Radboud Universiteit Nijmegen 

MASTER THESIS

Bewust zijn van het belang van informatiebeveiliging

Auteur:	ing. Aziz Suhonic (s0721085)
Onderwijsinstelling:	Radboud Universiteit Nijmegen
Faculteit:	Faculteit der Natuurwetenschappen, Wiskunde en Informatica (FNWI)
Opleiding:	Informatiekunde
Afdeling:	Digital Security
Afstudeerbegeleider:	dr. Peter van Rossum
Afstudeernummer:	103IK
Versie:	1.0

Inhoudsopgave

Voorwoord

Voor u ligt het master thesisverslag van Aziz Suhonic. Centraal staat het bewust zijn van het belang van informatiebeveiliging. Dit master thesisverslag is bedoeld voor afronding van mijn studie Informatiekunde aan de faculteit der Natuurwetenschappen, Wiskunde en Informatica (FNWI) aan de Radboud Universiteit Nijmegen.
In het afstudeeronderzoek is onderzocht in hoeverre er een verband is tussen het volgen van een bepaald opleidingstype en het bewustzijn van het belang van informatiebeveiliging. Specifiek is er gekeken of de studenten die tijdens hun opleiding te maken hebben gehad met informatiebeveiliging zich bewuster zijn van het belang hiervan, dan de studenten die hiermee niet te maken hebben gehad.

In dit voorwoord wil ik graag alle mensen bedanken die tijdens mijn onderzoek behulpzaam zijn geweest. In het bijzonder de heer Peter van Rossum voor het begeleiden van mijn afstudeeronderzoek en Gerard Kraaijvanger voor het doornemen en verbeteren van mijn master thesisverslag op taal- en spelfouten. Daarnaast wil ik de studenten van Informatiekunde, Rechten, Natuurkunde, Wiskunde en Biologie bedanken voor hun bijdrage bij het invullen van de enquête.
Tot slot wil ik iedereen bedanken die een bijdrage heeft geleverd aan dit resultaat.

Aziz Suhonic
Nijmegen, juli 2009

Samenvatting

Informatiebeveiliging is actueel. Hoe vaak horen we niet in het nieuws of lezen we in de krant dat een bedrijf of instelling getroffen is? Als het gaat om één bedrijf of één individu, valt de schade nog wel mee maar wat als het gaat om tientallen of honderden mensen?
Volgens het rapport 'Cybercrime against businesses' zijn 67% van de bedrijven door minstens één vorm van cybercrime getroffen. Alleen cybercriminaliteit bij bedrijven leidde volgens het rapport tot een verliespost van 867 miljoen dollar in 2005. Ook de overheid probeert mensen bewuster te maken van de gevaren van cybercrime door meer informatie te geven over informatiebeveiliging.

Uit het voorgaande kan er geconcludeerd worden dat de informatiebeveiliging steeds belangrijker wordt. Maar in hoeverre zijn de mensen zich hiervan bewust. Het gebrek aan voorlichting wordt als de reden gegeven voor het niet bewust zijn van de gevaren die cybercriminaliteit met zich meebrengt.
De aanname die hiermee ontstaat, is dat voorlichting van belang is bij het creëren van informatiebeveiligingsbewustzijn. Binnen het wetenschappelijk onderwijs zijn er opleidingstypen die aandacht besteden aan informatiebeveiliging. Een tweetal voorbeelden hiervan zijn informatica en informatiekunde. Uit de aanname welke eerder is gegeven, zou het betekenen dat de studenten die deze opleidingstypen volgen, bewuster zijn van het belang van informatiebeveiliging dan hun medestudenten van andere opleidingstypen vandaar de volgende onderzoeksvraag:

- Is er een verband tussen het opleidingstype en het bewust zijn van het belang van informatiebeveiliging?

