

Urgentie

Social engineering

De risicofactor voor deze attack is hoog. Bescherming hier tegen is dan ook “zeer noodzakelijk”. Kortom, investeren in het opleiden van de gebruikers en om te signaleren wanneer een kwaadwillende een poging waagt om informatie los te krijgen terwijl hij deze niet mag hebben heeft een zeer hoge prioriteit.

Dumpster diving

Ook voor deze attack geldt een zeer hoge risicofactor. Samen met de lage score in de CIA bepaling zorgt dit er voor dat de urgentie toch als “noodzakelijk” moeten worden aangemerkt. Het is verstandig om aandacht

te besteden om het vernietigen van belangrijke informatie in de organisatie in te bedden waardoor zowel de privacy van de patiënt als de informatie op het LSP betrouwbaar is en blijft.

Monitoren van netwerkinformatie
De risicofactor als de CIA laten een over het algemeen een lage score zien. Afluisteren van data blijft met encryptie nog steeds mogelijk, maar naar mate er een verhoogde encryptie wordt gebruikt zal de interesse hiervoor afnemen voornamelijk vanwege de moeite om de gewenste informatie te verkrijgen. De vertrouwelijkheid is de enige aspect waarbij de attack deels een effect op zou kunnen hebben. De andere twee aspecten, betrouwbaarheid en beschikbaarheid hebben nog minder te leiden onder de effecten. De noodzaak om deze attack onmogelijk te maken is daarom “minder noodzakelijk”.

Buy
Het omkopen van een gebruiker om zodoende specifieke gegevens te verkrijgen waardoor toegang tot het systeem mogelijk wordt is een attack die moeilijk is tegen te gaan, iedereen heeft, zoals reeds eerder is opgemerkt, uiteindelijk zijn prijs.

Hoewel de risicofactor een zeer lage score laat zien wat wordt veroorzaakt door een lage kans maar zeer hoge omvang. De gevolgen kunnen dus dramatisch zijn wanneer de kans zich ook maar een keer voordoet. De effecten op de CIA zijn daarbij ook zeer hoog. Als we dit bij elkaar optellen komen tot de conclusie dat het vrijwel “noodzakelijk” is om deze attack onder de aandacht te brengen en actie te gaan ondernemen om de kans inderdaad zeer laag te houden.

Reverse engineering
De risicofactor wordt laag geschat omdat voordat er daadwerkelijk een attack kan plaats vinden veel research er aan vooraf gaat. Het beperkte domein is daarbij niet voor iedereen interessant. Vooral niet als we dit vergelijken met het belang van het verkrijgen van de werking van bijvoorbeeld Microsoft® producten. Toch mag niet uitgesloten worden dat er ook hier partijen zijn die graag meer inzicht willen in de patiëntgegevens of de werking van het systeem.

De kans op een dergelijke attack is daarom van een zodanig niveau dat deze niet direct bedreigend is, maar niet onderschat mag worden. Hoewel de risicofactor laag is, blijft de omvang alsmede de effecten op de CIA hoog. De urgentie voor deze attack wordt daarom geschat op “noodzakelijk”, maar het heeft niet de prioriteit. Dit vanwege de zeer lage kans en de grote investering die gedaan moet worden in tijd en energie die nodig is om deze attack succesvol ten uitvoer te brengen.

Aanbevelingen
Social engineering
Bescherming tegen social engineering is moeilijk omdat de zwakste schakel in het beveiligingssysteem, de gebruiker, door een kwaadwillende wordt ingezet om met behulp van misleidende trucjes, toegang tot het LSP te verschaffen. Hoewel er veel geld wordt geïnvesteerd in technische maatregelen om de beveiliging

van een systeem zo optimaal mogelijk te maken, dient men bij beveiliging de menselijke maat niet te onderschatten. Deze is immers de zwakste schakel in een beveiliging.

Mogelijke bescherming tegen deze attack is door gebruikers te trainen in het signaleren van mogelijke attacks in deze vorm, te trainen in wat ze in dergelijke situaties moeten handelen alsmede een gebruikersovereenkomst op te stellen waarin regels zijn vastgelegd waaraan een gebruiker zich dient te houden.

Maar dient men ook alert te zijn op verdachte personen die mogelijkerwijs misbruik willen maken van de situatie en zich voordoen als een ander persoon. Het effectief controleren wie zich in een gebouw bevindt is vooral lastig in grote organisaties als een ziekenhuis. Kleinere praktijken, als bijvoorbeeld bij een huisarts, is dit beter in de gaten te houden. Toegang tot het gebouw moet veelal voor iedereen mogelijk blijven. Echter, zal misschien zelfs kunnen overwegen de vrije toegang tot bepaalde afdelingen of kantoren te beperken.

Dumpster diving
Papierafval dat de afdeling verlaat en belangrijke informatie bevat dient consequent te worden vernietigd. Het is aan te bevelen erop toe te zien dat documenten ook daadwerkelijk door de verantwoordelijke gebruikers wordt vernietigd. Op deze wijze wordt het voor een kwaadwillende moeilijker om aan informatie te komen, waarmee hij vervolgens een attackpoging kan uitvoeren.

Monitoring netwerkinformatie
Hoewel het volgens artikel 139c [CLE05] het verboden is om gegevens zonder toestemming af te tappen, af te luisteren of op te nemen, wordt deze methode nog altijd gebruikt. Verbazingwekkend is dan ook dat men het in de specificaties wel heeft over beveiligde systemen, maar dat er niet gesproken wordt over het encrypten van de datacommunicatie? Dit kan echter wel een goede extra beveiliging vormen voor de informatie die men met elkaar uitwisselt. Het wordt dan immers ook minder interessant om deze gegevens te verzamelen, waardoor uiteindelijk ook deze attackmethode minder interessant wordt voor potentiële kwaadwillende.

Om een veilige communicatie in zijn geheel te krijgen is alleen encryptie helaas niet voldoende. Hiervoor zal men een aantal technieken moeten gebruiken om dit mogelijk te maken, zoals; encryptie, digitale handtekeningen, authenticatie en een VPN.

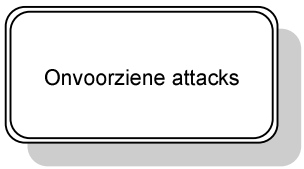
Buy
Om omkoping tegen te gaan is het aan te raden gebruikers, beheerders en ontwikkelaars een overeenkomst te laten ondertekenen waarin staat dat zij informatie met betrekking tot het systeem alleen mogen gebruiken voor het uitoefenen van hun werkzaamheden. Indien, achteraf, wordt geconstateerd dat dit wel is gebeurd kan men overgaan tot het opleggen van overeenstemmende sancties. In het ergste geval kan men de persoon kunnen ontslaan en aangifte tegen hem doen voor het doorspelen van informatie aan

derden. Uiteraard zal men hiervan ook lering kunnen nemen om er in de toekomst voor te zorgen dat dergelijke omkooppraktijken niet meer mogelijk zijn.

Gebruik maken van reverse engineering
Men zal moeten voorkomen dat een kwaadwillende deze methode niet kan gebruiken door te zorgen dat de applicatie niet in handen van deze kan komen of doordat hij zich in het ontwikkelteam begeeft deze vertaalslag makkelijk kan uitvoeren. Het is dus noodzakelijk dat men er alles aan doet om te zorgen dat de applicatie niet in de verkeerde handen terecht komt, anders zijn gevolgen niet te overzien. In dat opzicht is het daarom belangrijk dat de broncode binnen de muren van de ontwikkel- en beheerafdelingen blijven en niet naar buiten kunnen lekken. Dit zal echter lastig worden omdat men een extern (commercieel) bureau heeft ingeschakeld om het LSP te laten bouwen. Op meerdere gebieden bemoeilijkt dit de betrouwbaarheid van de werking van het systeem als de daarop geslagen gegevens.

8.9 Fysiek niveau: onvoorziene attacks

Ontwikkelingen gaan door en volgen voornamelijk door het internet elkaar steeds sneller op. Door deze constante vernieuwing en verbeteringen zien ook steeds nieuwe attacks om, in dit geval, een systeem binnen te kunnen komen het levenslicht. En telkens reageert de informatiebeveiliging daar weer op met ook weer nieuwe toepassingen en oplossingen.



Figuur 8.14: Attack tree “onvoorziene attacks”

Deze constante golf van nieuwe mogelijkheden vergt vooral een vooruitziende blik van de informatiebeveiliging. Zij moeten immers, op tijd en liever nog iets eerder, reageren op deze ontwikkelingen. Desondanks blijft het mogelijk dat er kwaadwillende toepassingen of methodes worden gebruikt die niet in de laatst uitgevoerde risicoanalyse zijn opgenomen. Dat kan vanwege de vernieuwing, maar ook omdat men deze niet heeft onderkend vanwege het onbekende.

Prioriteit is dus om snel in te zien welke nieuwe ontwikkelingen mogelijk een probleem kunnen gaan vormen voor het systeem en daar zo snel mogelijk een risicoanalyse over los te laten. De kans dat een kwaadwillende het systeem kan ondermijnen en met succes zijn doel weet te bereiken wordt hierdoor aanzienlijk verminderd. De risicoanalyse is een proces dat constant erop toeziet dat alle risicovolle attacks met hun kans- en omvangsfactor voor het systeem bekend zijn.

