De bouwstenen van Social Engineering:

Een gestructureerd overzicht getoetst bij de overheid

Plan van Aanpak

Versie: Final

Arjan Kieskamp
Studentnummer: 0441147
Email: a.a.kieskamp@student.ru.nl

Robert Smit
Studentnummer: 0444855
Email: crsmit@student.ru.nl

Radboud Universiteit Nijmegen

Inhoudsopgave

1 Inleiding 1
2 Achtergrondinformatie 1
3 Onderzoeksinformatie 3
3.1 Probleemgebied 3
3.2 Doelstelling 3
3.3 Probleemstelling 4
3.3.1 Onderzoeksvragen 4
3.3.2 Deelvragen 4
3.4 Verankering 5
4 Strategie 5
4.1 Methode 5
4.1.1 Literatuuronderzoek 5
4.1.2 Opstellen begripsbepaling 6
4.1.3 Opstellen conceptueel framework 6
4.1.4 Informatieverzameling bij ministeries 6
4.1.5 Informatieverwerking 6
4.1.6 Representativiteit van informatie 8
4.1.7 Geheimhouding en publicatie van informatie 8
4.2 Resultaten 9
4.3 Aannames en uitgangspunten 9
4.4 Taakverdeling 9
5 Contactpersonen 11
6 Literatuurlijst 12
6.1 Internet 12
6.2 Boeken 12
7 Bijlagen 13
7.1 Bijlage I Geheimhouding en publicatie van gevoelige informatie 13
7.1.1 Over deze bijlage 13
7.1.2 Publicatie 15

1 Inleiding

In dit document wordt het plan van aanpak beschreven van het onderzoek: De bouwstenen van Social Engineering: Een gestructureerd overzicht getoetst bij/op de overheid. Dit onderzoek wordt uitgevoerd als afsluitend onderdeel van de studie Master of Information Science aan de Radboud Universiteit te Nijmegen.

Het onderzoek zal worden uitgevoerd als duo en worden begeleid als duo door Martijn Oostdijk en Wolter Pieters. Het onderzoek zal onderverdeeld worden in twee deelopdrachten waardoor een duidelijke scheiding ontstaat in de bijdrage van beide studenten. Op deze wijze kunnen we beide laten zien wat onze individuele capaciteiten zijn om zodoende te kunnen voldoen aan de gestelde eisen van het afstuderen.

In de hierop volgende hoofdstukken zal worden beschreven wat de inhoud van het onderzoek is en wat de uitgangspunten zijn. Daarnaast zal beschreven worden op welke wijze het onderzoek zal worden aangepakt, welke werkverdeling er wordt toegepast en hoe globaal de planning van activiteiten is ingedeeld.

2 Achtergrondinformatie

In onze huidige samenleving zijn er steeds meer organisaties afhankelijk van informatie. Om als informatie-intensieve organisatie competitief en slagvaardig te zijn is een juiste en tijdige aanlevering van informatie van groot belang. Doordat informatie een steeds belangrijkere rol speelt is de beveiliging van informatie noodzakelijk. Redenen hiervoor zijn het waarborgen van de juistheid, tijdigheid van informatie en het voorkomen van vervalsing, onderschepping en ontbreken van informatie. Steeds meer bedrijven besteden daarom aandacht aan informatiebeveiliging door het onderdeel te maken van hun bedrijfsbeleid of op te nemen in een afzonderlijk informatiebeveiliging beleidsdocument. Het beleid is vaak een document op hoog niveau waarin verschillende aandachtsgebieden zoals organisatie, verantwoordelijkheden en minimale eisen wordt beschreven. Een concrete invulling van het beleid dat zich uit in verschillende maatregelen zal meestal door de desbetreffende verantwoordelijken worden bepaald.