Om deze onderzoeksvraag te kunnen beantwoorden is een onderzoek uitgevoerd, waarbij onder vijf verschillende opleidingstypen een enquête is gehouden onder 70 studenten. Hierin is gekeken of de studenten die tijdens hun opleiding niet te maken hebben gehad met informatiebeveiliging, even hoge scores behalen met betrekking tot informatiebeveiligingsbewustzijn als de studenten van informatiekunde.

Uit de antwoorden op de deelvragen kan er geconcludeerd worden dat er een verband bestaat tussen het opleidingstype en het bewustzijn van het belang van informatiebeveiliging. Op alle drie indicatoren kennis, gedrag en mening is door het opleidingstype informatiekunde een hogere score behaald in vergelijking met andere opleidingstypen.
De verschillen die waargenomen zijn tussen de opleidingstypen zijn significant. Op de indicator kennis is er een verschil van 1,1 punt tussen de opleidingstypen informatiekunde en rechten, 1,3 punt tussen informatiekunde en de opleidingstypen biologie en natuurkunde en 1,4 punt tussen de opleidingstypen informatiekunde en wiskunde.
Op de indicator gedrag is er een verschil van 0,6 punt tussen de opleidingstypen informatiekunde, natuurkunde en rechten. Tussen de opleidingstypen informatiekunde, wiskunde en biologie is er een verschil van 0,7 punt berekend.
Op de indicator mening is er een verschil van 0,9 punt tussen de opleidingstypen informatiekunde, natuurkunde en wiskunde. Tussen de opleidingstypen informatiekunde en rechten is er een verschil van 0,8 punt berekend. Een verschil van 1,3 punt is er berekend tussen de opleidingstypen informatiekunde en biologie.

Bij een verschil van 0,6 punt of hoger mag er geconcludeerd worden dat er een significant verschil is tussen de opleidingstypen. Aangezien het opleidingstype informatiekunde op alle indicatoren een score behaalt die minimaal 0,6 hoger is dan wat de andere opleidingstypen behalen, mag er geconcludeerd worden dat er inderdaad een verband is tussen het opleidingstype en bewust zijn van het belang van informatiebeveiliging.

Naast het verband tussen het opleidingstype en bewustzijn van het belang van informatiebeveiliging is er een sterk verband tussen de indicatoren gedrag en mening. Er is een correlatie berekend van 0,71 tussen deze twee indicatoren. Door het berekenen van de p-waarde is vastgesteld dat de bovenstaande uitkomst van 0,71 significant is. De berekende p-waarde bedroeg 0,004. Omdat deze lager uitvalt dan 0,05 hebben we te maken met statistisch significant verband tussen de indicatoren. Tussen de indicatoren kennis/mening en kennis/ gedrag is er een matig verband geconstateerd. De waardes die hierbij berekend zijn 0,43 tussen de indicatoren kennis en mening, 0,41 tussen de indicatoren kennis en gedrag. De hierbij uitgekomen p-waarde is, 0,11 en 0,14. Aangezien beide van deze p-waarden hoger zijn dan 0,05, kan er niet gesproken worden van statistisch significant verband tussen deze indicatoren.

1. Probleemstelling

Informatiebeveiliging is actueel. Hoe vaak horen we niet in het nieuws of lezen we in de krant dat een bedrijf of instelling getroffen is? Als het gaat om één bedrijf of één individu valt de schade nog wel mee. Maar wat als het gaat om tientallen of honderden mensen, zoals het televisieprogramma Zembla 'Wij weten alles van u' in november 2008 liet zien?(1) Hierin worden er op Russische criminele sites de gestolen creditcardgegevens van een aantal mensen gekocht, waarmee vervolgens tal van aankopen worden gedaan. Dat we hierover horen, heeft te maken met de ernst van de zaak. Het gaat om calamiteiten. Over kleinere incidenten hoor je niks in de media, maar deze komen op grote schaal voor. Volgens het rapport 'Cybercrime against businesses' is 67% van de bedrijven door minstens één vorm van cybercrime getroffen. Alleen cybercriminaliteit bij bedrijven leidde volgens het rapport tot een verliespost van 867 miljoen dollar in 2005.(2)

