Facebook Privacy

Radboud Universiteit Nijmegen
Bachelorscriptie

Naam: Bas Visser
Studentnummer: s0815004
Opleiding: Informatica
Vakcode: IBI009 (9ec)
Begeleiders: Luca Consoli & Theo van der Weide

December, 2011

Abstract

Sociale media zijn in opkomst en zijn een actueel onderwerp. Maar deze opkomst brengt ook gevaren met zich mee. Er zijn meerdere berichten van sociale media gebruikers die door verkeerde privacy instellingen tegen grote problemen aan zijn gelopen. Zo was er in 2011([9]) een Duitse Facebook gebruiker die per ongeluk de privacy instelling van haar verjaardag uitnodiging via Facebook op public heeft gezet in plaats van private. Hierdoor zijn meer dan 1500 personen op haar verjaardag afgekomen en moest er politie aan te pas komen om het feest goed te laten verlopen. Dit is een redelijk onschuldig voorbeeld van de gevolgen van het verkeerd omgaan met de privacy in sociale media, maar de gevolgen kunnen soms erger zijn.

De vraag die gesteld moet worden is: Wordt de privacy van al die gebruikers nog wel gewaarborgd? Dit is een belangrijke vraag waar meer onderzoek naar gedaan moet worden. Daarom wil ik in deze studie aandacht besteden aan deze vraag. Onderzoek doen naar alle sociale media gebruikers van alle soorten sociale media zou te breed zijn. Daarom zal dit onderzoek zich beperken tot de sociale media website Facebook en daarvan alleen de Nederlandse studenten als Facebook gebruikers.

Contents

1 Probleemstelling

De onderzoeksvraag is:

Hoe is de beveiliging van Facebook opgebouwd en hoe gaat de Facebook gebruiker om met de verantwoordelijkheid om hierin een rol te spelen en zijn eigen beveiliging te waarborgen?

Het antwoord op deze onderzoeksvraag zal een indicatie geven in hoeverre de Facebook gebruiker op de hoogte is van zijn eigen bijdrage in zijn beveiliging en hoe de Facebook gebruiker hier mee om gaat.

Het onderzoek bestaat uit een aantal onderdelen. Eerst zal worden gekeken hoe de beveiliging van Facebook in elkaar zit door te kijken naar de verschillende privacy instellingen. Ook zal er een analyse worden gemaakt van de structuur achter Facebook. Aan de hand van deze analyse van Facebook zal de beveiligingsstructuur bepaald kunnen worden. Vervolgens zal door middel van een enquête onderzocht worden of de gemiddelde Facebook gebruiker op de hoogte is van zijn rol in de beveiliging van Facebook. Als laatste zal gezocht worden naar oplossingen om de Facebook gebruiker beter op de hoogte te brengen van zijn rol in de beveiliging, en er zal gezocht worden naar een aanpassing in het beveiligingsmodel van Facebook die de persoonlijke gegevens van gebruikers beter kan beschermen.

2 Verantwoording

2.1 Maatschappelijke relevantie

Steeds meer mensen maken tegenwoordig gebruik van sociale media, dus het is een actueel onderwerp. Maar de groei van sociale media brengt ook een risico met zich mee. Veel persoonlijke gegevens worden vrijgegeven via deze sociale media en dit kan in verkeerde handen vallen. Daarom is het belangrijk dat er onderzoek gedaan wordt naar de beveiliging van sociale media en hoe de gebruikers om gaan met de eigen bijdrage in deze beveiliging. Verder zal onderzoek worden gedaan naar de mogelijkheden om de beveiligingsstructuur van Facebook te verbeteren. Ook zal worden onderzocht of verbetering van de communicatie richting de Facebook gebruikers over hun rol in de beveiliging, een oplossing kan bieden voor het beter waarborgen van de privacy van de Facebook gebruikers.

2.2 Persoonlijke relevantie

Zelf ben ik ook genteresseerd in dit onderwerp omdat ik zou willen weten welke beveiligingsstructuur Facebook gebruikt. Ook heb ik gelezen dat er vaak wat mis gaat bij de bescherming van persoonlijke informatie, waardoor deze informatie in de verkeerde handen terecht komt. Daarom zou ik ook willen weten in hoeverre de Facebook gebruiker op de hoogte is van zijn rol in de beveiliging en hoe de Facebook gebruiker hier mee om gaat. En wat Facebook doet om de privacy van haar gebruikers te beschermen.

3 Theoretisch kader

3.1 Kennisgebieden

Het kennisgebied van dit onderzoek is een combinatie van Informatica en Informatiekunde. Het onderzoek naar de beveiligingsstructuur van Facebook zal Informatica kennisgebieden raken en het onderzoek naar het gedrag en de kennis van de Facebook gebruikers zal Informatiekunde kennisgebieden raken.

3.2 Voorgaande onderzoeken

Harvey Jones en Jos Hiram Soltren hebben een onderzoek ([3]) gedaan naar de privacy op Facebook en hebben in dit onderzoek drie belangrijke dingen geconcludeerd. Ten eerste, de gebruikers van Facebook geven teveel persoonlijke informatie prijs en zijn zelf vaak niet op de hoogte van het feit dat ze zoveel informatie prijsgeven. Ten tweede, Facebook doet niet genoeg om de privacy van hun gebruikers te beschermen. Ten derde, derde partijen zijn actief op zoek naar de persoonlijke informatie van Facebook gebruikers.

Verder zijn er nog twee belangrijke papers ([1,2]) van Gross en Acquisti waarin beschreven wordt hoe Facebook gebruikers zich gedragen, hoe Facebook gebruikers omgaan met hun privacy en hoeveel persoonlijke informatie Facebook gebruikers prijsgeven. Een belangrijke conclusie in het onderzoek ([1,2]) van Gross en Acquisti is dat maar zeer weinig Facebook gebruikers gebruik maken van de privacy settings om hun persoonlijke informatie af te sluiten van ongewenste derde partijen.

Het onderzoek ([3]) van Jones en Soltren zal ik gebruiken als basis voor het theoretisch kader van mijn onderzoek. Jones en Soltren hebben dit onderzoek ([3]) gedaan in 2005 en hebben hun experimenten voornamelijk geconcentreerd op het Facebook gedrag van MIT studenten. In mijn onderzoek wil ik het onderzoeksgebied uitbreiden naar andere Facebook gebruikers. Verder wil ik onderzoeken of de resultaten die Jones en Soltren in 2005 verkregen nog steeds toepasbaar zijn in het heden, of dat Facebook gebruikers tegenwoordig toch op een veiligere manier omgaan met hun persoonlijke gegevens.

Er zijn een aantal duidelijke verschillen tussen dit onderzoek en voorgaande onderzoeken. Ten eerste zijn de voorgaande onderzoeken jaren geleden uitgevoerd. Aangezien Facebook zeer dynamisch is en constant updates krijgt zal er in de tussentijd veel veranderd zijn. Ik zal met dit onderzoek kunnen bepalen of de conclusies die jaren geleden zijn getrokken in voorgaande onderzoeken nog steeds gelden. Ten tweede is er een duidelijk verschil in de focus die Jones en Soltren in hun onderzoek leggen op het Facebook gedrag van de MIT studenten. Dit onderzoek zal de focus leggen op het Facebook gedrag van Nederlandse universitaire studenten. Door de resultaten van de enquête te verwerken en te filteren via een enquêtevraag over opleidingsniveau kan deze focus worden bereikt. Hierdoor

kan ook een vergelijking worden gemaakt tussen Nederlandse en Amerikaanse universitaire studenten wat betreft het Facebook gedrag.

4 Theorie & Definities

"App"

Facebook geeft de volgende definitie van een app:

What is an app on Facebook?

Apps on Facebook are designed to enhance your experience on the site with engaging games and useful features like Events and Photos. Some apps are built by Facebook developers, but most are built by outside developers who use Facebook's APIs and abide by Facebook's Developer Principle and Policies.

Een app is dus een soort plug-in op Facebook paginas waarin gebruikers bijvoorbeeld spelletjes kunnen spelen. Deze apps worden zowel gemaakt door Facebook zelf als door ontwikkelaars van buitenaf. Een belangrijk aspect van apps voor dit onderzoek is dat bij het opstarten van de apps vaak gevraagd wordt om toegang te verlenen tot je persoonlijke gegevens ten behoeve van de app. Zo kan men bijvoorbeeld prestaties in een spel app delen met vrienden via de Facebook pagina.