Om de informatie in de organisatie goed te kunnen beveiligen zijn maatregelen op zowel technisch niveau als organisatorisch niveau noodzakelijk. Op technisch niveau hebben de organisaties hun informatiebeveiliging vaak op orde. Dit komt door dat bedreigingen op dit niveau meestal vooraf te bepalen en te herkennen zijn waardoor er concrete technische maatregelen genomen kunnen worden. Op organisatorisch gebied is dit echter niet het geval [1]. Ten eerste is het de vraag of op dit niveau wel alle bedreigingen te herkennen zijn en of de maatregelen wel toereikend zijn. Ten tweede is het de vraag of de maatregelen, welke vooral door de mensen in de organisatie moeten worden uitgevoerd, wel bekend zijn bij deze mensen. De mens als zwakste schakel in het informatiebeveiligingsproces is vaak een ondergeschoven gebied binnen de informatiebeveiliging. De meeste organisaties hebben het

idee dat wanneer de technische maatregelen in orde zijn zij voldoende beschermt zijn. Dit is echter niet het geval omdat de het gebruik van de mens als zwakste schakel voor het verkrijgen van gevoelige informatie in vele gevallen eenvoudig en sneller is dan het inbreken in de informatiesystemen van een organisatie. Deze manier om deze informatie los te krijgen bij de mens door de mens te kraken als zwakste schakel in de informatiebeveiliging wordt Social Engineering genoemd [2].

3 Onderzoeksinformatie

3.1 Probleemgebied

Over het onderwerp Social Engineering zijn al veel artikelen geschreven. Elke auteur behandelt vaak slechts een klein deel van het onderwerp of probeert met behulp van voorbeelden duidelijk te maken wat Social Engineering is. In geen enkel artikel wordt er een poging gedaan om een volledig beeld te scheppen wat het begrip Social Engineering nou precies inhoudt.

Omdat informatie steeds belangrijker wordt besteden steeds meer organisaties aandacht aan hun informatiebeveiliging. Social Engineering wordt vaak niet als serieuze dreiging meegenomen in de informatiebeveiliging waardoor organisaties een makkelijk doelwit zijn voor Social Engineering. Organisaties dienen daarom hun informatiebeveiliging op peil te brengen door Social Engineering als dreiging op te nemen. De overheid is de grootste informatie-intensieve organisatie van Nederland en werkt met allerlei gevoelige informatie over overheids- en burgerzaken. Van de overheid mag dus verwacht worden dat zij vanwege haar verantwoordelijkheid tegenover de burgers zorgvuldig met deze gevoelige informatie omgaat [3]. Dit betekent dat de overheid op gebied van informatiebeveiliging de zwakste schakel, haar medewerkers moet beschermen tegen Social Engineering. Vanuit de gedachte om in dit onderzoek Social Engineering zo volledig mogelijk in kaart te brengen zal een poging gedaan worden om de overheid in de praktijk te toetsen om vast te stellen of de overheid voldoende beschermd is tegen Social Engineering.

3.2 Doelstelling

De doelstelling van dit onderzoek is het verduidelijken van het begrip Social Engineering. Dit zal gedaan worden door het opstellen van een begripsbepaling en een overzichtelijk conceptueel framework gebaseerd op bestaande literatuur. De begripsbepaling draagt bij aan de onderbouwing van begrippen onder andere genoemd in het framework. Het framework zelf moet bijdragen aan een verbeterd inzicht door te visualiseren wat Social Engineering precies inhoud en waar de bedreigingen zich in de organisatie kunnen bevinden.

Tevens heeft dit onderzoek als doel te bepalen of de overheid beschermd is tegen Social Engineering. Dit zal gedaan worden door interviews bij de verschillende ministeries af te nemen. Vervolgens wordt er een algemeen advies opgesteld dat zal bestaan uit een opsomming van aandachtspunten die kunnen leiden tot een betere bescherming tegen Social Engineering. Het advies is gebaseerd op overeenkomsten tussen de ministeries vergeleken met de begripsbepaling en het framework en zaken die zijn opgevallen tijdens en bij de uitwerking van de interviews.