Uit het voorgaande kan er geconcludeerd worden dat de informatiebeveiliging steeds belangrijker wordt. Maar in hoeverre zijn de mensen zich hiervan bewust. Uit het onderzoek van Eleonora 'Cybercrime bij internetbankieren' is 97% van de ondervraagden zich niet bewust van de gevaren bij internetbankieren.(3) Het gebrek aan voorlichting wordt als de reden gegeven voor het niet bewust zijn van de gevaren internetbankieren. Ook de overheid probeert mensen bewuster te maken van de gevaren van cybercrime door meer informatie te geven over informatiebeveiliging. Zo zijn de websites digibewust.nl en samentegencybercrime.nl gelanceerd. Hiermee hoopt men dat mensen bewuster worden van het belang van informatiebeveiliging.(4)

De aanname die hiermee ontstaat, is dat voorlichting van belang is bij het creëren van informatiebeveiligingsbewustzijn. Binnen het wetenschappelijk onderwijs zijn er opleidingstypen die aandacht besteden aan informatiebeveiliging. Een tweetal voorbeelden hiervan zijn informatica en informatiekunde. Uit de aanname welke eerder is gegeven, zou het betekenen dat de studenten die deze opleidingstypen volgen zich bewuster zijn van het belang van informatiebeveiliging dan hun medestudenten van de andere opleidingstypen.
Om dit te toetsen zal binnen dit onderzoek gekeken worden of er een verband is tussen het volgen van een bepaald opleidingstype en het bewust zijn van het belang van informatiebeveiliging. Specifiek zal gekeken worden of de studenten die tijdens hun opleiding te maken hebben gehad met informatiebeveiliging zich bewuster zijn van het belang hiervan dan de studenten die hiermee niet te maken hebben gehad.

Onderzoeksvraag: Is er een verband tussen het opleidingstype en het bewust zijn van het belang van informatiebeveiliging?

2. Verantwoording

Er zijn een aantal onderzoeken gedaan naar het bewust zijn van het belang van informatiebeveiliging. Een onderzoek waarin uitspraken worden gedaan over het bewust zijn van het belang van informatiebeveiliging is; 'Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm'.(5) Een van de bevindingen is het ontbreken van bewustzijn bij medewerkers van het belang van informatiebeveiliging. Informatiebeveiliging staat of valt met het gedrag van medewerkers en effectieve controle op gedrag ontbreekt nog te vaak. Een ander onderzoek waarin bewustzijn ter sprake komt is; 'Informatiebeveiliging en bewustzijn'.(7) Hierin wordt aangegeven dat de meeste mensen zich bewust zijn zolang de maatregelen redelijk zijn en de steun van het management hebben. In de literatuur wordt er ook gesproken over de campagnes voor bewustwording van informatiebeveiliging. Volgens Killmeyer zijn er doelstellingen en belangen die bereikt moeten worden bij informatiebeveiligingbewustwording-campagnes.(8) Alle doelen die hierin worden genoemd richten zich op de werknemers.