"Phishing"

Phishing is een vorm van internetfraude waarbij een kwaadwillende partij een vertrouwde partij imiteert. Het doel is om de internet gebruiker zijn persoonlijke gegevens zoals gebruikersnaam en wachtwoord te laten versturen naar de kwaadwillende partij. Vervolgens zal de kwaadwillende partij deze gegevens gebruiken om de internet gebruiker schade aan te doen. Zo kan bijvoorbeeld de bankrekening van de internet gebruiker leeggehaald worden als de bankgegevens via phishing bij de kwaadwillende partij terecht zijn gekomen.

5 Methode

5.1 Onderzoeksfunctie

Het onderzoek bestaat uit een aantal onderzoeksfuncties. Het eerste deel van het onderzoek is een beschrijvend onderzoek, waarin de opbouw van de beveiliging van Facebook in kaart gebracht wordt. Zowel de rol die Facebook zelf speelt, als de rol die de Facebook gebruikers dienen te spelen in de beveiliging.

Vervolgens zal het onderzoek een verklarend en evaluerend onderdeel bevatten, waarin onderzocht wordt of de Facebook gebruiker voldoende op de hoogte is van zijn rol in zijn beveiliging en of de Facebook gebruiker ook daadwerkelijk gebruik maakt van de beveiligingsinstellingen op Facebook.

Als laatste zal het onderzoek een ontwerpend onderdeel bevatten, waarin onderzocht wordt wat er gedaan kan worden om de Facebook gebruiker beter op de hoogte te brengen van zijn rol in de waarborging van zijn privacy. Daarnaast wordt er onderzocht hoe Facebook haar beveiligingsmodel kan aanpassen, zodat Facebook gebruikers beter beschermd kunnen worden tegen derde partijen die hun persoonlijke informatie in handen willen krijgen.

5.2 Deelvragen

Deelvragen voor dit onderzoek zijn:

1. *Hoe is de beveiliging van Facebook opgebouwd?*
2. *Welke rol dient een Facebook gebruiker te spelen in het waarborgen van zijn eigen beveiliging?*
3. *Is de Facebook gebruiker op de hoogte van de verantwoordelijkheid om een rol te spelen in het waarborgen van zijn eigen beveiliging?*
4. *Wat kan er gedaan worden om de Facebook gebruiker beter op de hoogte te brengen van zijn rol in de waarborging van zijn privacy?*
5. *Hoe kan Facebook haar beveiligingsmodel aanpassen zodat Facebook gebruikers beschermd worden tegen derde partijen die hun persoonlijke informatie in handen willen krijgen?*

Voor het beantwoorden van deelvraag 1 zal de informatiestroom achter Facebook geanalyseerd worden. Op basis van de analyse van de informatiestroom achter Facebook zal dan de beveiligingsstructuur van Facebook worden bepaald.

Voor het beantwoorden van deelvraag 2 zal de website van Facebook geanalyseerd worden en de verschillende privacy instellingen zullen worden weergegeven. Hiermee zal bepaald kunnen worden welke rol de gebruiker dient te spelen in de privacy van Facebook.

Voor het beantwoorden van deelvraag 3 zal er een enquête worden uitgevoerd om te meten in hoeverre Facebook gebruikers op de hoogte zijn van hun rol in de beveiliging van Facebook en in hoeverre ze ook daadwerkelijk gebruik maken van de beveiligingsfuncties op Facebook.

Voor het beantwoorden van deelvragen 4 en 5 zal ten eerste gebruik worden gemaakt van de enquête. In de enquête zal met een aantal beoordelingsvragen en een aantal open vragen gevraagd worden naar de mening over de bescherming van de persoonlijke gegevens. De respondenten worden gevraagd naar tevredenheid over de bescherming van hun persoonlijke gegevens en naar het vertrouwen dat zij hebben in Facebook om zorgvuldig met hun persoonlijke gegevens om te gaan. Daarnaast zal door middel van de open vragen gevraagd worden naar suggesties voor verbetering van zowel het op de hoogte brengen van de gebruikers als de bescherming van de persoonlijke gegevens. Ten tweede zullen er verbeteringen worden bedacht aan de hand van voorgaande onderzoeken en eigen inzicht door het bestuderen van de beveiligingsstructuur van Facebook.

De doelgroep van de enquête zijn studenten aan Nederlandse universiteiten. Bij de analyse van de enquête zullen de resultaten hierop worden gefilterd. Er waren volgens het CBS([6]) 241.686 studenten aan universiteiten in Nederland in 2010/2011. Vervolgens wordt de steekproefgrootte bepaald met de volgende statistische formule:

$$SG = \frac{(P * z^2 * p(1-p))}{(z^2 * p(1-p) + (P-1) * (F^2))}$$

Waarin:
SG = steekproefgrootte
P = populatiegrootte
z = standaardafwijking (normaal 1.96 voor een betrouwbaarheid van 95%)
p = kans op een bepaald antwoord (normaal 0.5 als dit niet te bepalen is)
F = foutmarge

Als in deze formule de populatiegrootte van het CBS wordt ingevuld en een foutmarge van 10% wordt het:

$$SG = \frac{(241.686 * 1.96^2 * 0.5(1-0.5))}{(1.96^2 * 0.5(1-0.5) + (241.686-1) * (0.10^2))}$$

Hieruit volgt SG = 96,002 Er zijn dus minstens 96 deelnemers nodig om een foutmarge van 10% te behalen. Als het uiteindelijke aantal deelnemers lager ligt zal de foutmarge moeten worden aangepast. De enquête zal worden verspreid door middel van email, via mailing lijsten van de universiteit zal een email worden verstuurd naar ongeveer 200 studenten. In die email zal niet alleen worden

gevraagd om de online enquête in te vullen maar ook om de email door te sturen naar andere studenten. Door middel van deze zogenaamde snowballing techniek zullen er niet alleen meer respondenten zijn, maar ook een grotere spreiding in de doelgroep. Studenten die de eerste email reeks krijgen zullen deze email doorsturen naar studenten van andere faculteiten en andere universiteiten.

Data analyse

Bij de analyse van de enquête zal er eerst een filtering plaatsvinden van de onbruikbare deelnames. De deelnames van niet-universitaire studenten zullen worden gefilterd door een enquêtevraag naar het opleidingsniveau van de respondent. Verder zullen deelnames gefilterd worden waarin is ingevuld dat de deelnemer geen gebruik maakt van Facebook, door middel van een enquêtevraag over het gebruik van Facebook. De overgebleven deelnames zullen vervolgens worden geanalyseerd en uit deze deelnames zullen conclusies worden getrokken over de deelvragen in het onderzoek.

6 Deelvraag 1: Hoe is de beveiliging van Facebook opgebouwd?

6.1 Facebook architectuur

In 2009 heeft Aditya Agarwal, de Engineering Director van Facebook, een presentatie ([5]) gegeven over de structuur van Facebook. Facebook bestaat uit een aantal belangrijke software onderdelen: LAMP, Memcache, Thrift en Scribe.

LAMP

LAMP staat voor Linux, Apache, MySQL en PHP. Deze vier software onderdelen vormen samen de basis van de Facebook webserver. Linux is het besturingssysteem van de webservers en is de link tussen de hardware en de applicaties die draaien op deze webservers. Apache is de webserver software die http-requests van de client verwerkt. MySQL en PHP draaien op de Apache webserver software. MySQL zorgt voor de interactie met de database en PHP is de programmeertaal waarmee dynamische websites gegenereerd kunnen worden.

Memcache

Memcache is een memory caching systeem dat is bedoeld om dynamische websites met databases sneller in gebruik te maken. Het zorgt ervoor dat gegevens die de client uit de database opvraagt lokaal worden opgeslagen. Als de client later dezelfde gegevens nodig heeft, kunnen deze gegevens via Memcache uit het RAM geheugen worden gehaald. Hierdoor hoeft de client niet steeds opnieuw database requests te doen voor dezelfde data. Voor Facebook zal dit ervoor zorgen dat de website sneller draait voor de gebruiker, omdat een deel van de gegevens lokaal kunnen worden opgeslagen.

Thrift

Thrift is een software framework dat verschillende applicaties en programmeertalen met elkaar verbindt. Het zorgt ervoor dat de verschillende onderdelen van de Facebook architectuur op een goede en snelle manier met elkaar samenwerken. Thrift zorgt er bijvoorbeeld voor dat de aggregators van Scribe verbonden worden met de database software, waardoor de gewenste data op een snelle manier gefilterd kan worden.