3.3 Probleemstelling

3.3.1 Onderzoeksvragen

1. Wat omvat het begrip Social Engineering?
2. Is de overheid beschermt tegen Social Engineering?

3.3.2 Deelvragen

Bij onderzoekvraag 1

1. Wat is een bruikbare definitie van het begrip Social Engineering voor dit onderzoek?
2. Wat zijn de belangrijkste doelen van Social Engineering?
3. Welke mogelijke Social Engineering aanvallen zijn er en wat zijn de kenmerken hiervan?
4. Zijn er overige factoren die invloed hebben op Social Engineering?
5. Is Social Engineering te structureren in een framework zodat het inzichtelijker wordt?

Bij onderzoeksvraag 2

1. Wat doet de overheid tegen Social Engineering?
2. Is de overheid bestand tegen de verschillende soorten aanvallen uit ons framework?
3. Is het framework van toegevoegde waarde voor een verbeterde bescherming tegen Social Engineering?

3.4 Verankering

Het thema informatiebeveiliging speelt een steeds belangrijkere rol in het dagelijkse leven. Het vraagt daarom om het nodige onderzoek naar de zwakke plekken in de informatiebeveiliging bij organisaties die werken met "gevoelige informatie". Technische oplossingen zijn vaak voldoende beproefd om indringers buiten de deur te houden; de zwakste schakel in de informatiebeveiliging is de mens en vaak wordt dit probleem onderschat. Vanuit een informatiekundige invalshoek is het zeer interessant om onderzoek te doen naar de combinatie van informatiebeveiliging en de mens als zwakste schakel hierin. Inperking van het onderzoek zal plaatsvinden op:

- Social Engineering, omdat de mens als zwakste schakel in de beveiliging van informatie vaak wordt onderschat [3],[4], zal dit onderzoek zich beperken tot de verschillende mogelijke vormen van Social Engineering. Onderzoek op het gebied van Social Engineering zal hopelijk leiden tot een meer aandacht voor dit onderwerp, expliciete opname in het beveiligingsbeleid en bewustzijn van de medewerkers bij de overheid.

- Nationale overheid, zie hoofdstuk 3.1 . De nationale overheid bestaat uit een aantal ministeries. Door onderzoek te doen bij deze ministeries kan een beeld gevormd worden hoe de overheid omgaat met de bedreigingen op het gebied van Social Engineering en of de overheid beschermd is tegen Social Engineering.

4 Strategie

4.1 Methode

4.1.1 Literatuuronderzoek

Om een goed beeld te kunnen vormen wat Social Engineering nou precies is dient er een onderzoek uitgevoerd te worden naar wat er al aan literatuur over dit onderwerp aanwezig is. Hiervoor worden verschillende wetenschappelijke bronnen[1] gehanteerd en wordt er met behulp van zoekmachines op internet gezocht naar relevante artikelen.

Na de verzameling van de literatuur wordt er gekeken naar de relevantie van de artikelen en de bijdrage die zij kunnen leveren aan het onderzoek.

[1] Deze bronnen zijn: Universiteitsbibliotheek database, IEEE, ACM en scholar.google.com

4.1.2 Opstellen begripsbepaling

Aan de hand van de geselecteerde literatuur worden de verschillende onderdelen van Social Engineering beschreven in de begripsbepaling. De begripsbepaling zal onder andere een definitie geven van Social Engineering zoals gebruikt in dit onderzoek. Daarnaast worden de verschillende onderdelen van Social Engineering, zoals doelen, aanvallen en overige factoren beschreven. De begripsbepaling dient als basis voor het opstellen van het conceptuele framework.

4.1.3 Opstellen conceptueel framework

Met de begripsbepaling als uitgangspunt wordt er eerste poging gedaan om te komen tot een overzichtelijk conceptueel framework. Het framework moet bijdragen aan een verbetert inzicht wat Social Engineering precies inhoud en waaruit het is opgebouwd. Hierbij geldt dat het framework gezien moet worden als ordenend principe van bestaande literatuur over Social Engineering.