Er zijn een aantal redenen waarom dit onderzoek wordt uitgevoerd. De eerste reden is maatschappelijke relevantie. Dit onderzoek is maatschappelijk relevant, omdat het belang van informatiebeveiliging een steeds groter 'issue' is in Nederland. Er wordt veel over dit probleem gesproken in de media en de overheid is bezig om dit probleem aan te pakken door allerlei maatregelen te nemen, zoals nieuwe wetgeving tegen cybercrime.(6) De gewenste situatie is dat mensen zich bewust zijn van het belang van informatiebeveiliging. Om deze situatie te bereiken en het probleem op te lossen, is het van belang om te weten welke mogelijke oorzaken er zijn voor dit probleem. Het is dus noodzakelijk om onder andere te weten of er een verband is tussen het type opleiding wat een student volgt en het bewustzijn. Dit onderzoek draagt bij aan het vergaren van de benodigde kennis om het maatschappelijke probleem op te lossen; als namelijk blijkt dat er een verband is tussen het opleidingstype en het bewustzijn van het belang van informatiebeveiliging, dan kan er gerichter voorlichting worden gegeven over het belang van informatiebeveiliging, zodat bij kan worden gedragen aan het behalen van de gewenste situatie m.b.t. het bewust zijn van het belang van informatiebeveiliging. Als bijvoorbeeld blijkt dat de studenten, waar geen aandacht wordt besteedt aan informatiebeveiliging tijdens hun opleiding, zich minder bewust zijn van het belang van informatiebeveiliging, dan kan de overheid deze opleidingen gerichter benaderen door speciale campagnes. Het onderzoek is dus belangrijk, omdat de overheid moet weten of ze gerichter campagnes moet voeren onder bepaalde typen opleidingen of informatiebeveiliging opnemen binnen de opleiding.

Daarnaast is er een andere reden om het bewustzijn van het belang van informatiebeveiliging te meten tussen de verschillende opleidingstypen. Neys vertaalt security awareness naar de menselijke bijdrage aan het realiseren van een niveau van informatiebeveiliging en maakt daarbij onderscheid tussen een noodzakelijke en een gewenste bijdrage van werknemers.(10) Dit kan vertaald worden naar de studenten die de werknemers van morgen zijn. Indien de bijdrage van een student niet op niveau is, zal het noodzakelijke niveau van informatiebeveiliging niet worden gerealiseerd. Ook al zijn de technische maatregelen wel op niveau. Beveiligingsbewustzijn is de bepalende factor in de bijdrage die een student levert aan het niveau van informatiebeveiliging en dus

is de noodzaak tot inzicht in hoe het zit met beveiligingsbewustzijn van de studenten van de verschillenden opleidingstypen. Vervolgens kunnen er maatregelen genomen worden. Een van de maatregelen zou kunnen zijn de ontwikkeling van systemen die automatisch inspelen op informatiebeveiligings-bewustzijn binnen bepaalde branches waar de studenten van een bepaald opleidingstype gaan werken. Een andere maatregel zou kunnen zijn dat de organisaties waar studenten van een bepaalde opleidingstype gaan werken, meer informatiebeveiliging bewustzijn trainingen te geven.

Dit onderzoek heeft een optimale opbrengst, omdat het gezochte antwoord op de onderzoeksvraag zo informatief mogelijk is. Er zal een uitspraak gedaan kunnen worden over het bewust zijn van het belang van informatiebeveiliging van de studenten aan de Radboud Universiteit Nijmegen; hierbij zal niet alleen worden gekeken naar het bewustzijn tussen de verschillende opleidingstypen, maar ook naar het verband tussen de verschillende indicatoren en hoeveelheid voorlichting dat ze hebben gehad tijdens hun opleiding.

3. Theoretisch kader

Dit onderdeel van het onderzoeksplan bestaat uit drie gedeelten. Allereerst wordt het kennisgebied ingeperkt. Daarna wordt deze inperking in een lopende tekst toegelicht (keuzes en veronderstellingen). Als laatste wordt het theoretische model behandeld.

3.1 Inperking van het kennisgebied

- Informatica en Informatiekunde
  - Beveiliging
    - Informatiebeveiliging
      - Informatiebeveiligingsbewustzijn
        - Kennis, gedrag en mening ten aanzien van informatiebeveiliging