Scribe

Scribe is aggregator systeem die kan bepalen welke gegevens de client precies nodig heeft en wat de beste manier is om deze gegevens te filteren. Met behulp van een complex filtering systeem kan Scribe server-side bepalen welke gegevens de Facebook gebruiker precies nodig heeft. Hierdoor wordt het aantal gegevens dat wordt verstuurd tussen de gebruiker en de webserver beperkt. Doordat er

minder gegevens worden verstuurd, zal Facebook sneller draaien en de server load zal minder zwaar zijn. Beperking van de server load is erg belangrijk voor een website als Facebook met miljoenen gebruikers.

6.1.1 NewsFeed onderdeel

Steeds meer mensen maken tegenwoordig gebruik van sociale media, dus het is een actueel onderwerp. Maar de groei van sociale media brengt ook een risico met zich mee. Veel persoonlijke gegevens worden vrijgegeven via deze sociale media en dit kan in verkeerde handen vallen. Daarom is het belangrijk dat er onderzoek gedaan wordt naar de beveiliging van sociale media en hoe de gebruikers om gaan met de eigen bijdrage in deze beveiliging. Verder zal onderzoek worden gedaan naar de mogelijkheden om de beveiligingsstructuur van Facebook te verbeteren. Ook zal worden onderzocht of verbetering van de communicatie richting de Facebook gebruikers over hun rol in de beveiliging, een oplossing kan bieden voor het beter waarborgen van de privacy van de Facebook gebruikers.

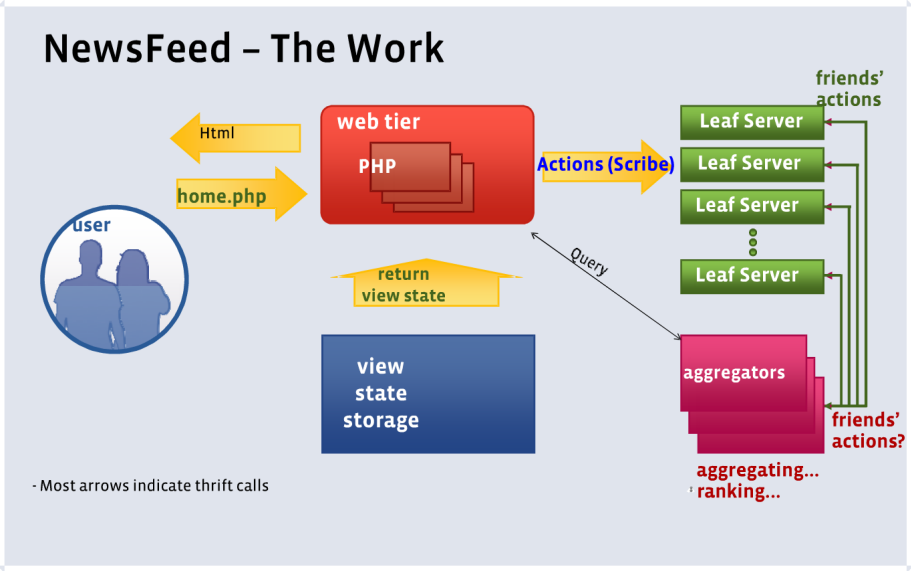

Figure 1: Model uit Agarwal, A., 2008, Facebook: Science and the Social Graph, QCon SF 2008 ([5])

De interactie van de Facebook gebruiker met de NewsFeed vindt plaats via de web tier. De PHP server software genereert de dynamische website voor de NewsFeed via de view state. De acties van de gebruiker op de website worden omgezet in server requests via queries met Scribe. Het Scribe aggregator

systeem zal de gegevens voor de NewsFeed opvragen uit de juiste Leaf Servers waarin de benodigde data zich bevindt. Scribe aggregators zullen vervolgens de data ranken, omdat er maar een beperkt aantal gegevens aan de gebruiker getoond kunnen worden. De data wordt geranked op meest interessante nieuws onderwerpen van vrienden. Daarnaast wordt gekeken of de gebruiker bepaald nieuws al eerder heeft gezien, ook dit wordt gefilterd. Als de Scribe aggregators een ranking hebben gemaakt van de gegevens, worden de overgebleven gegevens teruggestuurd naar de gebruiker. Vervolgens genereert de PHP server software een NewsFeed website gebaseerd op deze gegevens waardoor de gebruiker de gegevens kan zien op zijn Facebook website.

6.2 Facebook Immune System (FIS)

Sommige partijen proberen op verschillende manieren aan persoonlijke gegevens van Facebook gebruikers te komen ([8]). Zo worden bijvoorbeeld valse friend requests verstuurd naar gebruikers in de hoop dat ze deze accepteren. Zodra de gebruiker deze friend requests accepteert, verleent hij de kwaadwillende partij toegang tot alle persoonlijke gegevens die alleen toegankelijk zijn voor vrienden. Ook proberen partijen aan de inlog gegevens van Facebook gebruikers te komen, waardoor ze meteen toegang krijgen tot alle persoonlijke gegevens die de gebruiker op Facebook heeft gezet. Om dit te voorkomen heeft Facebook een speciaal beveiligingssysteem opgezet dat gebruikers moet beschermen tegen phishing, fraude en scams.

Het systeem genaamd Facebook Immune System (FIS, [4]) voert realtime checks uit op alle read en write acties die op Facebook worden uitgevoerd. Dit systeem is gemaakt met een aantal design principles ([4]) als uitgangspunt:

- Het systeem moet aanvallen snel kunnen detecteren en snel op de aanvallen reageren.
- Het systeem moet een breed en ontwikkelend aanvalsvlak kunnen verdedigen.
- Het systeem moet op verschillende onderdelen van Facebook kunnen opereren, bijvoorbeeld chat, NewsFeed en friend requests.
- De classificatie van de checks moet realtime worden uitgevoerd, en synchroon lopen met handelingen van de gebruikers.

Het FIS systeem maakt gebruik van Thrift voor de classificatie modules. In Stein et al ([4]) wordt beschreven hoe het FIS systeem classificeert door middel van figuur 2.

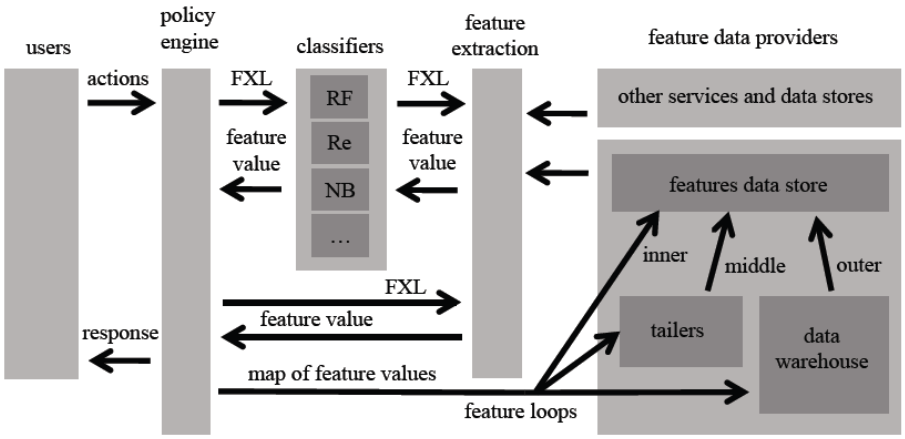

Figure 2: Model uit Stein et al, 2011, "Facebook Immune System" ([4])

De acties van de gebruiker worden door middel van de policy engine geclassificeerd met verschillende classificatie algoritmen zoals Random Forest (RF), Naive Bayes (NB) en Regression (Re). De classificatie wordt door middel van de feature extraction gemapped naar een response. Eerdere aanvallen worden bij de feature extraction herkend via de externe en interne data opslag. Vervolgens wordt via de feature loops de geclassificeerde data opgeslagen zodat de feature extraction de aanval voortaan sneller herkent. Ook wordt er gebruik gemaakt van externe data opslag voor de herkenning van verkeerde acties.