4.1.4 Informatieverzameling bij ministeries

Open interviews
De informatieverzameling bij de overheid zal bestaan uit een aantal open interviews bij onderdelen van verschillende ministeries. Deze interviews zullen gehouden worden met mensen die te maken hebben met de concrete invulling van het op hoogniveau opgestelde informatiebeveiliging beleid. Per ministerie zal er minimaal met twee personen gesproken worden.

Voorafgaand aan het interview zullen er aan de hand van de begripsbepaling en het conceptuele framework interview vragen geformuleerd worden (maximaal 10) die verstuurd worden aan de verschillende geïnterviewde personen. Reden hiervoor is dat zij zich voldoende voor kunnen bereiden op het eigenlijke interview wat moet leiden tot concretere antwoorden. Tijdens het interview zal er dieper op deze vragen worden ingegaan. Elk interview zal ongeveer één uur in beslag nemen.

4.1.5 Informatieverwerking

Begripsbepaling
De begripsbepaling komt tot stand door de analyse van bestaande literatuur over Social Engineering. In deze analyse zullen de verschillende artikelen met elkaar worden vergeleken en zal er bepaald worden welke informatie er relevant is voor de begripsbepaling. De begripsbepaling moet een duidelijke beschrijving zijn van alle aspecten van Social Engineering afkomstig uit de verschillende literaire bronnen.

Conceptueel framework

Informatie uit de begripsbepaling zal gebruikt worden bij het opstellen van het conceptueel framework. De informatie zal gebruikt worden in brainstormsessies, voor het maken van prototypes van het framework en toetsing van het framework. Bij de toetsing is het de bedoeling dat de onderdelen in het framework te herleiden zijn uit de begripsbepaling. Het framework geeft deels antwoord op onderzoeksvraag één.

Open interviews
Onderzoeksvraag twee wordt beantwoord aan de hand van de verschillende afgenomen interviews waarbij de begripsbepaling en het framework als basis dienen. Door de verschillende interviews wordt er bepaald of de ministeries beschermd zijn tegen Social Engineering.

Van elk interview zal er een kort interviewverslag worden geschreven met daarin een bondige formulering van de antwoorden op de gestelde vragen. Deze verslagen zullen te goedkeuring naar de verschillende geïnterviewden verstuurd worden. Na goedkeuring kunnen de resultaten uit de verslagen gebruikt worden voor het opstellen van het algemeen advies.

Advies ministeries

Het advies zal opgesteld worden aan de hand van de resultaten verkregen uit de verschillende interviews. Het advies zal algemeen van aard zijn wat betekent dat de ministeries niet met naam en toenaam in het advies genoemd worden zodat niet kan worden afgeleid welke resultaten van welk ministerie afkomstig zijn.

In de volgende stappen wordt uitgelegd hoe het advies tot stand moet komen.

1. Als eerste moet er bepaald worden wat de ministeries als geheel doen tegen Social Engineering om zo onderzoeksvraag 2.1 te beantwoorden. Dit betekent dat de verschillende onderdelen die onder één ministerie vallen met elkaar vergeleken moeten worden. Door de resultaten per interviewvraag tussen verschillende onderdelen met elkaar te vergelijken kunnen overeenkomsten en verschillen tussen de onderdelen bepaald worden. De overeenkomsten tussen de verschillende onderdelen zijn representatief voor het ministerie als geheel en kunnen gebruikt worden om uitspraken te doen over het ministerie zelf.

2. In stap 2 worden de resultaten van de verschillende ministeries uit stap 1 per interviewvraag met elkaar vergeleken. Hierbij worden de overeenkomsten tussen de verschillende ministeries met elkaar bepaald om zo uitspraken te kunnen over de gehele overheid.