3.2 Toelichting

Het vakgebied van dit onderzoek is beveiliging. Beveiliging is een onderdeel van informatica en informatiekunde. Specifiek zal het onderzoek zich richten op één kennisgebied. Dit kennisgebied is informatiebeveiliging. Binnen de informatiebeveiliging is er gekozen voor een verdere inperking omdat er gekeken wordt naar bewustzijn (kennis, gedrag en mening) ten aanzien van informatiebeveiliging onder de studenten van de Radboud Universiteit Nijmegen.
Dit onderzoek heeft tevens raakvlakken met het vakgebied van de sociale wetenschappen. Toch is er niet gekozen voor een verdere inperking binnen dit vakgebied. Dit komt omdat er een aantal onderzoeken gedaan zijn waarin al modellen ontwikkeld zijn voor het meten van informatiebeveiligingsbewustzijn. Het heeft geen toegevoegde waarde voor dit onderzoek om een nieuw model te ontwikkelen waarbij wel gekeken zou moeten worden binnen het vakgebeid sociale wetenschappen naar wat er allemaal bekend is over bewustzijn. Dit komt uitgebreid aan bod in het hoofdstuk ´1.3 Theoretisch model´.

3.3 Theoretisch model

3.3.1 Informatiebeveiliging bewustzijn

In de literatuur zijn er een aantal definities te vinden over wat informatiebeveiligingsbewustzijn is. Een van de definities definieert het Information Security Forum (ISF) en luidt als volgt:

Informatiebeveiligingsbewustzijn is de graad of mate waarin elk lid van het personeel begrijpt: het belang van informatiebeveiliging, het niveau van informatiebeveiliging dat voor de organisatie noodzakelijk is, de veiligheid van hun individuele verantwoordelijkheden en er ook naar handelt. (9)

Wat hier naar voren komt is dat het gaat om de mate waarin medewerkers begrijpen wat het belang, het niveau en de verantwoordelijkheden zijn die men heeft ten opzichte van informatiebeveiliging voor de organisatie en er ook naar handelt. Neys heeft dezelfde definitie van het Information Security Forum gebruikt:

Security awareness is de mate waarin elke medewerker de volgende punten begrijpt: het belang van informatiebeveiliging, het niveau van informatiebeveiliging dat voor de organisatie noodzakelijk is en er ook naar handelt.(10)

Het verschil met de definitie van het Information Security Forum is dat het punt van de individuele verantwoordelijkheid is weggelaten. Omdat dit volgens Neys verwoord wordt binnen het informatiebeveiligingsbeleid, wat volgens haar het minimaal vereiste niveau is voor een organisatie. Binnen dit onderzoek wordt de definitie van ISF gehanteerd.

3.3.1.1 De meetmethodes

Op welke wijze kan informatiebeveiliging bewustzijn gemeten worden? Het artikel het meten van informatiebeveiligingsbewustzijn gaat in op een drietal methodes voor het meten van informatiebeveiliging bewustzijn.(11)

De eerste methode is fysieke observatie en mysteryguest. Hierbij gaat het er om dat de mysteryguest zich fysiek op locaties door kantoren en gebouwen begeeft. Daarbij dient de mysteryguest op basis van een vooraf opgestelde checklist te letten op incidenten die duiden op een tekort aan bewustzijn. Deze methode vergt sociale vaardigheden van degene die de meting uitvoert. Deze zijn echter niet aan iedereen gegeven. Voor een bewustzijnsmeting die objectief en nauwkeurig moet zijn en bij herhaling of bij uitvoering door verschillende personen dezelfde resultaten moet opleveren, is deze eigenschap niet ideaal.

De tweede methode is face to face interviews. Via voorbereide vraaggesprekken is te achterhalen hoe medewerkers tegen informatiebeveiliging aankijken, wat ze er onder verstaan, hoe ze in bepaalde omstandigheden zouden handelen, hoe ver hun kennis van het informatiebeveiligingsbeleid en de daaruit afgeleide regels en richtlijnen van de organisatie reikt. Deze methode leent zich niet goed uit voor de onderzoeken waar de benodigde steekproefkader groot is. Dit komt omdat een gesprek al snel een uur tot anderhalf uur duurt. Daarnaast vergt het uitwerken van gehouden gesprekken aanzienlijke inspanning. Deze meetmethode is sterk afhankelijk van de interviewvaardigheden van de onderzoeker en is afhankelijk van de voor de gesprekken geselecteerde personen.