8.10 Overzicht

Het onderstaande overzicht geeft een totaalbeeld van scores per dreiging en de vermeende classificatie tot noodzakelijkheid.

Meting / Dreigingen	C	I	A	Kans-factor	Omvangs-factor	Totaal score
Inloggegevens verkregen door deze te zoeken in en rondom kantoor of huis, verkregen door persoonlijke items te doorzoeken of door deze van de pc of netwerk te halen.	1 (3)	1 (3)	1 (1)	3	3	Zeer noodzakelijk
Gebruikers afpersen, omkopen, misleiden, bedreigen, chanteren of vragen de inloggegevens af te geven.	1 (3)	1 (3)	1 (1)	2	3	Noodzakelijk
Gebruikers observeren of afluisteren om zodoende de inloggegevens te verkrijgen.	1 (3)	1 (3)	1 (1)	3	3	Noodzakelijk
Inloggegevens verkregen doordat een kwaadwillende software gebruikt of installeert waarmee vervolgens de inloggegevens worden verkregen.	1 (3)	1 (3)	1 (1)	3	3	Zeer noodzakelijk
Inloggegevens verkregen door softwarematig afluisteren van verbindingen.	1 (3)	1 (3)	1 (1)	1	3	Noodzakelijk
Inloggegevens verkregen door opzetten van een nep-site waardoor gebruiker denkt dat deze originele site bezoekt, maar feitelijk gebruik maakt van een malafide website.	1 (3)	1 (3)	1 (1)	1	3	Minder noodzakelijk
Beheerder of (ex-) medewerker/gebruiker afpersen, omkopen, bedreigen, misleiden, chanteren of vragen inloggegevens van een gebruiker waarover de betreffende gebruiker beschikt.	1 (3)	1 (3)	1 (1)	2	3	Noodzakelijk
Beheerders of andere (ex-) medewerkers/ gebruikers observeren of afluisteren om zo inloggegevens te verkrijgen van een andere gebruiker waarover deze gebruiker beschikt.	1 (3)	1 (3)	1 (1)	3	3	Zeer noodzakelijk
Chipinformatie van de UZI-pas wordt gelezen en gekopieerd op een blanco kaart of ander medium opgeslagen om toegang te verkrijgen tot het LSP.	1(3)	1(3)	1(1)	1	3	Noodzakelijk
Communicatie tussen UZI-pas en paslezer wordt afgeluisterd en gebruikt om hiermee vervolgens toegang te verkrijgen tot het LSP.	1(3)	1(3)	1(1)	1	3	Noodzakelijk
De UZI-pas wordt gestolen of geleend van de rechtmatige gebruiker om vervolgens toegang tot het LSP te verkrijgen.	1(3)	1(3)	1(1)	3	3	Zeer noodzakelijk
Via het UZI-register, al dan niet via een (malafide) medewerker, wordt getracht een UZI-pas te verkrijgen om hier vervolgens toegang mee te verkrijgen tot het LSP.	1(3)	1(3)	1(1)	1	3	Noodzakelijk

Meting / Dreigingen	C	I	A	Kans-factor	Omvangs-factor	Totaal score
Doormiddel van het uitvoeren van een portscan probeert een kwaadwillende er achter te komen welke poorten open staan om vervolgens te trachten toegang tot het systeem te krijgen om instellingen te wijzigen.	1	1	1	3	1	Minder noodzakelijk
Door het achterhalen van wachtwoord of inloggegevens van een applicatie krijgt men toegang tot de applicatie waardoor instellingen gewijzigd kunnen worden, extra rechten kunnen worden toegekend aan een gebruiker of logs kunnen worden verwijderd.	3	3	3	1	3	Noodzakelijk
Kwaadwillenden maken gebruik van fouten in de software, de dreiging die hiermee ontstaat, kan grote gevolgen hebben voor een systeem omdat de bugs soms niet bekend zijn waardoor het systeem risico's loopt.	3	3	3	3	3	Zeer noodzakelijk
Door het uitvoeren van een buffer overflow probeert een kwaadwillende het systeem binnen te treden anders dan via de inlogprocedure, hij tracht daarbij mogelijkerwijs taken uit te voeren die normaliter niet zijn uit te voeren.	3	3	3	1	3	Noodzakelijk
Door het installeren van een virus op een pc probeert een kwaadwilende toegang te krijgen tot de besmette pc en via deze pc verder in het netwerk binnen te dringen, de pc af te luisteren of gegevens te bemachtigen.	3	3	3	3	3	Zeer noodzakelijk
Door spoofing te gebruiken probeert een kwaadwillende de gebruiker te misleiden en zodoende zijn inloggegevens te verkrijgen, de communicatie af te luisteren en zich voor te doen als een andere partij en daardoor voor hem belangrijke informatie te verkrijgen.	3	3	1	1	3	Minder noodzakelijk
Toegang tot de applicatie krijgen door gebruik te maken van kennis, het wachtwoord of de diensten van personen met rechtmatige toegang tot de applicatie.	3	3	3	1	3	Noodzakelijk
Doormiddel van trusting trust probeert de aanvaller toegang tot de applicatie te krijgen.	3	3	3	1	3	Noodzakelijk
Gebruik maken van bugs en fouten van (conflicterende) hardware.	3	3	3	1	3	Zeer noodzakelijk
Detecteer zwakke plek bij hardware.	1	1	1	1	1	Minder noodzakelijk
Een kwaadwillende probeert toegang te verkrijgen tot de serverruimte om vervolgens daar door fysiek toe doen het LSP te kunnen betreden.	3	3	3	1	3	Zeer noodzakelijk

Meting / Dreigingen	C	I	A	Kans-factor	Omvangs-factor	Totaal score
Door gebruik te maken van de bereidheid van mensen alsmede de onwetendheid kan een kwaadwillende proberen informatie te verkrijgen die niet vrijgegeven zouden mogen worden aan derden.	3	3	3	3	3	Zeer noodzakelijk
Met dumpster diving probeert een kwaadwillende voor hem interessante informatie te achterhalen die door gebruikers worden weggegooid zonder deze te vernietigen.	2	2	1	3	3	Noodzakelijk
Informatie dat over het netwerk wordt verzonden kan van grote waarde zijn vooral wanneer dit mogelijk is zonder dat men hiervan op de hoogte is.	3	1	1	2	3	Minder noodzakelijk
Informatie verkrijgen via gebruikers van het LSP door het bieden van geld als tegenprestatie.	3	3	3	1	3	Noodzakelijk
Het ontrafelen van de werking van de applicatie en te leren van de beslissingen die de ontwerper heeft gemaakt met als uiteindelijke doel een gerichte attack op het LSP mogelijk te maken.	2	2	2	1	3	Noodzakelijk

Tabel 8.15: Totaaloverzicht CIA-classificaties en risicofactoren van de

8.11 Conclusie

8.11.1 Gebruik van attack trees

De attack trees zijn eenvoudig in gebruik, overzichtelijk en geven inzicht in de wijze waarop kwaadwillende het uiteindelijke doel (op onrechtmatige wijze) zouden kunnen bereiken. Het geeft, wanneer ook de nodige attributen er in worden verwerkt een helder overzicht dat in een aantal oogopslagen volledig is door iedereen kan worden begrepen. Echter, het identificeren en construeren van de attack tree is niet zo eenvoudig en een vervelende en tijdrovende klus. Natuurlijk hadden attacks ook op een andere manier in kaart gebracht kunnen worden, maar dat komt de uiteindelijke leesbaarheid niet ten goede.

De attack trees bevatten dan wel vele mogelijke kwaadwillende manieren die allen het uiteindelijke doel hebben om op onrechtmatige wijze toch toegang te kunnen krijgen tot het systeem. Toch kan men nooit een volledige attack tree opleveren waarin alle mogelijkheden in zijn opgenomen. Dat is niet reëel en haalbaar vanwege het feit dat ook de ontwikkelingen niet stil staan en er daarom steeds weer nieuwe manieren opduiken die mogelijk een risico zouden vormen voor het systeem. Het is daarom aan te raden om de risicoanalyse op een aantal vooraf bepaalde momenten af te sluiten en na verloop van tijd opnieuw uit te voeren om de nieuwe ontwikkelingen erin op te nemen en niet (meer) relevante attack mogelijkheden te verwijderen.

Hoewel de methode eenvoudig is en er relatief snel resultaten kunnen worden geboekt, komen een aantal onderdelen in aanmerking voor verbetering. Zo is het identificeren van mogelijke attacks afhankelijk van de kennis die een onderzoeksteam heeft om een de attack mogelijkheden te onderkennen. De mate van kennis bepaalt de uiteindelijke breedte van de attack tree. Een onderzoeker moet immers eerst een attack onderkennen en vervolgens bepalen of deze belangrijk genoeg is om in de attack tree op te nemen. Het is daarnaast ook belangrijk om de mate van detaillering in de gaten te houden. Te gedetailleerde attack trees bevatten wel veel nuttige informatie maar zorgen tevens voor een onhandel- en onleesbare attack tree.