7 Deelvraag 2: Welke rol dient een Facebook gebruiker te spelen in het waarborgen van zijn eigen beveiliging?

7.1 Facebook privacy onderdelen

Facebook heeft een privacy informatie pagina waarin ze zelf beschrijven hoe de privacy op Facebook werkt. Er zijn vier onderdelen op privacy die altijd te zien zijn voor iedereen:

- Profiel foto
- Naam
- Netwerken
- Username / User ID

Daarnaast is de privacy van de volgende onderdelen door de gebruiker in te stellen:

- Foto's
- Status updates
- Comments op andere berichten
- Vrienden toevoegen
- "Like" drukken op een pagina of website
- Relatie status

Facebook heeft een ingebouwde Privacy Settings pagina voor de default privacy instelling, de gebruiker heeft hiervoor de keus uit:

- Public (toegankelijk voor iedereen)
- Friends (alleen voor vrienden)
- Custom (zelf instellen via lijsten wie precies toegang heeft)

Deze default privacy instelling bepaalt de toegang tot de standaard persoonlijke gegevens voor onderdelen die geen eigen privacy keuze hebben. Bijvoorbeeld fotos en status updates moeten individueel worden ingesteld, omdat deze onderdelen een eigen privacy instelling keuze hebben op de aanmaak webpagina.

Privacy instelling mogelijkheden voor deze aparte onderdelen zijn:

- Public (toegankelijk voor iedereen)
- Friends (alleen voor vrienden)
- Only Me (alleen voor de gebruiker zelf)

- Custom (zelf instellen via lijsten wie precies toegang heeft)

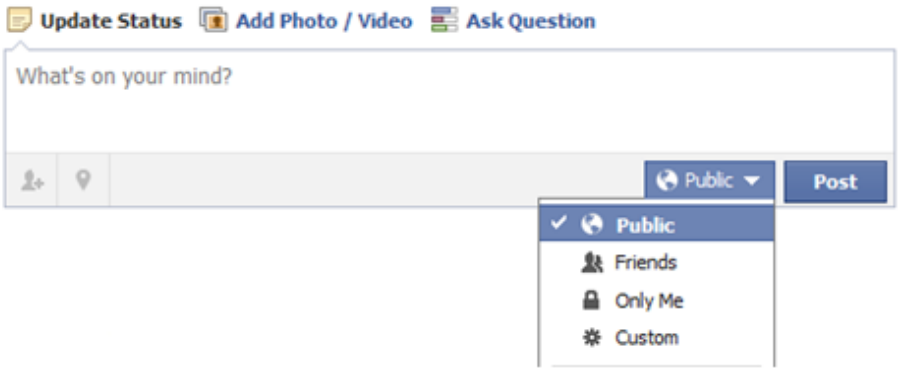

Figure 3: http://www.facebook.com ([7])

De gebruiker kan op Facebook lijsten aanmaken en specifieke personen toevoegen aan deze lijsten. Deze lijsten kunnen dan via de Custom privacy instelling gebruikt worden om de toegang te beperken tot de personen in een bepaalde lijst.

Bij aanmaak van de Facebook account zijn er al een aantal lijsten standaard aangemaakt, bijvoorbeeld Close Friends, Acquaintances en Family. Daarnaast is er ook standaard de Restricted lijst bij aanmaak van een Facebook account. De personen die de gebruiker in de Restricted lijst toevoegt, krijgen geen toegang tot persoonlijke gegevens die de privacy instelling Friends hebben. Met deze lijst kan de gebruiker personen toevoegen als vriend op Facebook, terwijl deze personen toch alleen toegang hebben tot de persoonlijke gegevens die de privacy instelling Public hebben.

7.2 Beantwoording deelvraag

Welke rol dient een Facebook gebruiker te spelen in het waarborgen van zijn eigen beveiliging?

Facebook gebruikers moeten weten wat de eigenschappen zijn van de verschillende privacy instellingen. Als de gebruiker hier niet goed van op de hoogte is, kunnen persoonlijke gegevens bij verkeerde partijen terecht komen. Ten eerste moet de gebruiker de default privacy instelling gebruiken om de toegang te regelen voor alle persoonlijke gegevens die geen eigen privacy keuze hebben. Vervolgens moet de gebruiker weten welke onderdelen op Facebook een eigen privacy keuze hebben, zoals fotos en status updates. De gebruiker moet bij aanmaak van deze onderdelen een aparte privacy instelling geven.

Om de toegang makkelijker te regelen heeft de gebruiker de mogelijkheid om lijsten aan te maken. In deze lijsten kan de gebruiker aparte personen toevoegen en vervolgens de toegang van bepaalde persoonlijke gegevens beperken tot deze personen. Ook kan de gebruiker deze lijsten gebruiken om personen uit te sluiten van toegang tot persoonlijke gegevens die ingesteld zijn op Friends.

8 Deelvraag 3: Is de Facebook gebruiker op de hoogte van de verantwoordelijkheid om een rol te spelen in het waarborgen van zijn eigen beveiliging?

8.1 Enquête

Om een antwoord te geven op deze vraag wordt er gebruik gemaakt van de resultaten van de enquête ([13]).

8.1.1 Filtering enquête

Voordat de enquête representatief is voor de beantwoording van de deelvragen in dit onderzoek moeten eerst de onbruikbare deelnames uit de resultaten gefilterd worden. Totaal hebben 98 deelnemers de enquête ingevuld. Ten eerste zullen de deelnames worden gefilterd waarbij ingevuld is dat de deelnemer geen gebruik maakt van Facebook, omdat deze deelnames geen informatie kunnen bieden over het gebruik van Facebook. In figuur 4 is te zien dat 7 van de 98 deelnames betreft.

Figure 4: Eerste filteringsvraag

Vervolgens zullen alle deelnames worden gefilterd waarbij de deelnemer een opleidingsniveau onder universiteit heeft, omdat de focus van het onderzoek ligt op het Facebook gebruik van universitaire studenten. De conclusie van het onderzoek zal dan ook alleen conclusies trekken over universitaire studenten. In figuur 5 is te zien dat dit 8 van de 98 deelnames betreft.

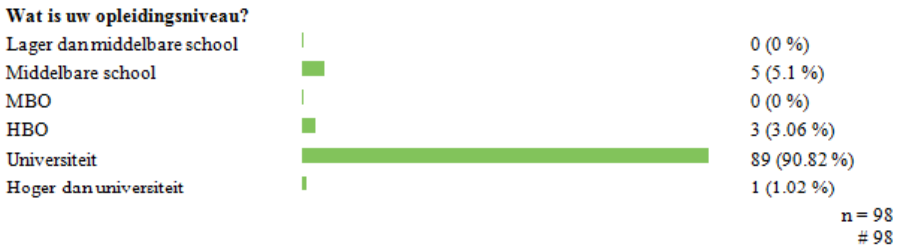

Figure 5: Tweede filteringsvraag

Na filtering van deze deelnames blijven er 84 deelnames over. Deze deelnames zullen worden gebruikt voor de beantwoording van de onderzoeksvragen. Dit aantal ligt onder de benodigde deelnames van 96 voor een foutmarge van 10%. Met de eerder genoemde statistische formule volgt uit een steekproefgrootte van 84 dat de werkelijke foutmarge 10.69% is. Dit is nog steeds een acceptabele foutmarge, dus de enquête blijft ook met 84 deelnames representatief voor het onderzoek.

Ook is het belangrijk dat er een gelijke verdeling is in het geslacht van de respondenten zodat de conclusies die uit de resultaten volgen gelden voor zowel mannelijke als vrouwelijke studenten. In figuur 6 is te zien dat dit inderdaad het geval is. 52% van de respondenten is man en 48% van de respondenten is vrouw, dus vrijwel een gelijke verdeling. Verder is de gemiddelde leeftijd van de respondenten 22 jaar, ook dit komt overeen met de doelgroep universitaire studenten.

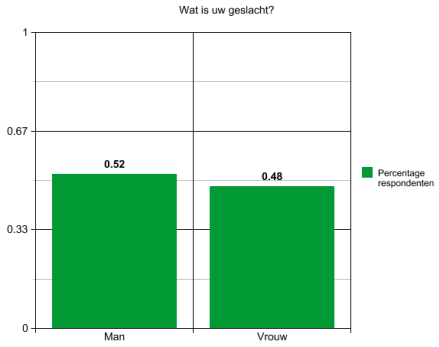

Figure 6: Geslachtsverdeling

8.1.2 Resultaten

De eerste relevante enquêtevraag voor deze deelvraag is: Zou u ooit iemand als vriend op Facebook hebben als u deze persoon nog nooit in het echt heeft ontmoet?. In figuur 7 is te zien dat 67% van de deelnemers aangeeft iemand niet als vriend te hebben als hij/zij deze persoon nog nooit in het echt heeft ontmoet. Dit komt overeen met het onderzoek van Soltren en Jones([3]) in 2005, uitgevoerd op MIT studenten. Zoals te zien is in figuur 8 geeft daarin 63.45% van de respondenten aan dat ze iemand niet als vriend accepteren op Facebook als ze deze persoon nog nooit in het echt hebben ontmoet.