De derde methode is online IB-peilingen. Hierbij wordt een digitale vragenlijst speciaal geprepareerd en 'losgelaten' op alle medewerkers van de organisatie of een bepaalde subgroep. De vragenlijst is via internet of het intranet webbased te beantwoorden en de deelname is al dan niet vrijwillig en/of anoniem. De vragenlijst is zeer belangrijk, deze moet absoluut goed zijn. Er is maar één gelegenheid om hem op te stellen. Als de meting loopt is de vragenlijst niet meer te wijzigen. Let bij het opstellen op de aspecten kennis, houding en gedrag.

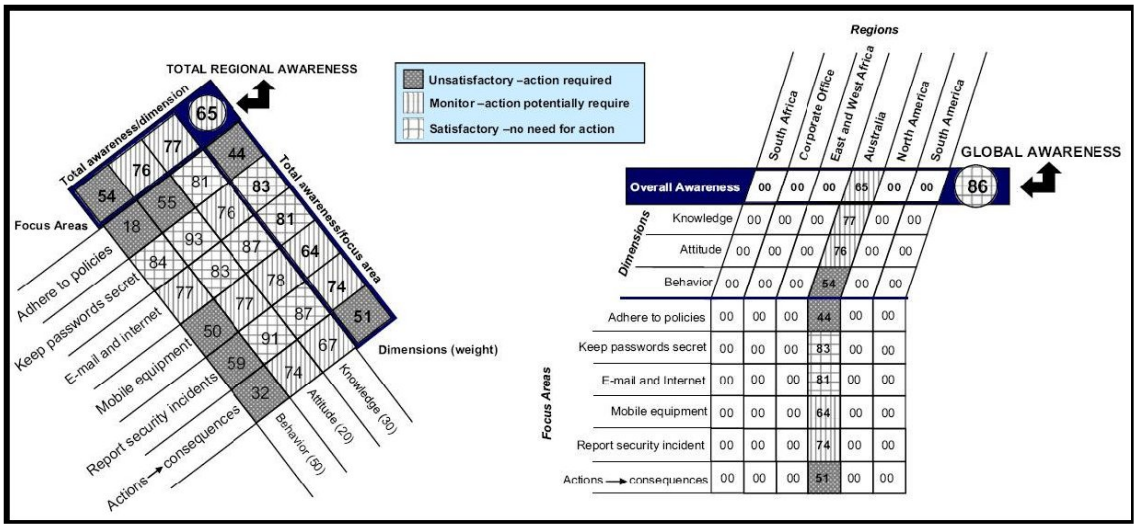
3.3.1.2 De meetmodellen

Naast de methodes zijn er een aantal modellen in de literatuur te vinden voor het meten van informatiebeveiligingsbewustzijn. Binnen het onderzoek van Kruger en Kearney wordt er een prototype beschreven om het informatiebeveiligings-bewustzijn te meten.(12)

Hierbij worden 35 vragen gesteld die ingaan op de attitude, kennis en gedrag. Per aspect richt hun model zich verder op zes verschillende gebieden. De zes kritische risicogebieden zoals zij het noemen. Het gaat om de volgende gebieden:

- *Altijd voldoen aan het bedrijfsbeleid,*
- *Houd wachtwoorden en persoonlijke identificatienummers geheim,*
- *Gebruik e-mail en het internet met zorg,*
- *Wees voorzichtig bij het gebruik van mobiele apparatuur,*
- *Meld incidenten zoals virussen, diefstallen en verliezen,*
- *Wees u ervan bewust dat alle acties gevolgen hebben.*

De uitkomst van een informatiebeveiligingsbewustzijnmeting kan er als volgt uitzien.