3. De resultaten uit stap 2 worden vergeleken met de begripsbepaling en het conceptuele framework om hieruit tekortkomingen te bepalen en zo een algemeen advies te vormen.

De informatie verkregen uit de verschillende interviews zal behandeld worden zoals beschreven in paragraaf 4.1.6.

Eindscriptie en presentatie
De tussenresultaten en eindresultaten van dit onderzoek zullen verwerkt worden in de eindscriptie. Over het onderzoek zal een presentatie gehouden worden met daarin onze belangrijkste bevindingen. Voor informatie over geheimhouding van in de scriptie aanwezig informatie wordt verwezen naar 4.1.6.

4.1.6 Representativiteit van informatie

Begripsbepaling
De begripsbepaling is gebaseerd op de reeds aanwezige wetenschappelijke literatuur aanwezig over het onderwerp Social Engineering. Van deze literatuur mag worden aangenomen dat deze representatief is.

Conceptueel framework
Het conceptueel framework is gebaseerd op de begripsbepaling welke gebaseerd is op bestaande wetenschappelijke literatuur. Hieruit volgt dat termen gebruikt in het framework consistent zijn doordat zij wetenschappelijk zijn onderbouwd.

Interview resultaten
Omdat er per ministerie maar een beperkt aantal mensen geïnterviewd kan worden is het de vraag of de informatie die hieruit naar voren komt representatief is voor het gehele ministerie.

Het streven is om interviews te houden met mensen die te maken hebben met de concrete invulling van het op hoog niveau opgestelde informatiebeveiliging beleid. Daarom wordt er in dit onderzoek vanuit gegaan dat de geïnterviewde personen op de hoogte zijn van alle zaken omtrent informatiebeveiliging. In de interviews wordt bij bepaalde vragen om de mening van de geïnterviewde(n) gevraagd. Omdat de wijze waarop zij tegen het onderwerp aan kijken bepalend zal zijn bij de ontwikkeling of uitvoering van het beleid wordt dit beschouwd als geldend voor het ministerie of onderdeel daarvan.

4.1.7 Geheimhouding en publicatie van informatie

Omdat de informatie verkregen bij de verschillende ministeries gevoelig van aard kan zijn is in bijlage I aangegeven hoe er in dit onderzoek wordt omgegaan met gevoelige informatie.

4.2 Resultaten

- Een begripsbepaling van Social Engineering
- Conceptueel framework
- Interviewverslag(en) (alleen beschikbaar voor onderzoekers)
- Algemeen advies aan ministeries
- Scriptie met resultaten van het onderzoek.

4.3 Aannames en uitgangspunten

Om te komen tot een succesvol eindresultaat dienen er vooraf aannames en uitgangspunten opgesteld te worden.

- Medewerkers van de verschillende ministeries zijn bereid mee te werken aan het onderzoek in de vorm van het geven van interviews.
- De gehanteerde methode in de vorm van literatuurstudie en interviews levert voldoende informatie op om te komen tot een overzichtelijk conceptueel framework.
- Er is een gedocumenteerd beleid omtrent informatiebeveiliging bij de verschillende ministeries aanwezig.
- Er zijn minimaal drie ministeries bereid mee te werken aan het onderzoek
- Per ministeries kan er minimaal één interview afgenomen worden

4.4 Taakverdeling

In de hier onderstaande tabel staat de taakverdeling globaal weergegeven. De taken die zowel bij de kolom "Arjan" als bij de kolom "Robert" afzonderlijk zijn aangekruist houden in dat ieder apart aan een taak werkt maar dat deze taak meerdere producten oplevert. Zo bestaat de taak "Plan van Aanpak opstellen" uit verschillende producten die door ieder apart worden opgesteld. Het brainstormen over de inhoud en opzet van het framework is een voorbeeld van een taak waar gezamenlijk aan wordt gewerkt.