Na het identificeren van mogelijke attacks zijn deze in de attack tree geplaatst. Dit tekenproces is langdurig en gaat gepaard met veel schuiven en aanpassen van de attacks. Dit probleem wordt complexer naarmate de onderkende attacks een aantal niveaus kent. De structuur wordt dan zo onoverzichtelijk en complex dat dit een chaos aan vertakkingen oplevert, waardoor het voorkomt dat subattacks in elkaar overlopen en wat uiteindelijk zorgt voor een onoverzichtelijk geheel.

Het ontbreken van een hulpmiddel waarmee op eenvoudige wijze een attack tree kan worden geconstrueerd zorgt voor extra grote problematiek bij het digitaal vervaardigen van een attack tree én bij eventuele wijzigingen nadien. Door het ontbreken van een dergelijke tool gaat veel tijd verloren voor het construeren van attack trees met programma's die daar niet voor bedoeld zijn. Het dus aan te raden dat er voor het construeren van attack trees een case tool beschikbaar komt waarmee dat mogelijk wordt. Het proces rond het creëren van een attack tree, zoals de lay-out, de verwerkingstijd, de hanteerbaarheid en het vermogen om attack trees in de toekomst eenvoudig aan te passen wordt hierdoor verbeterd en versnelt.

8.11.2 Gebruik van risicoanalyse methode

Wanneer de mogelijke attacks zijn onderkend en zijn opgenomen in een attack tree kunnen de risicofactoren, de dreigingen die door de attacks ontstaan en de mogelijke gevolgen worden belicht. In eerste instantie wordt per attack de kans en de omvang bepaald wanneer deze ook daadwerkelijk realiteit wordt. Probleem hierbij is dat beide factoren geschat moeten en dat men, om dit te kunnen, over ruim voldoende domeinkennis dient te beschikken alvorens dit te kunnen. De uitkomst, de risicofactor is dus het resultaat van schattingen, waarbij de kansfactor een ondergeschikt belang speelt tegenover de omvangsfactor. De omvangsfactor is namelijk zeer moeilijk in te schatten voor deze attacks, omdat wanneer een kwaadwillende eenmaal zichzelf toegang heeft verschaft tot het systeem, hij feitelijk toegang heeft tot de informatie waarvoor hij een attack heeft uitgevoerd. En dus de omvang van de attack al desastreus is voor de betrouwbaarheid van het systeem.

Het principe van schatten kent een valkuil, namelijk verkeerd inschatten. Voor dreigingen waarmee men minder bekend is, is er dus een grotere kans op een verkeerde schattingen. Dit kan tot gevolg hebben dat een attack, in de risicoanalyse, verkeerd wordt ingeschaald waardoor men een verkeerd beeld krijgt van de dreiging en de noodzaak om hier iets tegen te doen. Prioriteiten kunnen hierdoor op de verkeerde attacks komen te liggen waardoor werkelijke dreigingen onderbelicht raken. Dit principe geldt uiteraard voor elke

analyse. Het is daarom aan te raden deskundigen bij dit proces te betrekken die op basis van hun kennis een onderbouwde inschatting kunnen maken van de risico's en de kans op hun ontstaan.

Ook voor het bepalen van de scores voor de onderdelen van de CIA-triad vindt plaats door schattingen gebaseerd op kennis en feiten. Dat schatten is niet eenvoudig omdat scores aan de CIA wel overwogen moet worden toegekend. Een verkeerde schatting heeft gevolgen voor de uiteindelijke uitkomst van de risicoanalyse en kan leiden tot het wegnemen van risico's die feitelijk minder belangrijk zijn.

Het uiteindelijke doel van een risicoanalyse is om risico's en hun kans op ontstaan alsmede hun schadeomvang inzichtelijk te maken. Op basis van uitkomsten kunnen doelgericht maatregelen genomen om risico's met een hoge prioriteit te verminderen of zelfs weg te nemen, terwijl risico's met een lagere prioriteit op een later moment alsnog kunnen worden opgelost. Echter is het van belang te beseffen dat een risicoanalyse een momentopname betreft en na verloop van tijd wederom dient te worden uitgevoerd. Op deze wijze kan bekeken worden of maatregelen hebben geholpen en nieuwe risico's worden ontdekt. Door het periodiek uitvoeren van een dergelijke analyse houdt men greep op de risico's en kan voor een groot deel tijdig maatregelen genomen worden.

8.11.3 Resultaten risicoanalyse methode

De uitgevoerde RAM geeft inzicht in attacks die een kwaadwillende op het LSP zou kunnen uitvoeren om op onrechtmatige wijze toegang te krijgen. Daarnaast worden de hoogte van de kans en omvang van een eventuele succesvolle attack gegeven. Met de aangedragen aanbevelingen is het mogelijk de attack te bestrijden of deze in kans en/of omvang te doen afnemen.

De resultaten van de uitgevoerde risicoanalyse in dit hoofdstuk zijn gedetailleerd, maar beschrijven bewust niet alle vertakkingen in de attack trees van begin tot het einde. De omvang van dit document zou daardoor leiden tot een onoverzichtelijk geheel. De gegeven aanbevelingen zorgen desondanks ervoor dat de essentie van de attack wordt bestreden. Dit heeft zijn uitvoer op de daaronder gelegen attacks.

Om tot resultaten te kunnen komen moeten de attacks kwantificeerbaar worden gemaakt. Dit is nodig om te kunnen zien welke attacks en risico's een hoge prioriteit hebben en welke niet. Op basis van deze kennis kunnen verantwoordelijken beslissingen nemen en uiteindelijk bepalen welke attacks voor maatregelen in aanmerking komen, op welke wijze dit wordt gedaan en hoeveel geld hiervoor wordt uitgetrokken.

De resultaten laten zien dat het LSP, in tegenstelling tot wat het NICTIZ in haar specificaties beweert [NIC05a], wel degelijk bloot wordt gesteld aan krachten van buitenaf waardoor het systeem en de infrastructuur minder veilig zijn dan men tot op heden aanneemt. Wanneer er niets wordt gedaan aan het verbeteren van de infrastructuur en de beveiliging van het LSP zal men ook de consequenties moeten dragen die zich ongetwijfeld zullen aandienen.

De ontdekte attacks en hun risico's zorgen ervoor dat men maatregelen zal moeten nemen om de veiligheid en de betrouwbaarheid van het systeem te verhogen. Echter de voorgestelde oplossingen zijn alleen effectief wanneer de informatiebeveiliging ook daadwerkelijk in de gehele infrastructuur wordt verankerd en nageleefd. Zonder bewustwording van veiligheid, beveiliging en het correct omgaan met het informatiesysteem bij de gebruikers heeft het nemen van de nodige maatregelen geen toegevoegde waarde en is het verspilde moeite, tijd en dus geld.

"Developing a comprehensive medical information system was
a more complex task than putting a man on the moon had been."
Morris Collen

9. Conclusie en opmerkingen

In dit afsluitende hoofdstuk zullen de deelvragen en de uiteindelijke onderzoeksvraag worden beantwoord. Daarnaast worden opmerkingen gegeven die mogelijkerwijs in aanmerking komen om bijvoorbeeld de betrouwbaarheid, veiligheid en beheer van het LSP en de infrastructuur te verbeteren.

9.1 Antwoord deelvraag 1

Hoe zit het NICTIZ LSP in elkaar?

a. Hoe zit het LSP in elkaar?
b. Hoe verloopt de toegangprocedure?
c. Hoe verloopt de logprocedure?
d. Welke ontwerpkeuzes heeft men gemaakt?
e. Wat zijn de voor- en nadelen van een centraal of een decentrale LSP en/of een centrale of een decentrale gegevensopslag?
f. Welke implementatiekeuzes zou men kunnen overwegen?

Het antwoord op deze vraag wordt gegeven in de hoofdstukken 4, 6 en 7. Tezamen geven ze een algehele indruk van de beoogde inrichting en werking van het LSP en haar functies. Tevens worden ook twee essentiële functies, toegang en logging, nader beschreven. Het beschrijven van het LSP is noodzakelijk om inzicht te krijgen in het systeem dat het NICTIZ voor ogen heeft maar dient ook om vervolgvragen te kunnen beantwoorden. Aanbevelingen betreffende implementatiemogelijkheden die het NICTIZ zou kunnen overwegen op te nemen in het LSP en de infrastructuur komen in het onderstaande stuk nader aan bod.

9.1.1 Opmerkingen

Het NICTIZ heeft de voorkeur uitgesproken om de verkeerstoren, het LSP, een centrale positie in de basisinfrastructuur te geven. Het centraal positioneren van het LSP en de opgeslagen patiëntgegevens garanderen dat de zorgverlener vrijwel direct hierover kan beschikken. Dat is een goede uitgangspositie en komt de kwaliteit van de zorg ten goede. De zorgadministratie rondom de patiënt wordt minder doordat met name redundante informatie minder vaak voorkomt. De betrokken zorgverleners kunnen de laatste gegevens ook direct opvragen waardoor constateringen worden bewaard en extra onderzoek alleen nodig is wanneer de zorgverlener op basis van de gegevens en de input van de patiënt dat nodig acht. Daarnaast

biedt het samenstellen van een patiëntendossier via elektronische weg voordelen als het gaat om de breedte van het dossier, de actualiteit daarvan en conclusies die men kan trekken omdat alle bij de zorgverleners bekende medische gegevens over de patiënt via het LSP toegankelijk is. Hoewel het een goed idee is om patiëntinformatie via de digitale snelweg beschikbaar te maken, zijn er helaas ook problemen en nadelen ten opzichte van de door het NICTIZ voorgestelde infrastructuur. Nadelen die de voordelen teniet kunnen doen.