Dit is een interessant resultaat omdat dit aangeeft dat het grootste deel van de studenten waakzaam is bij het toevoegen van vrienden op Facebook en niet zomaar iedereen accepteert als vriend op Facebook. De meeste privacy instellingen zijn gekoppeld aan de vriendschapsstatus op Facebook, bepaalde persoonlijke gegevens zijn alleen zichtbaar voor Facebook vrienden. Dit resultaat zou dus een indicatie kunnen zijn dat het grootste deel van de studenten bewust omgaat met de privacy wat betreft het toegang verlenen tot persoonlijke gegevens aan onbekenden.

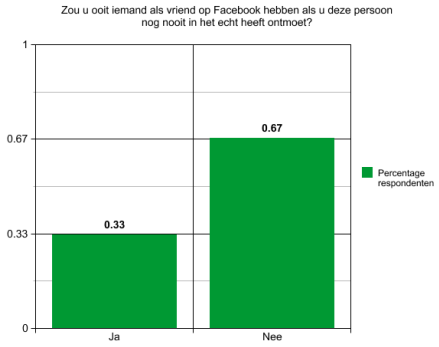

Figure 7: Eerste enquête vraag

Number Allowing Strangers To Friend n=383				
	Number	Percentage	Males	Females
No	243	63.45%	109	129
Yes	30	7.83%	17	12
Sometimes	110	28.72%	44	65

Figure 8: Tabel uit Jones, H., Soltren, J.H., 2005, "Facebook: Threats to Privacy"([3])

De volgende relevante enquêtevraag voor deze deelvraag is: *"Wist u dat Facebook privacy instellingen heeft waarmee u toegang tot bepaalde delen van uw Facebook pagina kunt instellen?"* In figuur 9 is te zien dat 98% van de respondenten aangeeft op de hoogte te zijn van het bestaan van de privacy instellingen op Facebook.

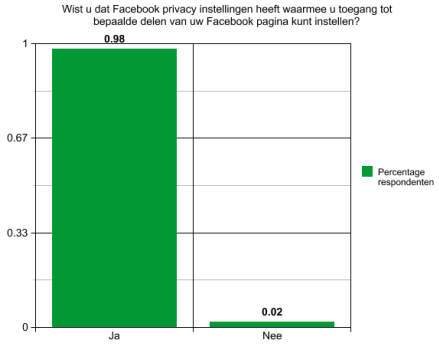

Figure 9: Tweede enquête vraag

De volgende enquêtevraag die hieraan is gerelateerd is: *"Heeft u ooit gebruik gemaakt van de privacy instellingen op Facebook om de toegang tot bepaalde delen van uw Facebook pagina in te stellen?"* In figuur 10 is te zien dat bij deze vraag 92% van de respondenten heeft aangegeven gebruik te maken van de privacy instellingen.

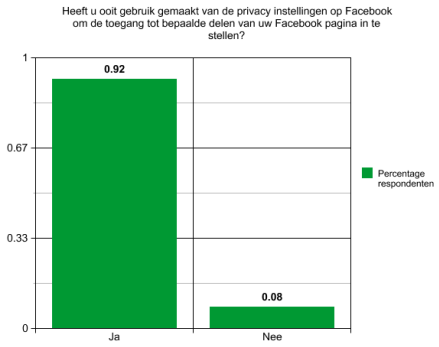

Figure 10: Derde enquête vraag

Facebook and My Privacy: Familiarity and Utilization n=419						
	Number Familiar	Males	Females	Number Using	Males	Females
No Answer	30	15	33	39	18	19
No	100	38	59	234	111	119
Yes	289	133	152	146	57	86

Figure 11: Tabel uit Jones, H., Soltren, J.H., 2005, "Facebook: Threats to Privacy"([3])

In figuur 11 is het resultaat te zien van de enquête die Jones en Soltren([3]) uitvoerden in 2005 op de studenten van MIT. In dit onderzoek werd er op een soortgelijke manier gevraagd naar het op de hoogte zijn van het bestaan van de privacy instellingen op Facebook en het gebruiken van deze privacy instellingen op Facebook. Uit dit onderzoek is gebleken dat 74% van de respondenten op de hoogte was van het bestaan van de privacy instelling op Facebook in 2005 en dat 41% van de respondenten ook daadwerkelijk gebruik maakte van deze privacy instellingen op Facebook in 2005.

Een mogelijke verklaring voor het verschil tussen de resultaten van Jones en Soltren([3]) in 2005 en de resultaten van dit onderzoek in 2011 is dat men in de loop der tijd bewuster omgaat met de privacy op Facebook en meer zorg heeft voor de bescherming van de persoonlijke gegevens. Een andere mogelijke verklaring voor het verschil tussen de resultaten is dat studenten uit de Verenigde Staten minder bewust omgaan met hun privacy op Facebook dan studenten in Nederland. Het is niet met zekerheid te zeggen welke van deze verklaringen de juiste is.

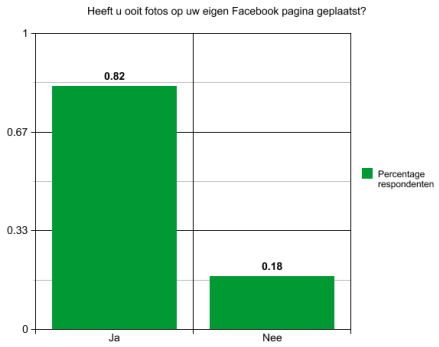

Figure 12: Vierde enquête vraag

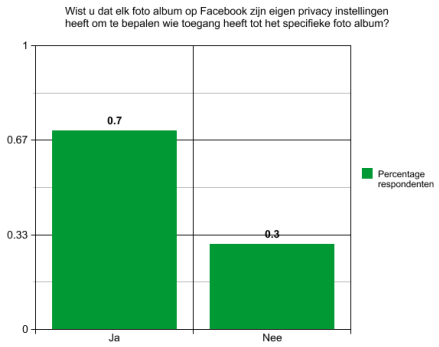

Figure 13: Vijfde enquête vraag

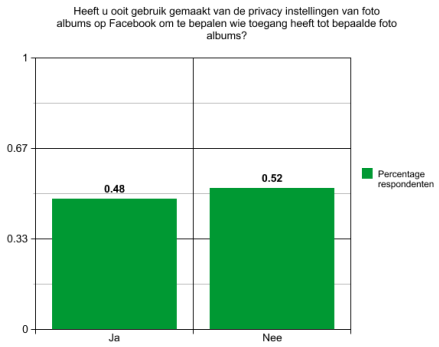

Figure 14: Zesde enquête vraag

Uit de vraag: *"Heeft u ooit fotos op uw eigen Facebook pagina geplaatst?"* volgt dat 82% van de respondenten ooit fotos op zijn/haar eigen Facebook pagina heeft geplaatst, zoals te zien is in figuur 12. Verder volgt uit de vraag: *"Wist u dat elk foto album op Facebook zijn eigen privacy instellingen heeft om te bepalen wie toegang heeft tot het specifieke foto album?"* dat 70% van de respondenten op de hoogte is van het bestaan van privacy instellingen voor elk specifiek foto album, zoals te zien is in figuur 13. Uit de vraag: *"Heeft u ooit gebruik gemaakt van de privacy instellingen van foto albums op Facebook om te bepalen wie toegang heeft tot bepaalde foto albums?"* volgt dat 48% van de respondenten ook daadwerkelijk gebruik heeft gemaakt van de privacy instellingen voor een specifiek foto album, zoals te zien is in figuur 14.

Er blijkt dus een interessant verschil te zijn: 98% van de respondenten is op de hoogte van de algemene privacy instellingen op Facebook, en maar 70% van de respondenten is op de hoogte van de privacy instellingen van elk specifiek foto album op Facebook. In het gebruik van deze privacy instellingen zit een

nog groter verschil: 92% van de respondenten gebruikt de algemene privacy instellingen op Facebook, en maar 48% van de respondenten gebruikt de privacy instellingen van elk specifiek foto album op Facebook. Ondanks dat 82% van de respondenten aangeeft wel gebruik te maken van de mogelijkheid om fotos te plaatsen op Facebook.