Taak	Arjan	Robert	Arjan en Robert
Plan van Aanpak			
• Opstellen	X	X	
• Bijstellen		X	
Literatuuronderzoek			
• Verzamelen relevante literatuur	X	X	
• Opstellen bruikbare definitie Social Engineering		X	
• Vaststellen doelen Social Engineering		X	
• Vaststellen Social Engineering aanvallen en kenmerken	X		
• Vaststellen overige factoren Social Engineering	X		

Framework			
• Brainstormen inhoud framework			X
• Brainstormen opzet framework			X
• Opstellen prototype modellen	X	X	
• Evalueren prototype modellen			X
• Opstellen definitieve modellen		X	
• Beschrijven framework	X	X	
Interviews bij Overheid			
• Acquisitie ministeries	X	X	
• Voeren oriënterende gesprekken	X	X	
• Opstellen geheimhoudingsclausule	X		
• Opstellen interviews			X
• Afnemen interviews	X	X	
• Uitwerken interviews	X	X	
• Analyse interview resultaten			
o Per onderdeel van ministerie	X	X	
o Tussen ministeries			X
• Vergelijking resultaten met begripsbepaling	X		
• Vergelijking resultaten interviews met framework		X	
• Opstellen advies			X
Scriptie			
• Beantwoording hoofdonderzoeksvragen	X	X	
• Opstellen conclusies			X
• Opstellen aanbevelingen			X
• Opstellen reflectie onderzoek	X	X	
• “Fine tunen” van scriptie	X	X	
• Reviewen scriptie			X
Presentatie			
• Opstellen presentatie			X
• Houden van presentatie			X

5 Contactpersonen

Naam: Arjan Kieskamp
Organisatie: Radboud Universiteit
Functie: Student
Telefoonnr.: 06-26030890
E-mail: a.a.kieskamp@student.ru.nl
Relatie: Onderzoeker

Naam: Robert Smit
Organisatie: Radboud Universiteit
Functie: Student
Telefoonnr.: 06-24537481
E-mail: crsmit@student.ru.nl
Relatie: Onderzoeker

Naam: Wolter Pieters
Organisatie: Radboud Universiteit
Functie: Junior onderzoeker
Telefoonnr.: +31 24 3652599
E-mail: w.pieters@cs.ru.nl
Relatie: Supervisor

Naam: Martijn Oostdijk
Organisatie: Radboud Universiteit
Functie: Assistent Professor
Telefoonnr.: +31 24 3652713
E-mail: martijno@cs.ru.nl
Relatie: Supervisor

6 Literatuurlijst

6.1 Internet

[1]: Redactie security.nl, http://www.security.nl/article/10266/1/Mitnick%3A_Betere_security_draait_niet_om_technologie.html
[2]: Redactie Security.nl http://www.security.nl/article/12217/1/Social_engineering_meest_onderschatte_dreiging.html
[3]: Dekker, P., Vertrouwen in de Overheid. Een verkenning van actuele literatuur en enquêtes, Augustus 2001 http://www.tilburguniversity.nl/globus/publications/01.03.pdf

6.2 Boeken

Oost H. & Markenhof A., Een onderzoek voorbereiden, HB uitgevers, 2002

Oost H. Een onderzoek uitvoeren, HB uitgevers, 2002

Hulshof M., Leren Interviewen, Wolters Noordhoff, 2001

7 Bijlagen

7.1 Bijlage I Geheimhouding en publicatie van gevoelige informatie

7.1.1 Over deze bijlage

Informatie van het type *bijzonder* of *gevoelig*[2] dat verkregen wordt bij de verschillende overheidsinstellingen in geschreven of digitale vorm, zal gedurende en na afronding van dit onderzoek zorgvuldig worden behandeld. De mogelijkheid tot misbruik van deze informatie door derden wordt hiermee voorkomen. In deze bijlage zal uiteen worden gezet hoe aan de waarborging van de geheimhouding van deze informatie invulling wordt gegeven. Er zal een onderverdeling gemaakt worden naar de wijze waarop bijzondere of gevoelige informatie wordt opgeslagen en verschillende mogelijkheden waarop bepaalde onderzoeksresultaten zullen worden gepubliceerd.