9.1.2 Verwijsindex

Patiëntinformatie up-to-date

Hoewel de patiëntgegevens direct voor elke zorgverlener beschikbaar moet worden via de verwijsindex, kan de verwijsindex nooit alle bij de zorgverlener bekend zijnde gegevens bevatten. Immers, wanneer zich een wijziging voordoet, zal de informatie niet direct in het dossier zijn opgenomen. De verwijsindex probeert echter wel de laatst bekende gegevens te leveren, maar levert in deze situatie dus niet de actuele status van een patiënt. Dit is te wijten aan de verwerkingstijd van patiëntgegevens en kan alleen worden opgelost wanneer alle informatie direct in het betreffende patiëntendossier wordt verwerkt.

Technisch gezien spelen er ook zaken die er voor kunnen zorgen dat niet de actuele gegevens van een patiënt wordt opgehaald. Hiermee nu nog geen rekening gehouden wordt. Zaken als;

- Werken alle koppelingen in de verwijsindex wel?
- Refereren deze verwijzingen ook naar de actuele gegevens van een patiënt bij iedere zorgverlener?
- En wat als patiëntinformatie niet opvraagbaar is, of juist wel, maar deze niet via verwijzingen beschikbaar is gesteld?

Het voordeel dat men heeft doordat zorgverleners sneller een actueel beeld kunnen vormen van de historie van een patiënt, heeft wel als nadeel dat de afhankelijkheid van de zorgverlener van het systeem groeit.

Single point of contact en failure

De afhankelijkheid van het systeem zal alleen maar groeien doordat iedere zorgverlener verplicht wordt door het Ministerie van Volksgezondheid, Welzijn en Sport (Ministerie van VWS) zijn systeem aan de infrastructuur aan te sluiten. Hoewel dit er voor zorgt dat alle patiëntinformatie in theorie gegarandeerd voor alle zorgverleners bereikbaar wordt, heeft dit wel een aantal consequenties voor de infrastructuur. De vele connecties zullen onder andere heel veel dataverkeer gaan opleveren waardoor men op voorhand zeker moet zijn dat het systeem én het netwerk dit aan kunnen. Door te kiezen voor een centrale LSP zal alle communicatie enkel via een knooppunt verlopen. De beschikbaarheid van de informatie kan, wanneer er problemen ontstaan, er voor zorgen dat informatie-uitwisseling onmogelijk wordt gemaakt. Er is dan sprake van een SPOF omdat elk systeem afhankelijk is van deze ene LSP.

Het principe van een SPOC kent genoeg voordelen zoals op het gebied van infrastructuur en ook beheer. Maar ook een aantal nadelen. Een van die keerzijde van een SPOC is dat wanneer op enig moment zich binnen het LSP een probleem voordoet, dit impact heeft op ondermeer de performance van het systeem en die gevolgen zijn in de gehele infrastructuur merkbaar. Hoewel zorgverleners lokaal nog over hun

patiëntinformatie kunnen beschikken is het op landelijk niveau opvragen van gegevens dan moeilijker. Het LSP wordt een bottleneck waar niet op is te vertrouwen. Zaken als de kwaliteit van de informatie, de betrouwbaarheid van het systeem en het draagvlak worden hierdoor geschaad, met als mogelijk gevolg dat men voorzichtiger wordt met het ontwikkelen van nieuwe systemen of ideeën. Wat uiteindelijk resulteert in een achteruitgang van de ontwikkelingen op het gebied van elektronisch werken.

Decentraal ipv centraal

Een mogelijk alternatief is om het LSP op te delen in meerdere LSP verkeerstorens en decentraal (regionaal) te plaatsen. Deze LSP's zouden dan een identieke verwijsindexen moeten bevatten om miscommunicatie tegen te gaan. Bedoeling van de decentralisatie is om het contact met een LSP te garanderen en op deze wijzen er voor te zorgen dat communicatie met een van de LSP's is gegarandeerd. De eerder genoemde SPOF is hierdoor niet meer aan de orde terwijl het SPOC-principe blijft gehandhaafd.

Door het decentrale karakter zal tevens de load per LSP gebalanceerd zijn in tegenstelling tot wanneer één LSP al het dataverkeer moet verwerken. Dit komt de performance op meerdere gebieden ten goede, zoals; de snelheid van verwerking, de betrouwbaarheid van het systeem en beschikbaarheid van gegevens. Nadeel van deze structuur is echter dat de beheerskosten aanmerkelijk zullen stijgen, versiebeheer een probleem wordt, de beveiliging op orde moet zijn en de verantwoordelijkheid bij meerdere beheerteams ligt. Met als gevolg, meer personeel, langere communicatielijnen, een grotere kans op miscommunicatie en storingen door de inzet van meerdere systemen.

Er zijn nog meer opvallende keuzes gemaakt. Zo heeft het back-upsysteem een minder prominente rol dan noodzakelijk. Waarom een systeem gebruiken waarvoor geldt dat bij eventuele calamiteiten dit systeem pas binnen 24 uur weer volledig operationeel moet zijn? In de zorg kan men geen rekening houden met systemen die falen waardoor informatie onbereikbaar wordt. Zorg stopt niet wanneer een systeem ermee op houdt. Een mogelijke oplossing is om een tweede (back-up) LSP synchroon in te zetten naast de LSP. Bij calamiteiten met het LSP zou de backup-LSP de taken direct moeten over nemen, waardoor zorgverleners zo min mogelijk last hebben van problemen. Deze zekerheid draagt bij aan de betrouwbaarheid van het gehele zorgapparaat. Wanneer men had gekozen voor decentrale LSP's is het geen probleem dat de back-up niet direct actief zou zijn. Immers de andere LSP's vangen de klap op. De keuze van een infrastructuur is helaas niet alleen afhankelijk van mogelijkheden. Immers, welke keuze men ook maakt de investeringen die men wil doen bepaald mede hoe het zorgsysteem eruit zal gaan zien.

LSP in extern beheer

Wat tevens als een nadeel kan worden gezien, is dat het LSP buiten het zorgdomein wordt gerealiseerd. Hoewel CSC reeds ervaring heeft opgedaan met het bouwen van soortgelijke systemen is niet uit te sluiten dat deze mogelijkerwijs kan profiteren van de kennis die het heeft over het LSP. Zo is niet te garanderen dat patiëntgegevens binnen het zorgdomein blijven, waardoor de privacy in het geding komt. Daarnaast heeft een kwaadwillende extra kansen om bij dit bedrijf op zoek te gaan naar de nodige informatie om zo het LSP te kunnen betreden, omdat deze beschikt over de blauwdrukken, broncode en alle ins- en outs. Daarbij komt ook nog eens dat toegangscontrole en controle op de informatie niet mogelijk is wanneer een

kwaadwillende zich binnen dit domein begeeft, waarbij de kans dat de functionele ontwerpen van het LSP systeem worden hergebruikt in andere systemen of zelfs worden doorverkocht.

Problemen als deze kunnen opgelost worden wanneer deze partner zich ook daadwerkelijk binnen het zorgdomein bevindt en dus onderdeel uitmaakt van het zorgsysteem in Nederland. Het NICTIZ, dat zich knooppunt en kenniscentrum voor ICT en innovatie in de zorg noemt, zal zich meer moeten ontwikkelen tot een volwaardige op zorg toegespitste ICT-specialist voor de landelijke zorg waarbij men alle kennis in huis heeft om projecten ook daadwerkelijk zelfstandig te kunnen uitvoeren.

Verwijsindex niet virtueel

Hoewel het LSP en de daarin opgeslagen verwijsindex doet vermoeden dat we virtueel in het dossier van een patiënt kunnen snuffelen, weten we inmiddels dat dit maar deels correct is. Virtueel staat, in dit geval, voor het nabootsen van papieren patiëntendossiers uit de werkelijkheid in de digitale wereld. Dit principe werkt echter redundantie in de hand.

Als een zorgverlener informatie van een patiënt wil opvragen, zal na het invoeren van de zoekinstructie via de verwijsindex informatie van de betreffende patiënt (van de leverende zorgverlener) naar de vragende zorgverlener worden verzonden en lokaal opgeslagen in een digitaal dossier. De zorgverlener kan nu de actuele gegevens bekijken. Door deze constructie ontstaat bij elke vragende partij dus dossiers van patiënten. Nadat deze gegevens zijn opgeslagen is verdere controlemogelijkheden over deze gegevens niet meer mogelijk. Ze zijn immers correct afgeleverd. Telkens wanneer diezelfde zorgverlener de meest actuele patiëntinformatie tot zijn beschikking wil hebben zal hij deze via het LSP moeten opvragen om er zeker van te zijn dat hij over de enige en juiste informatie kan beschikken en op basis daarvan juiste uitspraken kan doen. Wat doet men als dit niet gebeurd? Is dat de verantwoordelijkheid van de zorgverlener? Wat als dit ernstige nadelige gevolgen heeft voor de patiënt? Het systeem zou deze toch moeten voorkomen in plaats van weer nieuwe gevallen creëren?