Hieruit volgt dat studenten minder op de hoogte zijn van het bestaan van privacy instellingen van elk specifiek foto album dan van het bestaan van de algemene privacy instellingen. Ook volgt hieruit dat ook al zijn 70% van de respondenten op de hoogte van het bestaan van de foto album privacy instellingen, er toch maar 48% van de respondenten gebruik van maakt. Het blijkt dus dat de studenten een stuk minder bewust omgaan met de privacy van hun fotos dan met de privacy van hun Facebook pagina zelf. De studenten hebben dus een stuk minder zorg voor de bescherming van hun fotos dan voor de bescherming van hun algemene persoonlijke gegevens.

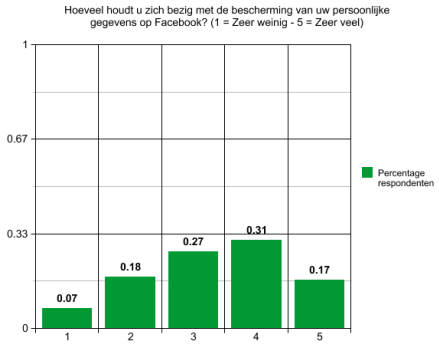

Figure 15: Zevende enquête vraag

De volgende relevante enquêtevraag is: *"Hoeveel houdt u zich bezig met de bescherming van uw persoonlijke gegevens op Facebook?"* In figuur 15 is te zien dat het grootste deel van de respondenten aangeeft zich veel bezig te houden met de bescherming van hun persoonlijke gegevens op Facebook. Ook dit is een indicatie dat de studenten bewust omgaan met de privacy op Facebook en een actieve rol spelen in de bescherming van hun persoonlijke gegevens.

8.2 Beantwoording deelvraag

Is de Facebook gebruiker op de hoogte van de verantwoordelijkheid om een rol te spelen in het waarborgen van zijn eigen beveiliging?

Er zijn een aantal indicaties in de resultaten van de enquête waaruit afgeleid kan worden dat de studenten als Facebook gebruikers grotendeels inderdaad op de hoogte zijn van hun verantwoordelijkheid om een rol te spelen in de bescherming van zijn eigen privacy. 98% van de studenten is op de hoogte van

de algemene privacy instellingen en 70% van de studenten is op de hoogte van de privacy instellingen voor elk specifiek foto album. Daarnaast geeft 67% van de studenten aan dat ze iemand niet als vriend op Facebook accepteren als ze deze persoon niet in het echt kennen. Ook geeft het grootste deel van de studenten aan dat ze zich bewust bezig houden met de bescherming van hun persoonlijke gegevens op Facebook.

Facebook kan waarschijnlijk betere informatie geven over het bestaan van aparte privacy instellingen voor foto albums, omdat hier een stuk minder kennis van is en een stuk minder gebruik van wordt gemaakt. Desondanks is de Nederlandse student over het algemeen goed op de hoogte van zijn verantwoordelijkheid om een rol te spelen in het beschermen van zijn privacy op Facebook. Bovendien maken de meeste studenten veel gebruik van algemene privacy instellingen, zijn ze terughoudend met het toevoegen van personen als vriend op Facebook als ze deze personen niet in het echt kennen en zijn ze over het algemeen veel bezig met de bescherming van hun persoonlijke gegevens op Facebook.

9 Deelvraag 4: Wat kan er gedaan worden om de Facebook gebruiker beter op de hoogte te brengen van zijn rol in de waarborging van zijn privacy?

9.1 Enquête

In de enquête zijn een aantal vragen gesteld over wat Facebook kan doen om de gebruiker beter op de hoogte te brengen van zijn rol in de privacy.

9.1.1 Suggesties van studenten

De studenten hebben als Facebook gebruikers via de volgende vraag suggesties aangedragen over wat Facebook kan verbeteren om de gebruiker beter op de hoogte te brengen van zijn rol in de privacy:

"Wat zou Facebook kunnen doen om haar gebruikers beter op de hoogte te brengen van het bestaan van de privacy instellingen?"

Suggestie:	Aantal keer genoemd:
Meer en betere uitleg / Tutorial of rondleiding op de website bij aanmaak Facebook account	30
Gebruikers dwingen om meteen een privacy keuze te maken zodra er een nieuw onderdeel wordt toegevoegd zoals een foto	3
Ze zijn al goed op weg sinds recente updates / Het is al duidelijk genoeg	2
Duidelijker maken dat Facebook apps toegang tot AL je gegevens vragen en waarschuwen voor de gevolgen hiervan	1

De eerste suggestie die vaak wordt genoemd is dat Facebook betere uitleg moet geven over de privacy instellingen. Facebook kan duidelijker zijn hoe de bepaalde onderdelen van de Facebook pagina apart beschermd kunnen worden. Dit kan bijvoorbeeld door een tutorial of rondleiding op de website bij het aanmaken van een Facebook account.

Op dit moment staat een nieuw toegevoegd onderdeel standaard toegankelijk voor iedereen tenzij de gebruiker dit later anders instelt. Een suggestie is om gebruikers te dwingen om meteen een privacy keuze te maken zodra er een nieuw onderdeel op de Facebook pagina wordt toegevoegd. Als de Facebook gebruiker

dus bijvoorbeeld een foto toevoegt aan zijn pagina zal deze niet standaard toegankelijk zijn, maar de Facebook gebruiker zal worden gevraagd een privacy instelling te kiezen voor deze foto, bijvoorbeeld “alleen voor vrienden”.

Ondanks dat de suggestie minder vaak is genoemd is het toch een belangrijke suggestie dat Facebook duidelijker moet zijn over de toegang van de “apps” op Facebook. Vaak is het zo dat deze app’s meteen toegang vragen tot al je persoonlijke gegevens terwijl ze maar een deel ervan nodig hebben. Facebook moet duidelijker hierover zijn en de gebruikers waarschuwen voor de gevolgen van een app toegang geven tot alle persoonlijke gegevens.

Ook hebben twee studenten genoemd dat Facebook al goed op weg is naar verbetering sinds recente updates en dat het eigenlijk al wel duidelijk is hoe de privacy instellingen werken en waar ze te vinden zijn. Dit komt overeen met de cijfers van het aantal studenten dat op de hoogte is van het bestaan van de privacy instellingen en de cijfers van het gebruik van deze instellingen door studenten. Toch zeggen deze cijfers niks over de rest van de Facebook gebruikers. Het kan zijn dat de andere Facebook gebruikers meer moeite hebben met het gebruiken van de privacy instellingen en wel baat hebben bij meer uitleg hierover.

Ondanks dat een aantal studenten al voldoende op de hoogte zegt te zijn van de privacy instellingen, blijkt dat toch een meerderheid van de studenten zegt wel behoefte te hebben aan meer uitleg hierover. In de enquête is de volgende vraag gesteld: *“Zou u uw persoonlijke gegevens zelf beter kunnen beschermen als Facebook meer uitleg zou geven over de werking van de privacy instellingen?”* In figuur 16 is te zien dat 63% van de studenten zegt zijn gegevens zelf beter te kunnen beschermen als Facebook meer uitleg zou geven over de werking van de privacy instellingen.

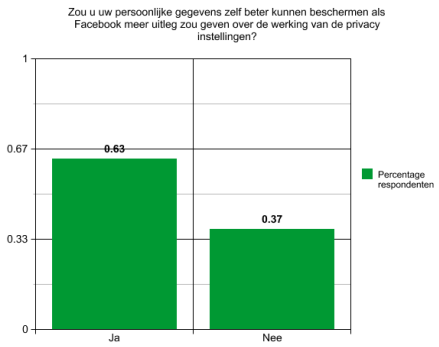

Figure 16: Achtste enquête vraag

9.2 Beantwoording deelvraag

Wat kan er gedaan worden om de Facebook gebruiker beter op de hoogte te brengen van zijn rol in de waarborging van zijn privacy?

De suggestie die het meest is genoemd door de respondenten is meer uitleg vanuit Facebook, bijvoorbeeld door het toevoegen van een tutorial of rondleiding op de website bij aanmaak van de Facebook account. Bij het aanmaken van een Facebook account wordt op dit moment al een korte rondleiding gegeven met instructies, maar er wordt weinig aandacht besteed aan de privacy instellingen bij deze instructies. Facebook kan de rondleiding uitbreiden en meer aandacht besteden aan de privacy onderdelen van Facebook, zodat de gebruiker niet ongewild toegang verleent tot zijn persoonlijke gegevens.