7.1.1.1 Vervoer schriftelijk materiaal

Vervoer van geschreven informatie van het type bijzonder of gevoelig zal zo veel mogelijk worden vermeden. Indien deze situatie zich toch voordoet dan zal het materiaal in een afgesloten tas met de grootste zorgvuldigheid worden vervoerd.

7.1.1.2 Vervoer digitaal materiaal

Informatie van het type bijzonder of gevoelig kan in digitale vorm op verschillende manieren worden vervoerd. In geval van een geheugendrager met directe toegang als USB-stick, floppy disk, Compact Disk, etc. zal informatie versleuteld worden opgeslagen met een algemeen bekend en geaccepteerd algoritme. (zie paragraaf opslag digitaal materiaal). In geval het van vervoer van informatie van het type bijzonder of gevoelig op een laptop zullen hiervoor de nodige voorzorgsmaatregelen worden getroffen (zie paragraaf opslag digitaal materiaal).

7.1.1.3 Opslag digitaal materiaal

Gedurende dit afstudeerproject wordt slechts gebruikt gemaakt van 2 laptops die beide zijn voorzien van een beveiligde bios, beveiligde hardeschijf, beveiligd Windows XP besturingssysteem voorzien van de laatste updates en anti virus / spyware. Daarnaast wordt er gebruik gemaakt van een beveiligde Linux server met slechts toegang voor de

[2] Met bijzondere of gevoelige informatie wordt verwezen naar niet-publieke informatie waarvan het uitlekken ervan in meer of mindere mate nadelige gevolgen kan hebben voor de overheid of overheidsinstelling.

onderzoekers van dit onderzoek, waarop informatie van het type bijzonder of gevoelig versleuteld kan worden opgeslagen.
De toegang tot informatie van elk type op de hardeschijf van de laptop is altijd beveiligd met een sterk wachtwoord, zelfs bij verwijdering van de hardeschijf is deze informatie niet toegankelijk. Informatie van het type bijzonder of gevoelig zal slechts onversleuteld op de hardeschijf bestaan als daar een reden voor is. Materiaal op harddisk of ander medium dat bijzondere of gevoelige informatie bevat zal slechts worden opgeslagen door het te versleutelen met een algemeen bekend en geaccepteerd algoritme in combinatie met een voldoende lange willekeurige sleutel. Deze sleutel zal worden opgeslagen in een met sterk wachtwoord beveiligd bestand op de hardeschijf.

7.1.1.4 Opslag schriftelijk materiaal

De opslag van geschreven informatie van het type bijzonder of gevoelig zal zoveel mogelijk worden beperkt. Materiaal dat niet nodig is voor onbepaalde tijd zal worden vernietigd (zoals aangegeven in paragraaf vernietiging schriftelijk materiaal). Informatie van het type bijzonder of gevoelig dat met reden bewaard moet blijven voor een bepaalde tijd zal zorgvuldig worden opgeslagen (lees buiten handbereik opgeborgen) in de werkkamer van de onderzoekers op de Radboud Universiteit. De werkkamer is slechts toegankelijk voor beide onderzoekers. Overige individuen hebben slechts toegang tot de werkkamer op uitnodiging van en bij aanwezigheid van minimaal een van de onderzoekers.

7.1.1.5 Vernietiging schriftelijk materiaal

Informatie van het type bijzonder of gevoelig zal worden vernietigd in geval er geen reden tot voortdurende opslag is. Het materiaal zal worden vernietigd door gebruik te maken van een papiervernietiger die het materiaal dusdanig vernietigd dat herstel praktisch gezien onmogelijk is. Bij kleinschalige vernietiging of herkenbaarheid wordt er gebruik gemaakt van het toevoegen van vergelijkbaar random dummy materiaal en een verspreide afvoer van het afval.