Hoewel de verwijsindex afhankelijk is van de bereidheid en zorgvuldigheid van de zorgverlener om wijzigingen zo snel mogelijk door te voeren in het informatiesysteem en dit door te geven aan de verwijsindex, zorgt deze constructie voor de nodige risico's. Gezien de betrouwbaarheid is het verstandig meerdere LSP's decentraal in te zetten. Het SPOF wordt hierdoor teniet gedaan, maar het SPOC-principe blijft gehandhaafd. Met meerdere servers, kan men gespreid en met een acceptabele load een zelfde service aanbieden maar met hogere betrouwbaarheid. Mocht een van de LSP's het begeven, dan kunnen de overige LSP's dit opvangen waardoor de zorgverleners geen enkele hinder ondervinden en dus service gegarandeerd blijft. Natuurlijk zal hierdoor wel op alle LSP's de verwijsindex te alle tijden identiek en actueel moeten zijn. Een ander punt van aandacht is de stijgende kosten voor beheer, de grotere kans op systeemfouten of -conflicten en kans op een minder stabiele infrastructuur vanwege de inzet van meerdere LSP's. Een ander mogelijkheid is het inzetten van een virtueel systeem. Alle informatie van en naar zorgverleners wordt via het web afgehandeld en informatie wordt niet lokaal opgeslagen, maar is wel voorzien van dezelfde functionaliteiten als nu is voorgesteld. Dit biedt onder andere de mogelijkheid om de betrouwbaarheid te verbeteren van het systeem omdat deze niet meer afhankelijk is van de systemen die

lokaal zijn opgesteld. Daarbij brengt een virtueel dossier minder risico's met zich mee als het gaat om juistheid van informatie en privacy van patiënten omdat de meest actuele gegevens worden opgehaald, maar niet lokaal wordt opgeslagen bij de zorgverlener. Hierdoor behoren problemen met opslag van patiëntdossiers lokaal bij de zorgverlener tot het einde, kent men geen versieconflicten met dossiers omdat de meest actuele gegevens online staan en heeft men minder problemen bij de zorgverleners doordat zij van het internet gebruik maken en niet van hun software-applicaties die lokaal draaien. Uiteraard zorgt dit er wel voor dat men rekening dient te houden met de capaciteiten van het centrale verwerkingssysteem omdat zowel het LSP als de infrastructuur extra worden belast. En wat betreft het probleem dat alle patiëntinformatie op een grote server zijn geplaatst kan men oplossen door te kijken hoe andere sectoren, zoals de bancaire, dit hebben opgelost.

9.1.3 Standaarden

Het LSP is een verkeerstoren die in contact zal komen te staan met de zorgsystemen bij alle zorginstellingen. Gegevens aanwezig in lokale zorgsystemen vormen de bron voor de inhoud van de verwijsindex. Door gebruik te maken van het HL7v3 protocol kan er op een uniforme wijze onderling worden gecommuniceerd. Alvorens dit mogelijk is dient het aan te sluiten zorgsysteem wel te beschikken over een XIS-typegoedkeuring, waarmee aangetoond is dat het systeem geschikt is voor aansluiting op het LSP en dus voldoet aan de door NICTIZ gestelde eisen.

Hoewel de aanpassingen wel noodzakelijk zijn om op het LSP aan te worden gesloten, is dit nog altijd een betere oplossing dan geheel nieuwe systemen aan te schaffen. Dit heeft zo zijn voordelen voor de zorgverlener, omdat deze onder andere het systeem dat hij gewend is te gebruiken kan blijven gebruiken. Kosten die gemoeid zijn bij de aanschaf van een licentie, het implementeren van de software en het invoeren van alle patiëntgegevens levert veel weerstand op die nu wordt vermeden. Echter, naast de typegoedkeuring dient elke zorgsysteem ook te voldoen aan de eisen van een GBZ. Hierbij wordt niet alleen gekeken naar technische eisen, maar ook naar procedurele en functionele eisen.

Bij de typegoedkeuring is de softwareleverancier de initiator om te zorgen dat zorginstellingen, die bij hem een gebruikerslicentie hebben afgesloten, met het LSP kunnen communiceren. De eisen die gesteld zijn om als GBZ te worden aangemerkt dient door de zorginstelling zelf te worden gerealiseerd. Wanneer men een softwarepakket gebruikt dat al over een typegoedkeuring beschikt, kan een verkort GBZ goedkeuringstraject worden doorlopen. Een mogelijk probleem voor zorginstellingen is dat men, afhankelijk van de software die men gebruikt, meer of minder kosten moet maken voor een GBZ- certificering. Heeft een zorgverlener niet de software in huis met XIS-typegoedkeuring dan kan dit extra kosten betekenen in het realiseren van een GBZ door het doorlopen van het gehele GBZ traject. Terwijl, wanneer de software welk is goedgekeurd dit deels kan worden overgeslagen. Wel traject ook zal moeten worden gevolgd, investeringen zullen worden gedaan om aansluiting te vinden op het LSP.

Wanneer de XIS- en GBZ-goedkeuringen binnen zijn, kan er via het HL7v3 protocol met elkaar worden gecommuniceerd en gegevens worden uitgewisseld. Het is onduidelijk waarom het NICTIZ gekozen heeft

voor deze reeds bestaande berichtenstandaard en waarom men niet direct gekozen heeft voor de Europese EPD-standaard EN13606 die binnen niet al te lange tijd de HL7v3 zal gaan vervangen. Met dit verbeterde protocol kan er meer dan alleen berichten uitwisselen. Wanneer hieraan wordt voldaan, voldoet het systeem aan de Europese norm waardoor het data, informatie en kennis kan uitwisselen tussen systemen. Daarnaast ondersteunt EN13606 ook de ISO standaard waardoor gegevens wereldwijd kunnen worden uitgewisseld. In deze tijd van internationalisering is het kiezen voor het HL7 standaard daarom niet toekomstgericht omdat er op het moment van schrijven nog geen koppeling mogelijk is tussen beide standaarden waardoor gegevensuitwisseling onmogelijk is.

9.1.4 Beveiliging

UZI-pas

De beveiliging van het LSP bestaat uit diverse facetten. In hoofdstuk 6 wordt ingegaan op de technische toepassingen die er voor moeten zorgen dat identificatie en gebruik van patiëntgegevens zorgvuldig en alleen mogelijk is voor diegene die beschikt over de juiste tokens en bevoegdheden. Zo zal men er op technisch gebied alles aan doen om te zorgen dat de beveiliging optimaal is en blijft. Echter, beveiliging bestaat niet alleen uit technische toepassingen. De UZI-pas blijft een hulpmiddel dat, wanneer deze goed wordt gebruikt, kan garanderen dat alleen de personen met de juiste rechten toegang krijgen tot het LSP. Wanneer een UZI-pas aan een collega wordt uitgeleend, omdat deze zijn persoonlijke pas heeft vergeten, wordt het systeem alsnog toegankelijk gemaakt, zonder dat deze persoon over de juiste rechten beschikt. Het NICTIZ zal zich moeten realiseren dat ook in zorgorganisatie het gewenste beveiligingsniveau wordt zal moeten worden ingebed. Technische toepassingen zijn in deze slechts hulpmiddelen om het gebruik van het systeem in goede banen te leiden. Aan dat laatste wordt helaas te weinig aandacht geschonken

Cryptografie

Om te voorkomen dat diezelfde kwaadwillende gegevens kan inzien zonder dat hij is ingelogd in het zorgsysteem of LSP dienen gegevens te zijn versleuteld. Dat versleutelen zal plaatsvinden via het PKI-protocol. In [ELL00] wordt echter duidelijk dat PKI helemaal niet zo veilig is als men wil doen geloven. Daarbij geeft [KO006] redenen aan waarom ook een SSL-verbinding, ondanks gestelde eisen, nog altijd onbetrouwbaar kan zijn.

Naast een veilige communicatie is het ook verstandig om de gegevens ook lokaal te versleutelen. Informatie en bestanden die lokaal niet versleuteld zijn opgeslagen vormen eveneens een bron waar een kwaadwillende handig gebruik van kan maken. Wanneer gegevens lokaal zijn versleuteld is het risico dat wanneer deze toch onverhoopt op straat belanden niet te gebruiken, mits er een sterke versleuteling heeft plaats gevonden. Het versleutelen van zowel de verbinding áls de data zorgt uiteindelijk voor een verhoogde betrouwbaarheid en verbeterde privacy.