Figuur 1: Uitkomst van een informatiebeveiligingsbewustzijnmeting (12)

Het ontwikkelde meetmodel is gebaseerd op technieken uit het kennisgebied van de sociale wetenschappen. De drie componenten die als basis gebruikt zijn voor het meetmodel zijn: attitude*, gedrag en kennis*. De uitkomst hiervan is dat binnen het meetmodel wordt gekeken naar:

- Wat weet een persoon? Kennis
- Wat doen ze? Gedrag
- Wat voelen ze voor het onderwerp? Attitude

Het uitgangspunt van de drie aspecten zoals die beschreven zijn, komen in overeenstemming met een tweetal andere onderzoeken ten aanzien van het verkrijgen van een informatiebeveiligingsbewustzijnsniveau.(13),(14)

Gezien er in meerdere onderzoeken aangegeven wordt dat het informatiebeveiligingsbewustzijn te meten is door te kijken naar kennis, gedrag en attitude zal het ontwikkelde meetmodel van Kruger en Kearney gebruikt worden binnen dit onderzoek. Hierdoor is het binnen dit onderzoek niet nodig om het vakgebied van de sociale wetenschappen te betrekken omdat het aanwezige model opgesteld is op basis van de technieken uit de sociale wetenschappen.

3.3.2 Informatiebeveiliging

In de literatuur zijn er een aantal definities te vinden over wat informatiebeveiliging is. Een van de definities definieert de Code voor Informatiebeveiliging en luidt als volgt:

Informatie is een bedrijfsmiddel dat, net als andere belangrijke bedrijfsmiddelen, waarde heeft voor een organisatie en voortdurend op een passende manier beveiligd dient te zijn. Informatiebeveiliging beschermt informatie tegen een breed scala aan bedreigingen, om de continuïteit van de bedrijfsvoering te waarborgen, de schade voor de organisatie te minimaliseren en het rendement op investeringen en de kansen van de organisatie te optimaliseren. Informatie komt in veel vormen voor. Het kan afgedrukt of beschreven zijn op papier, elektronisch opgeslagen zijn, per post of via elektronische media worden verzonden, getoond worden in films of de gesproken vorm aannemen. Welke vorm informatie ook heeft, of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn.(15)

Door Overbeek en anderen wordt informatiebeveiliging als volgt gedefinieerd:

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket maatregelen om de betrouwbaarheid van de informatie en de informatiesystemen te waarborgen.(16)

Het verschil met de definitie van de Code voor Informatiebeveiliging is dat het punt van de waarde van informatie als bedrijfsmiddel is weggelaten. Binnen dit onderzoek wordt de definitie van Code voor Informatiebeveiliging gehanteerd.

3.3.2.1 Bedreigingen, kwetsbaarheden en risico's

De informatievoorzieningen staan voortdurend bloot en zijn vatbaar voor vele verschillende bedreigingen. Binnen het onderzoek van Looijen worden bedreigingen in vier categorieën ingedeeld:

- Bedreigingen van natuurlijke aard; bliksem.
- Opzettelijke aard; diefstal.
- Niet opzettelijke aard; brand.
- Technische aard; storing in apparatuur.