7.1.1.6 Vernietiging digitaal materiaal

Informatie van het type bijzonder of gevoelig zal slechts onversleuteld op de hardeschijf bestaan als daar een reden voor is. Deze informatie zal worden vernietigd in geval er geen reden tot voortdurende opslag is. Permanente verwijdering zal ervoor zorgen dat het niet in verkeerde handen kan vallen. Ondanks dat bijzondere of gevoelige gegevens versleuteld worden opgeslagen zal in geval van goedkope verwijderbare media deze dusdanig vernietigd worden dat hergebruik onmogelijk is. In geval van bijvoorbeeld een USB-stick kan er een methode gebruikt worden om het geheugen vol te schrijven waardoor sporen worden verwijderd.

7.1.2 Publicatie

7.1.2.1 Non-publieke informatie

Non-publieke documentatie / informatie die wordt ontvangen van de verschillende overheidsinstellingen zal slechts in bezit blijven van beide onderzoekers en op geen enkele wijze worden verspreid aan derden, zelfs als deze derde een andere overheidsinstelling betreft. De vragende overheidsinstelling zal worden doorverwezen naar de overheidsinstelling die de documentatie heeft verstrekt.

7.1.2.2 Non-publieke informatie en Afstudeerbegeleiders

Indien het wenselijk is in het belang van het onderzoek om non-publieke informatie te gebruiken in een overleg met beide afstudeerbegeleiders zal hiervoor eerst toestemming worden gevraagd bij de desbetreffende overheidsinstelling. Dan en slechts dan zal na goedkeuring een specifiek deel non-publieke informatie worden overlegd.

7.1.2.3 Publicatie resultaten

Elke overheidsinstelling krijgt een week de tijd om goedkeuring te geven of om mogelijke problemen aan te geven voordat een rapportage in de vorm van een thesis, abstract of presentatie zal worden gepubliceerd. Hierbij zal onderscheid worden gemaakt naar:

Openbare versie

Een publicatie met onderzoeksresultaten die openbaar toegankelijk is, dit kan eventueel een gecensureerde versie zijn van een vertrouwelijke versie. Er zal nimmer met naam en toenaam naar een overheidsinstelling worden verwezen, wel kan er in een bepaalde situatie gesproken worden over een specifieke overheidstelling als X, Y of Z. Hieruit zal vervolgens op geen enkele wijze afleidbaar zijn over welke overheidsinstelling in deze situatie wordt gesproken. (Afstudeer scriptie / abstract)

Vertrouwelijke versie

Onderzoekers en overheidsinstellingen

- *Vertrouwelijk per overheidsinstelling*
  De gepubliceerde rapportage zal zodanig worden opgesteld dat de resultaten niet herleidbaar zijn naar een specifieke overheidsinstelling. Wel kan er in een bepaalde situatie gesproken worden over een bepaalde overheidstelling als X, Y of Z. Specifieke informatie over de desbetreffende overheidsinstelling wordt in deze publicatie wel vermeld. (Verslag interviews)

- *Vertrouwelijk onder de meewerkende overheidsinstellingen*

> De gepubliceerde rapportage is vertrouwelijk onder de meewerkende overheidsinstellingen. De overheidsinstellingen hebben onderling geen geheimen voor elkaar. (Advies ministeries)

Universiteit

Per hierboven genoemde twee punten kan onderscheid gemaakt worden of de beide afstudeerbegeleiders en eventueel een derde onafhankelijke lezer toestemming krijgen om de desbetreffende publicatie in zien. Hierover zal overleg gepleegd worden met de desbetreffende overheidsinstelling(en). Indien er geen toestemming verleend wordt bestaat er de mogelijkheid om censuur toe te passen waarna een nieuw verzoek tot leesrecht voor afstudeerbegeleiders en derde onafhankelijke lezer zal worden ingediend. (Beoordeling afstudeerscriptie door Universiteit)