Een andere suggestie die wordt genoemd is om de gebruikers direct te dwingen om een privacy keuze te maken bij aanmaak van een onderdeel. Zo kan de gebruiker bijvoorbeeld meteen gedwongen worden om een keuze te maken voor de default privacy bij aanmaak van de Facebook account. Voor de aparte onderdelen die niet onder de default privacy vallen kan bij elke individuele aanmaak de gebruiker worden gedwongen een keuze te maken voor dat onderdeel. Hierdoor kan Facebook de gebruikers meteen herinneren aan het feit dat ze een privacy keuze moeten maken bij elk onderdeel. Er zullen dan minder fouten worden gemaakt in de privacy instellingen en hierdoor zal de toegang tot persoonlijke gegevens minder vaak worden verleend aan de verkeerde personen.

10 Deelvraag 5: Hoe kan Facebook haar beveiligingsmodel aanpassen zodat Facebook gebruikers beschermd worden tegen derde partijen die hun persoonlijke informatie in handen willen krijgen?

10.1 Enquête

In de enquête is er een vraag gesteld over wat Facebook kan doen om de persoonlijke gegevens beter te beschermen. Daarnaast zijn er ook twee vragen gesteld over hoe tevreden de studenten zijn met de bescherming van hun persoonlijke gegevens op Facebook en hoeveel vertrouwen de studenten hebben in Facebook als het gaat om de bescherming van hun persoonlijke gegevens.

10.1.1 Suggesties van studenten

De studenten hebben als Facebook gebruikers via de volgende vraag suggesties aangedragen over wat Facebook zou kunnen doen om hun persoonlijke gegevens beter te beschermen:

"Wat zou Facebook kunnen doen om de persoonlijke gegevens van haar gebruikers beter te beschermen?"

Suggestie:	Aantal keer genoemd:
Geen gegevens doorverkopen / Geen gerichte reclame maken / Duidelijk zijn in wat ze precies met de persoonlijke informatie doen	14
Privacy instellingen standaard op “alleen voor vrienden” zetten	7
Instellingen makkelijker maken	5
Persoonlijke gegevens niet opslaan	4
Het is de verantwoordelijkheid van de gebruikers zelf om voor hun bescherming te zorgen	3
Facebook app ontwikkelaars opleggen dat ze alleen toegang vragen tot het deel van de persoonlijke gegevens die daadwerkelijk nodig zijn voor de app	1
Meer beveiligingsfuncties toevoegen	1

De meest genoemde suggestie is dat Facebook de gegevens niet moet doorverkopen aan derde partijen, dat Facebook geen gerichte reclame moet maken op basis van persoonlijke gegevens en als de gegevens worden doorverkocht dat Facebook dan in ieder geval duidelijk moet zijn over wat er precies met die gegevens gebeurt.

Ook een veel genoemde suggestie is om de privacy instellingen standaard op “alleen voor vrienden” te zetten. Op dit moment staan de privacy instellingen standaard op een toegang voor iedereen. Als de instellingen standaard op “alleen voor vrienden” zouden staan worden de gebruikers beter beschermd, ook als ze niet op de hoogte zijn van de privacy instellingen.

Vijf studenten zeggen dat ze de instellingen te moeilijk in gebruik vinden. Deze studenten vinden dat de privacy instellingen op Facebook makkelijker in gebruik gemaakt kunnen worden door bijvoorbeeld één duidelijke pagina te maken waar alle privacy overzichtelijk geregeld kan worden.

Een andere belangrijke suggestie is om de “app” ontwikkelaars op te leggen dat ze alleen toegang vragen tot het deel van de persoonlijke gegevens die daadwerkelijk nodig zijn voor de app. Hierdoor zal het niet meer voorkomen dat een Facebook gebruiker onverwacht toegang verleent aan al zijn persoonlijke gegevens als hij gebruik maakt van een app, zonder dat hij bewust is van de gevolgen hiervan.

Ook is genoemd dat er meer beveiligingsfuncties toegevoegd moeten worden zodat de gebruikers hun Facebook pagina beter kunnen beschermen. Bijvoorbeeld

de “alleen voor vrienden” functie uitbreiden zodat precies ingesteld kan worden welke vrienden toegang hebben tot een bepaald onderdeel. Dit is vooral handig voor Facebook gebruikers die veel vrienden hebben en moeilijk overzicht hebben aan wie ze nou precies toegang verlenen als ze gebruik maken van de “alleen voor vrienden” instelling.

10.1.2 Facebook tevredenheid en vertrouwen

In de enquête is de studenten gevraagd naar hun mening over hoe goed Facebook hun persoonlijke gegevens beschermt. Gevraagd werd: *”Hoe goed beschermt Facebook volgens u de persoonlijke gegevens van haar gebruikers?”* In figuur 17 is te zien dat de meerderheid van de studenten vindt dat Facebook hun persoonlijke gegevens slecht beschermt.

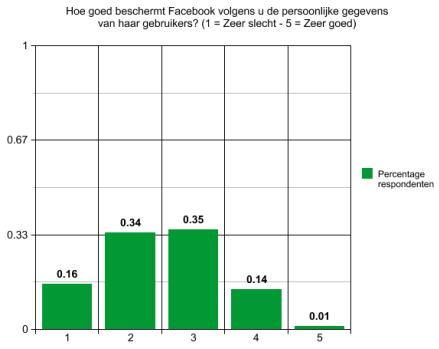

Figure 17: Negende enquête vraag

Daarnaast werd er gevraagd naar het vertrouwen dat de studenten hebben in Facebook als het aankomt op de bescherming van hun persoonlijke gegevens. Gevraagd werd: *”Hoeveel vertrouwen heeft u in Facebook als het gaat om de bescherming van uw persoonlijke gegevens?”* In figuur 18 is te zien dat ook hier de meerderheid van de studenten weinig vertrouwen heeft in Facebook als het aankomt op de bescherming van hun persoonlijke gegevens.

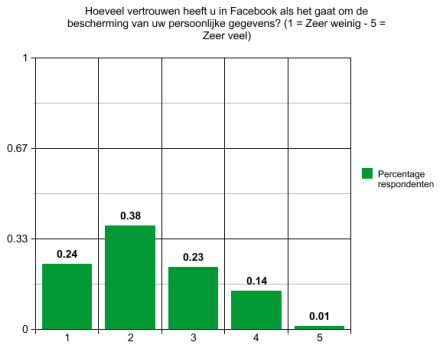

Figure 18: Tiende enquête vraag

10.1.3 Verbeteringen op basis van beveiligingsmodel

Bekend is dat derde partijen op verschillende manieren via phishing, fraude en scams de persoonlijke gegevens van Facebook gebruikers in handen proberen te krijgen. Als valse friend requests worden geaccepteerd of als gebruikers via phishing inloggegevens prijsgeven dan kunnen persoonlijke gegevens bij derde partijen terecht komen.

Omdat het FIS beveiligingssysteem van Facebook blijft leren van eerdere aanvallen zal de beveiliging steeds beter worden. Daarnaast zal Facebook dit systeem steeds moeten updaten zodat alle nieuwe aanvalssoorten kunnen worden tegengegaan. Belangrijk is ook dat Facebook rekening houdt met aanvallen vanuit de opkomende trend van de Facebook apps. Deze apps vragen vaak toegang tot persoonlijke gegevens van de gebruikers, en de gebruiker verleent vaak toegang omdat de app anders niet gebruikt kan worden. Dit zal een opkomende manier zijn waarmee derde partijen toegang kunnen krijgen tot persoonlijke gegevens van de gebruikers. Facebook zal een manier moeten vinden waarmee ze deze aanval kunnen tegengaan. Zo kan bijvoorbeeld het FIS systeem aangepast worden zodat het ook checks uitvoert op de read en write acties die een app uitvoert op de persoonlijke gegevens van de gebruikers.

10.2 Beantwoording deelvraag

Hoe kan Facebook haar beveiligingsmodel aanpassen zodat Facebook gebruikers beschermd worden tegen derde partijen die hun persoonlijke informatie in handen willen krijgen?