Niveau van de beveiliging

Uit onderzoek van de [INS04] is gebleken dat “ziekenhuizen op dit moment onvoldoende aandacht schenken aan risico’s die de toepassing van ICT met zich meebrengt. De patiënt loopt hierdoor een reële kans op gevaar.” Er is dus een zekere noodzaak om informatiebeveiliging in de zorg te implementeren en op orde te hebben voordat de zorginfrastructuur landelijk met elkaar is verbonden. De standaard NEN 7510 voorziet de zorg van een standaard beveiligingniveau op het gebied van ICT. Echter is dit een standaard dat slechts een aantal basisprincipes bij brengt. Zin heeft het alleen wanneer de gehele infrastructuur aan deze standaard voldoet. Daarnaast is het waarschijnlijk noodzakelijk om voor specifieke onderdelen het niveau van beveiliging zelfs scherper te maken dan de te hanteren basisstandaard. Dit omdat bijvoorbeeld de LSP op zeer specifieke onderdelen een hogere beveiligingsniveau zal moeten hebben omdat het hier om een cruciaal onderdeel in de infrastructuur betreft.

Systemen van de zorgverleners die op het LSP mogen worden aangesloten dient te zijn gecertificeerd volgens door het NICTIZ opgestelde eisen. Wanneer hieraan wordt voldaan volgt certificering en aansluiting op het LSP waarna informatie-uitwisseling mogelijk is. De certificering kan te allen tijden door het NICTIZ worden ingetrokken wanneer men niet meer voldoet aan de eisen. Niet duidelijk is wat er gebeurt wanneer een GBZ wordt afgesloten en daardoor patiëntinformatie vanaf deze locatie niet meer is op te vragen. Een zorgverlener kan daardoor niet alle patiëntinformatie inzien die hij misschien wel nodig heeft om een juiste diagnose te kunnen stellen.

Beschikbaarheid

De beschikbaarheid valt en staat bij de verbindingen met alle zorgsystemen aan het LSP. Communicatie zal veelal verlopen via het internet wat een onbetrouwbare communicatieverbinding is. Met behulp van diverse methoden, zoals besproken in sectie 5.2, kan deze onbetrouwbaarheid enigszins te niet worden gedaan. Wanneer het dataverkeer via een onbetrouwbaar kanaal verloopt en is niet te zeggen of derden dit verkeer heeft onderschept of gebruikt. Dit risico is dus niet uitgesloten. Toch kan dit veilige datacommunicatie worden gerealiseerd door deze via een besloten “zorgnetwerk” te transporteren. Gevaren vanuit de “buitenwereld” zijn hierdoor uitgesloten, omdat alleen zorgsystemen van dit netwerk gebruik kunnen maken en andere de toegang tot het netwerk wordt ontzegt.

Dat zorgnetwerk hoeft niet opnieuw te worden ontworpen. Een mogelijke kandidaat heeft zich reeds aangediend, namelijk SURFnet5. Dit netwerk, dat nú nog door het hoger onderwijs en universiteiten wordt gebruik, biedt vele kansen en mogelijkheden vooral vanwege het feit dat het reeds al actief is en dat binnen niet al te lange termijn is over te nemen omdat de universiteiten overgaan op een verbeterde versie, SURFnet6.

Maar ook KPN, biedt een besloten zorgnetwerk aan, SURFnet, ZorgConnect en E-zorg. Het voordeel van dit netwerk is dat het een landelijk, besloten netwerk, voor de hele zorgsector is waarbij via een verbinding toegang kan worden verkregen tot andere aangesloten zorgverleners in Nederland.

9.1.5 Logging

Het principe van logging is dat het gebruikt kan worden om naderhand te kunnen achterhalen welke acties een gebruiker op het LSP heeft uitgevoerd. Met behulp van dit overzicht kunnen beheerders dan altijd controleren of een actie ook daadwerkelijk rechtvaardig is geweest. Wanneer blijkt dat een actie onterecht heeft plaats gevonden, zou men maatregelen of sancties kunnen nemen, waarbij het logboek als bewijs dient.

Desondanks zijn er enkele problemen die de functionaliteit van het logboek negatief beïnvloeden. Zo zal de omvang van de logfiles aanzienlijk zijn waardoor het zoeken naar de juiste gegevens lastig, tijdrovend en veel resources vereist. Ook kan een kwaadwillende proberen deze gegevens te manipuleren waardoor niet meer te achterhalen is wie verantwoordelijk is voor een actie of welke acties er door een persoon zijn uitgevoerd. Daarbij komt dat met loggen er pas achteraf maatregelen kunnen worden getroffen wanneer de actie(s) zich al hebben voorgedaan.

De dagelijkse informatiestroom resulteert in vele logsacties en dus in grote bestanden met actiegegevens. De omvang van deze file vormt een probleem vooral omdat deze gegevens minimaal tien jaar direct opvraagbaar moeten zijn. Dit betekent ondermeer dat naast een slimme zoekmethode er ook de nodige aandacht zal moeten worden besteed aan het enorme dataverkeer en opslagruimte. Men zal een logsysteem moeten bouwen dat deze gegevens kan verwerken en opslaan, maar ook is te hanteren en te gebruiken om gegevens op te zoeken en te controleren. Het NICTIZ denkt wel na hoe deze problematiek zal moeten worden aangepakt, maar heeft hiervoor nog geen concrete oplossing. Hierdoor blijft in het midden hoe er invulling gegeven zal worden gegeven aan het beheer en het verwerken van deze data.

Naast het handmatig controleren van acties is het zeer zinvol om dit in ook continue geautomatiseerd plaats te laten vinden. Het handmatig controleren wordt dan alleen uitgevoerd wanneer men dit nodig acht, bijvoorbeeld wanneer resultaten aangeleverd door het geautomatiseerd proces hiervoor aanleiding toe geeft.

Het opslaan en zoeken naar acties die door gebruikers op het systeem zijn uitgevoerd dienen uiteraard ook beveiligd te worden, zodoende dat deze niet door eventuele kwaadwillenden kunnen worden in gezien (onder andere vanwege privacy) of gewijzigd. Belangrijke informatie gaat dan immers verloren waardoor bepaalde acties niet meer kunnen worden getraceerd of zelfs de link naar de gebruiker is aangepast.
Om te voorkomen dat loginformatie wordt overschreven door een (al dan niet) kwaadwillende, gebruikt men een methode om logfiles append-only te maken. Deze methode is een verfijning op de zogenaamde immutable files. Hierdoor kan iedere gebruiker op het LSP deze bestanden, nadat een actie heeft plaats gevonden, niet meer wijzigen of verwijderen. Voor het veiligstellen van de gebeurtenissen met behulp van de logfiles wordt het daardoor voor kwaadwillenden minder eenvoudig om belangrijke data te wijzigen of zelfs te verwijderen.

9.1.6 Afname van fouten of toch niet

De invoering van dit nieuwe systeem levert naast nieuwe toepassingen en verbeteringen ook problemen op waaraan in de diverse NICTIZ documentatie geen aandacht aan wordt geschonken. Zo bestaat er de kans dat gegevens verkeerd worden geïnterpreteerd door de verhoging van de digitale communicatie.
Daarnaast zullen er nieuwe fouten en problemen ontstaan door de invoering en gebruik van dit systeem. Immers levert een nieuw systeem nieuwe problemen op die voor de implementatie niet aan de orde waren. En dat terwijl de doelstelling ondermeer is om (zowel de medische als niet medische) fouten juist te reduceren.

Een patiëntdossier wordt samengesteld vanuit verschillende bronnen waar een patiënt onder behandeling is. Door het digitale netwerk wordt deze informatiestroom aanzienlijk uitgebreid waardoor het uitwisselen van informatie als gevolg daarvan ook zal gaan stijgen. Het digitaal uitwisselen heeft als voordeel dat men geen problemen meer heeft met het ontcijferen van handgeschreven aantekeningen. Keerzijde is dat gegevens verkeerd kunnen worden geïnterpreteerd. Dit is op te lossen door bij elke aantekening in een dossier een identificerende codering toe te voegen, waardoor andere zorgverleners kunnen nagaan wat de basis van de klachten is. De aanvullende bevindingen van de zorgverlener zorgen dan voor een patiënt afhankelijke invulling. Met toevoeging van deze codering is doorzoeken van dossiers of reeks van dossiers eenvoudiger in te richten, kan men eenvoudiger kijken wat andere zorgverleners in bepaalde gevallen hebben gedaan en wordt misinterpretatie voorkomen.

Deze bevinding wordt ook ondersteund door [ERN98] die het volgende concluderen: “Ten aanzien van de koppeling van de EPD's van de diverse zorgverleners is ook nog veel werk te doen. Op dit punt is het van belang om te realiseren dat dit niet slechts een technische kwestie is. Voldoende afstemming van de werkwijze van de betrokken zorgverleners is een voorwaarde om de in de EPD's opgenomen gegevens ook daadwerkelijk effectief in het zorgproces te kunnen benutten. Denk hierbij bijvoorbeeld aan het voeren van aansluitende zorgprotocollen. De stelling dat zorgverleners altijd effectief met elkaar kunnen samenwerken zolang hun systemen maar goed via technische protocollen (bijvoorbeeld HL7) met elkaar kunnen praten, berust ons inziens op een misverstand. Het gevaar schuilt in dit geval in de misinterpretatie van gegevens en vooral in het ontbreken van een methode om deze misinterpretatie aan het licht te brengen.”

Om gegevens goed te kunnen beoordelen en dossiers te kunnen doorzoeken is het verstandig om middels een uniforme terminologie en datamodel dit te realiseren. Het is ieder geval een stap naar standaardisatie van patiëntgegevens. Dat het moeilijk is hierin een goede middenweg in te vinden leert ons de historie. Het Unified Medical Language System (ULMS), dat jaren geleden in de Verenigde Staten werd opgezet heeft het uiteindelijk niet gered, waardoor het gehele project in de ijskast verdween.

Weinig rekening heeft men ook gehouden met de problematiek dat de infrastructuur met LSP en zorgsystemen ondanks verbeteringen voor diverse belanghebbenden ook nieuwe problemen zal introduceren.

Uit onderzoek van [SPA05] blijkt dat ICT een bijdrage alsmede een bedreiging kan zijn voor de kwaliteit van de zorg, waardoor de patiënt onnodig gevaar loopt. Zo wordt de NEN 7510 code in de zorginstellingen niet systematisch nageleefd, wat volgens de IGZ ondermeer leidt tot onjuiste invoer, verwisseling van gegevens, onjuiste interpretatie, verkeerd aanklikken, vernietiging van gegevens door virussen, verantwoordelijkheidsperikelen bij ontraceerbare acties van gegevensmutaties, uitval van apparatuur, fouten door niet aansluiten van apparatuur op het systeem en gebrekkige bescherming van privacy van de patiënten. Dergelijke risico's en problemen zijn ronduit schokkend, vooral in een sector als de gezondheidszorg waarbij de ICT een belangrijke bijdrage kan leveren aan het verbeteren van de zorg. Door ICT juist in de organisatie in te bedden kunnen resultaten worden geboekt die daadwerkelijk ook enige vorm van betekenis hebben.

9.2 Antwoord deelvraag 2

Hoe kan er op onrechtmatige wijze toegang tot het LSP worden verkregen en hoe kunnen daaruit voortvloeiende risico's worden beperkt?

a) Met welke methode kunnen de mogelijkheden die een kwaadwillende heeft om zijn doel te bereiken worden geïdentificeerd en schematisch in kaart worden gebracht?
b) Hoe kan per risico bepaald of het noodzakelijk is maatregelen te treffen tegen het geïdentificeerde risico.
c) Hoe kunnen invloeden van geïdentificeerde risico's worden beperkt?

Om inzicht te verkrijgen in de mogelijkheden die een kwaadwillende heeft is het noodzakelijk om een risicoanalyse uit te voeren. Met een dergelijke analyse is het de bedoeling risico's te identificeren en hiervoor maatregelen aan te dragen om uiteindelijk de risico's die het LSP negatief kunnen beïnvloeden te verminderen of zelfs weg te nemen. Om te weten te komen welke risico's er zijn, is het allereerst van belang de mogelijkheden die een kwaadwillende heeft, te identificeren. Het identificeren kan door gebruik te maken van de attack tree methode. Vanuit het oogpunt van de aanvaller wordt dan bekeken op welke wijzen het doel, het toegang krijgen tot het LSP, kan worden gerealiseerd. De risicofactoren en CIA-classificaties die aan de mogelijke attacks worden toegekend leveren uiteindelijk indicatiecijfers op. Met deze eindcijfers kan aangetoond worden in hoeverre het noodzakelijk is om de risico's op korte termijn weg te nemen omdat deze van invloed zijn op de vertrouwelijkheid, integriteit en betrouwbaarheid van het LSP. Kortom, de beslissing bevoegde personen kunnen op basis van deze gegevens besluiten welke risico's weg moeten worden genomen. In hoofdstuk 4 wordt in gegaan op de theorie rondom de risicoanalyse en de attack tree methode. De uiteindelijke uitvoering van de theorieën en de resultaten zijn in hoofdstuk 8 terug te vinden.

9.2.1 Opmerkingen

De risicoanalyse is gebaseerd vanuit het oogpunt van de aanvaller om toegang te krijgen tot het LSP. Door vervolgens de kans en de schade welke een dergelijke attack kan opleveren, wordt de risicofactor bepaald. Samen met de CIA vormt zich dan een identificerend getal dat de noodzaak aangeeft om te investeren in iets tegen deze attack en deze zo goed als het kan onschadelijk te maken of het effect ervan weg te nemen.

De risicoanalyse wordt getriggerd door de onderkende aanvalmogelijkheden die kwaadwillenden zouden kunnen uitvoeren om daarmee zichzelf toegang te verschaffen tot het LSP. De attack tree methode geeft inzicht in de mogelijkheden welke een kwaadwillende heeft om daadwerkelijk toegang te verkrijgen tot het LSP en op welke manier dit zich kan voltrekken.

Het principe van een attack tree is zo simpel dat deze eenvoudig is op te stellen. Problemen doen zich echter voor wanneer het doel zo breed is dat door het grote aantal attacks uiteindelijk de boomstructuur moeilijk te construeren is en daardoor onleesbaar wordt. Dit is mede ook te wijten aan het ontbreken van een tekenprogramma, waardoor het een lastige en tijdrovende klus wordt wat eveneens ten koste gaat van de effectiviteit van een risicoanalyse door de te lange doorlooptijd.

Het is dus aan te raden om een programma te ontwikkelen waardoor dit ontwikkelproces wordt vergemakkelijkt en versneld. Het identificeren van de inhoud van een boom blijft een klus van domeinexperts. Datzelfde geldt voor het schatten van de kans- en schadefactor en de CIA-score welke een attack kan hebben op het systeem wanneer deze wordt uitgevoerd. Deze vormen de basis waarop men uiteindelijk beslist of men dient te investeren in het oplossen of tegen gaan van een attack, waardoor deze minder of zonder succes kan worden uitgevoerd en daardoor toegang tot het LSP door een kwaadwillende wordt tegen gegaan.

Het uitvoeren van een dergelijke analyse moet door domeindeskundige worden uitgevoerd om zo te voorkomen dat de risicofactoren onjuist zijn geschat en waardoor men beslissingen en investeringen gaat doen die niet overeenkomen met de realiteit en dus geen invloed hebben op het bedwingen en tegenhouden van aanvallen. Met deze domeindeskundige worden dus dreigingen te niet gedaan en onnodige investeringen vermeden. Helaas is niets in de toekomst zeker en zijn de schattingen niets meer dan schattingen, waardoor de werkelijkheid anders kan uitpakken dan men vooraf had voorspeld.

Het bepalen welke attacks een direct risico vormen voor het LSP zijn in dit onderzoek aangeduid met “noodzakelijk” om op te lossen. In de werkelijkheid kijkt men niet alleen naar de risico’s, maar ook naar de impact van de attack, de kosten voor een oplossing, de haalbaarheid tot implementeren en vervolgens de impact op de werkbaarheid van deze oplossing op het systeem. De in dit onderzoek gehouden risicoanalyse geeft slechts de risico’s weer, hun mogelijke gevolgen wanneer er niets tegen wordt gedaan, de kans dat dit gebeurd vermenigvuldigd met de schade en een eventuele oplossing om de attack onschadelijk of minder effectief te maken. De risicoanalyse biedt dus een handvat om uiteindelijk te kunnen beslissen

welke attacks daadwerkelijk in aanmerking komen om te worden opgelost en welke men niet relevant genoeg vindt voor oplossen.

Hoewel de beschreven attacks een breed gebied in de beveiliging van een systeem beschrijven, is het niveau van detaillering moeilijk in te schatten. Teveel of juist te weinig details zorgt voor een onduidelijke analyse die uiteindelijk de beslissers geen goed zal doen waardoor de kans bestaat dat zij op basis daarvan verkeerde beslissingen gaan nemen. Om te zorgen dat men de juiste beslissingen neemt is het verstandig naar verloop van tijd te controleren of de gemaakte beslissingen invloed hebben gehad op de betrouwbaarheid van het systeem evenals nieuwe aanvalsmogelijkheden te identificeren. Dit iteratieve proces zorgt ervoor dat men constant op de hoogte blijft van de risico's die op een bepaald moment van invloed kunnen zijn op het systeem evenals te kunnen beslissen welke risico's in aanmerking komen om te worden aangepakt.

Met behulp van een risicoanalyse kan men een bepaald veiligheidsniveau bereiken en deze verbeteren, waardoor uiteindelijk de betrouwbaarheid in het systeem bij de gebruikers groeit en de kans dat het gebruik een succes wordt verbeterd. De kans bestaat echter wel dat zogenaamde "emerging risks" te laat worden ontdekt en door de periode waarin geen risicoanalyse plaats vindt wel een risico voor het systeem is. Dit als gevolg van het feit dat men een dergelijke analyse uitvoert op datgene wat men nu weet. De zekerheid dat men met een risicoanalyse niet heeft is dat alle risico's worden gevonden.

9.3 Antwoord op onderzoeksvraag

Welke mogelijkheden heeft een kwaadwillende om toegang te krijgen tot het LSP en hoe kunnen de invloeden van de gevonden risico's worden beperkt.