De meest genoemde suggestie door de respondenten is dat Facebook geen persoonlijke gegevens moet doorverkopen en geen gerichte reclame moet maken. Dit is waarschijnlijk geen rele optie voor Facebook, omdat een groot deel van hun inkomsten uit deze reclame en verkoop komt. Maar een interessant punt

dat verder wordt genoemd door de respondenten is dat Facebook in ieder geval duidelijk moet zijn wat er met de persoonlijke gegevens van de gebruikers gedaan wordt. Op dit moment is dit in kleine lettertjes te zien onderaan elke Facebook webpagina, maar dit kan duidelijker gemaakt worden. Facebook kan bijvoorbeeld de gebruiker de volledige Terms of Use en de Privacy Policy laten zien en ondertekenen als de Facebook account wordt aangemaakt. Op dit moment staat er in kleine lettertjes bij aanmaak van een Facebook account: "By clicking Sign Up, you agree to our Terms and that you have read and understand our Data Use Policy". Maar dit is onduidelijk en de gebruiker kan dit mogelijk missen als hij druk bezig is met het invullen van de gegevens voor de aanmaak van de Facebook account.

Een ander belangrijk punt dat wordt genoemd door de respondenten is dat de privacy instellingen standaard op "Alleen voor vrienden" gezet moet worden. Dit is een goede oplossing om gebruikers te beschermen die niet vaardig genoeg zijn in het gebruik van Facebook. Op deze manier wordt de gebruiker altijd beschermd, en kan hij zijn persoonlijke gegevens alleen prijsgeven als hij daar zelf bewust voor kiest. Het probleem dat echter blijft bestaan is dat een gebruiker derden als vriend zou kunnen toevoegen. Als kwaadwillende partijen als vriend worden toegevoegd, dan zullen zij toegang krijgen tot de persoonlijke gegevens van de gebruiker. Zelfs als de privacy instellingen standaard op "Alleen voor vrienden" staan.

Verder kan het beveiligingsmodel van Facebook worden aangepast door updates te blijven toevoegen aan het FIS systeem waardoor het ook de nieuwste aanvallen op persoonlijke gegevens kan tegengaan. Daarnaast kan het FIS systeem worden uitgebreid door het systeem ook checks te laten uitvoeren naar de read en write acties van Facebook apps, omdat dit een opkomende manier is waarmee derde partijen de persoonlijke gegevens van gebruikers in handen kunnen krijgen.

11 Conclusie

11.1 Beantwoording onderzoeksvraag

Hoe is de beveiliging van Facebook opgebouwd en hoe gaat de Facebook gebruiker om met de verantwoordelijkheid om hierin een rol te spelen en zijn eigen beveiliging te waarborgen?

De beveiliging van Facebook heeft al veel onderdelen om de gebruiker te helpen bij de bescherming van zijn privacy. Voorbeelden hiervan zijn:

- Rondleiding bij aanmaak account
- Uitleg over wat er precies gedaan wordt met de persoonlijke gegevens
- Bepalen wie er precies toegang heeft tot bepaalde gegevens

Toch zijn deze onderdelen niet bekend bij alle gebruikers, veel onderdelen die al bestaan worden toch als suggestie genoemd door de respondenten. Dit wijst erop dat de studenten onvoldoende op de hoogte zijn van bepaalde privacy onderdelen op Facebook. Facebook kan hier verbeteringen aanbrengen door meer uitleg te geven over het bestaan van deze onderdelen en over de werking hiervan

Door het steekproefkader kan geen uitspraak gedaan worden over alle Facebook gebruikers, die uitspraak is te breed. Wel kan er een uitspraak gedaan worden over Nederlandse studenten. Nederlandse studenten zijn over het algemeen bewust bezig met de bescherming van hun privacy. Ze zijn op de hoogte van privacy instellingen en maken hier ook gebruik van, ze zijn terughoudend met het toevoegen van een vriend op Facebook als ze deze persoon in het echt niet kennen en ze geven aan veel bezig te zijn met het beveiligen van hun persoonlijke gegevens op Facebook.

Er zijn door de studenten een aantal goede suggesties aangedragen die Facebook eventueel kan toepassen ter verbetering van de privacy:

- Privacy instellingen standaard op “alleen voor vrienden” zetten
- Gebruikers dwingen om meteen een privacy keuze te maken zodra er een nieuw onderdeel wordt toegevoegd zoals een foto
- Strenger toezicht op de toegang die Facebook “apps” hebben tot persoonlijke gegevens van Facebook gebruikers

Daarnaast kan het FIS beveiligingssysteem constant worden geupdate zodat het de nieuwste aanvalsvormen op persoonlijke gegevens kan tegengaan. Ook kunnen er uitbreidingen worden toegevoegd zoals een check op de read en write acties van Facebook apps.

Door middel van deze veranderingen kan de rol van de gebruiker in zijn eigen beveiliging worden verkleind, en de rol van Facebook hierin worden vergroot.

Door de rol van de gebruiker te verkleinen is de kans kleiner dat de persoonlijke gegevens bij verkeerde partijen terecht komen. Er moet rekening gehouden worden met het feit dat sommige Facebook gebruikers niet goed met het internet en websites kunnen omgaan. Door het makkelijker te maken voor deze gebruikers om hun privacy op een goede manier te regelen, zullen minder fouten gemaakt kunnen worden met de privacy.

11.2 Vervolgonderzoek

Mogelijke vervolgonderzoeken die gedaan kunnen worden naar aanleiding van dit onderzoek:

- Onderzoek naar het verschil tussen het Facebook gedrag van Amerikaanse en Nederlandse studenten
  - Komt het verschil in Facebook gedrag door het tijdsverschil van de onderzoeken (2005 en 2011) of door een cultuur/maatschappelijk verschil (Amerika en Nederland)?
- Breder onderzoek naar andere doelgroepen binnen de Facebook gebruikers, bijvoorbeeld een onderzoek naar de lager opgeleide Facebook gebruikers.
  - Gaan laagopgeleiden op een zelfde manier om met hun privacy op Facebook als hoogopgeleiden?

12 Bibliografie

Wetenschappelijke artikelen:

[1] Acquisti, A., Gross, R., 2006, "Imagined Communities: Awareness, Information Sharing and Privacy on The Facebook.", Privacy Enhancing Technologies, Cambridge, UK, 2006.

[2] Gross, R., Acquisti, A., (November 2005), "Information revelation and privacy in online social networks", WPES05, Alexandria, Virginia.

[3] Jones, H., Soltren, J.H., 2005, "Facebook: Threats to Privacy", Project MAC: MIT Project on Mathematics and Computing, http://www-swiss.ai.mit.edu/6.805/student-papers/fall05-papers/facebook.pdf (16 March 2007).

[4] Stein, T., Chen, E., Mangla, K., 2011, "Facebook Immune System", Proceedings of the 4th Workshop on Social Network Systems, New York, USA, 2011.

Overige bronnen:

[5] Agarwal, A., 2008, Facebook: Science and the Social Graph, QCon SF 2008, [Online], Available at: http://www.infoq.com/presentations/Facebook-Software-Stack .

[6] Centraal Bureau voor de Statistiek (CBS), Cijfers 2010/2011, Tabel: Schoolgrootte; onderwijssoort en levensbeschouwelijke grondslag, http://www.cbs.nl/nl-NL/menu/themas/onderwijs/cijfers/kerncijfers/instellingen-en-leerlingen-kc.htm

[7] Facebook, 2011/2012, http://www.facebook.com .

[8] Giles, J., 2011, "Inside Facebook's massive cyber-security system", [Online], Available at: http://www.newscientist.com/article/dn21095-inside-facebooks-massive-cybersecurity-system.html .

[9] Huffington post,"Facebook Party Gets Out Of Control After German Girl Forgets Privacy Setting", Available at: http://www.huffingtonpost.com/2011/06/05/facebook-party-out-of-control_n_871473.html .

[10] Ostrow, A., 2008, "Facebook Open Sources its Server Software", [Online], Available at: http://mashable.com/2008/10/24/facebook-scribe/ .

[11] Rothschild, J., 2009, "High Performance at Massive Scale Lessons learned at Facebook", Jacobs School of Engineering, [Online], Available at: http://video-jsoe.ucsd.edu/asx/JeffRothschildFacebook.asx .

[12] Shroepfer, M., 2009, "Facebook Seattle Engineering Road Show: Mike Shroepfer on Engineering at Scale at Facebook", [Online], Available at: http://www.25hoursaday.com/weblog/2009/10/29 /FacebookSeattleEngineeringRoadShowMikeShroepferOnEngineeringAtScaleAtFacebook.aspx

[13] ThesisTools Online Enquêtes, Joan van Rixtel, Enquête aangemaakt in 2011, http://www.thesistools.com .