Door het beantwoorden van beide deelvragen is er een fundament gecreëerd waardoor de hoofdvraag ook wordt beantwoord.

Appendix A: Tabellenlijst

Appendix B: Figurenlijst

Appendix C: Afkortingen

AIS	Apotheek Informatie Systeem
BSN	Burger Service Nummer
CA	Certification Authority
CIA	Confidentiality, Integrity, Availability
CSP	Certification Service Provider
DCN	Data Communicatie Netwerk
EN13606	Electronic Health Record Communication
EMD	Elektronische Medicatie Dossier
EPD	Elektronisch Patiënten Dossier
FTP	File Transport Protocol
GBZ	Goed Beheerd Zorgsysteem
GIBG	Centraal Informatiepunt Beroepen Gezondheidszorg
HIS	Huisarts Informatie Systeem
HL7v3	Health Level 7 versie 3
HTTP	HyperText Transfer Protocol
ICT	Informatie- en Communicatie Technologie
IDS	Intrusion Detection System
IGZ	Inspectie voor de Gezondheidszorg
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organisation for Standardization
LSP	Landelijk SchakelPunt
NAT	Network Adress Translation
NCSC	National Computer Security Center
NEN	Nederlands Normalisatie Instituut
NICTIZ	Nationaal ICT Instituut in de Zorg
P2P	Peer-to-Peer
PIN	Persoonlijk Identificatie Nummer
PKI	Public Key Infrastructure
PKIO	Public Key Infrastructure Overheid
RAM	Risico Analyse Methode
SBV-Z	Sectorale BerichtenVoorziening Zorg
SLA	Service Level Agreement
SOFI-nummer	Sociaal Financieel nummer
SPOC	Single Point Of Contact
SPOF	Single Point Of Failure
SSL	Secure Socket Layer
TLS	Transport Layer Security

TTP	Trusted Third Party
UPID	Universele Patiënten Identificatie Database
ULMS	Unified Medical Language System
USB	Universal Serial Bus
UZI-register/pas	Unieke Zorgverlener Identificatie register/pas
UZOVI	Unieke Zorgverzekeraars Identificatie
VOC	Verenigde Oost-Indische Compagnie
VPN	Virtual Private Network
WBP	Wet Bescherming Persoonsgegevens
WDH	Waarneem Dossier Huisartsen
WGBO	Wet op de Geneeskundige Behandelingsovereenkomst
XIS	Verzamelnaam voor AIS, HIS, ZIS e.d.
ZG	Zorgaanbiedergids
ZIM	Zorg Informatie Makelaar
ZIS	Ziekenhuis Informatie Systeem
ZSP	Zorg Service Providers

Appendix D: Bibliografie

[AND93] Anderson, R., *Why Cryptosystems Fail*, Comm. of the ACM, v. 37, n. 11, Nov., pp. 32-40, 11 November 1994.

[BUR04] Burleson, D. K., *Database auditing for risk management and regulatory compliance*, jaargang 165, Burleson Consulting, November 2004.

[CBS06] Centraal Bureau voor de Statistiek, *Gezondheid en zorg in cijfers 2006*, 2006.

[CLE05] Cleiren, C. P. M. en Nijboer, J. F., Tekst & Commentaar: Strafverordening, Kluwer, Deventer, 2005.

[DEG07] De Gelderlander, *Een misser per week*, jaargang 159, pagina 10-11, 28 Februari 2007.

[ELL00] Ellison, C., en Schneier, B., *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure*, Computer Security Journal, Volume XVI, Nummer 1, 2000.

[HAN05] Hansen, L., Velden, L. F. J., Hingstman, L., *Behoefteraming klinisch geriaters*, pp 11, 60-61, Nivel, 2005.

[ERN98] Ernst & Young, *Elektronische patiëntendossiers in Nederlandse ziekenhuizen*, 2003.

[FER98] Ferguson, P. en Huston, G., *What is a VPN?,* The Internet Protocol Journal, Volume 1, Nr 1, Cisco Systems, Maart 1998.

[INS04] Inspectie voor de volksgezondheid, *IGZ-rapport: ICT in de zorg*, Augustus 2004.

[JAN05] Janssen, D., *Social engineering: de menselijke schakel in de Informatiebeveiliging*, Master thesis, Radboud Universiteit Nijmegen, 2005.

[KIE06] Kieskamp, A. en Smit, R., *De bouwstenen van Social Engineering: Een gestructureerd overzicht getoetst bij de overheid*, Master thesis, Radboud Universiteit Nijmegen, 2006.

[KOO06] Kooman, F., *Websurfen met onbetrouwbare computers*, Bachelor thesis, Radboud Universiteit Nijmegen, December 2006.

[MAR86] Martin, J., *Information Engineering*, Savant, Carnforth, 1986.

[MAU06] Mauw, S. en Oostdijk, M., *Attack Trees: Door de bomen de bedreigingen zien*, GvIB Informatiebeveiliging, Vol. 7 pp. 16--17, Februari 2006.

[MAU05] Mauw, S. en Oostdijk, M., *"Foundations of attack trees"*, presented at Eighth Annual International Conference on Information Security and Cryptology, LNCS 3935, pp. 186--198, Seoul, 2005.

[MCC05] McCumber, J. en Kelly, L., *Assessing and Managing Security Risk in IT Systems*, CRC Press LLC, Boca Raton, 2005.

[MCD94] McDaniel, G., *IBM Dictionary of Computing*, McGraw-Hill Inc., New York, 1994.

[NCS87] National Computer Security Center, *Trusted Network Interpretation of the trusted computer system evaluation criteria*, Juli 1987.

[NEN04] Nederlands Normalisatie-instituut, *Implementatiehandboek NEN 7510: Informatiebeveiliging in de zorg*, Nederlands Normalisatie-instituut, 2004.

[NEN97] Nederlands Normalisatie-instituut, *NEN EN 1050 Safety of machinery: principles for risk assessement*, NEN-uitgeverij, Februari 1997.

[NIC05a] NICTIZ, *Specificatie van de basisinfrastructuur in de zorg,* versie 2.2, Juni 2005.

[NNI97] Nederlands Normalisatie-instituut, *Medische informatica - Indeling van beveiliging en bescherming van informatiesystemen in de gezondheidszorg* (*NVN-ENV 12924:1997 EN)*, December 1997.

[OVE99] Overbeek, P.L. en Sipman, W. H. M., *Informatiebeveiliging*, Tutein Nolthenius, Den Bosch, 1999.

[PFL03] Pfleeger, C. P. en Pfleeger, S. L., *Security in Computing*, Pearson Education Inc, Upper Saddle River, 2003.

[RID98] Ridderbeekx, E. J. M. en van den Berg, J., *Internetbeveiliging: een beheersperspectief*, Erasmus Universiteit, 1998.

[SCH00] Schneier, B., *Secrets & lies, digital security in a networked world*, Wiley Computer Publishing, New York, 2000.

[SCR05] Schrijvers, L., *Secure processing of confidential digital information in a potentially insecure environment*, Technische Universiteit Eindhoven, 2005

[SMI03] Smit, T., *Elektronische patiëntendossier te complex*, Computable, jaargang 12, nummer 35, pp. 1, Augustus 2003.

[SPA05] Spaink, K., *Medische Geheimen*, Nijgh & Van Ditmar en XS4ALL, Amsterdam, 2005.

[UZI05] UZI-register, *Veilige en betrouwbare informatie verzorgd!*, Juli 2005.

[UZO05] UZORG, *Elektronische Patiënten Dossier*, Congres Kivi Niria, Oktober 2005.

[VER01] Verschuren, P. en Doorewaard, H., *Het ontwerpen van een onderzoek*, Lemma B.V, Utrecht, 2001.

[VOL05] Spaink, K., *Het medische geheim is in gevaar*, Volkskrant, jaargang 95, 3 September 2005.

[WHE05] Wheeler, D. A., *Countering Trusting trust through Diverse Double Compiling*, Proc. 21st Annual Computer Security Applications Conference, pp. 33-48. Available in IEEE area of GMU digital library, 5-9 December 2005.

[WEI05] Weise, J., en Powell, B., *Using Computer Forensics when investigating system attacks*, Sun Microsystems Inc, April 2005.

[ZON02] ZonMw, *Geboden en verboden toegang tot het EPD*, Informatie- en Communicatietechnologie in de Zorg, 2002.

Internetlocaties

[WEBBSN] BSN, http://www.programmabsn.nl,
Geraadpleegd op: 5 Oktober 2005.

[WEBCOM] Computable, http://www.computable.nl/nieuws.htm?id=819815,
Geraadpleegd op: 18 Januari 2007.

[WEBCVI] CVIB, http://www.cvib.nl/cvibnew/2001/10/bruce_schneier.php,
Geraadpleegd op: 19 December 2006.

[WEBAVE] Avenua A /Razorfish, http://www.avenuea-razorfish.com/articles/InformationSecurity_Lodha.pdf, Geraadpleegd op: 8 December 2006.

[WEBMIC] Micosoft, http://www.microsoft.com, Geraadpleegd op: 14 Mei 2006.

[WEBNEN] NEN, http://www2.nen.nl, Geraadpleegd op: 15 Februari 2006.