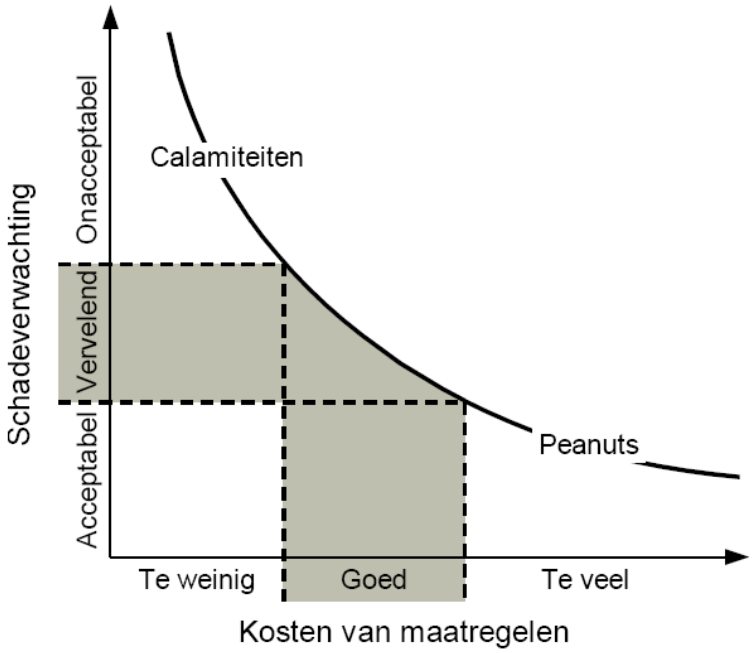
Binnen de literatuur wordt er over een bedreiging gesproken als een proces of een gebeurtenis in potentie een verstorende invloed heeft op de betrouwbaarheid van objecten in de informatievoorziening.(18)
Bedreigingen worden onderverdeeld naar de aspecten van betrouwbaarheid die ze negatief beïnvloeden.(16) Betrouwbaarheid bestaat uit de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.(15)

- Beschikbaarheid: bevat de garanties voor het afgesproken niveau van dienstverlening gericht op de beschikbaarheid van de dienst op de afgesproken momenten (bedrijfsduur, waarbij rekening wordt gehouden met uitvalstijden, storingen en incidenten).
- Integriteit: is het kwaliteitsbegrip dat juistheid, volledigheid, tijdigheid en geautoriseerdheid van de transacties omvat.
- Vertrouwelijkheid: is het kwaliteitsbegrip waaronder privacybescherming maar ook de exclusiviteit van informatie gevangen kan worden. Het

waarborgt dat alleen geautoriseerden toegang krijgen en dat informatie niet kan uitlekken.

Kwetsbaarheid is de mate waarin de informatievoorziening gevoelig is voor bedreigingen. Deze gevoeligheid ontstaat doordat één of meer objecten (gegevensinfrastructuur, applicaties) van de informatievoorziening het mogelijk maken dat één of meer bedreigingen (diefstal, virus of hacking) leiden tot een negatieve invloed op één van de betrouwbaarheidsaspecten (Beschikbaarheid, Integriteit en Vertrouwelijkheid). Gevoeligheid is hier de mate waarin gereageerd wordt op een binnenkomend signaal of een bepaald fysisch verschijnsel.(19)

Als laatst onderdeel van informatiebeveiliging zijn er risico's. Een risico is de gemiddelde schade over een gegeven tijdsperiode, die verwacht wordt doordat één of meer bedreigingen leiden tot een mogelijke (ver)storing van één of meer objecten van de informatievoorziening en wel zodanig dat dit leidt tot (ver)storing in de beschikbaarheid, integriteit en/of vertrouwelijkheid van de gegevensverwerking en informatievoorziening.(19)
Er is sprake van een risico als een of meer informatievoorzieningen getroffen kunnen worden door een of meer bedreigingen. De risico's geven aan welke schade verwacht mag worden als een of meerdere bedreigingen plaatsvinden. In figuur 3 wordt er aangegeven hoe de verhoudingen zijn tussen de schadeverwachting en de kosten van de maatregelen.(18)



Figuur 3: Schadeverwachting tegen kosten van maatregelen (18)

Binnen de figuur is te zien dat de schadeverwachting steeds meer acceptabel wordt naar mate er meer maatregelen worden genomen. Verder is binnen de figuur te zien dat er een drietal zones zijn. De bovenste zone laat zien dat indien er te weinig maatregelen genomen worden, schadeverwachting onacceptabel is bij ernstige bedreigingen. De onderste zone gaat om het nemen van teveel maatregelen. Wat betekent dat de kosten van een maatregel hoger zijn dan de schadeverwachting. De middelste zone is de meest interessante zone. Hier

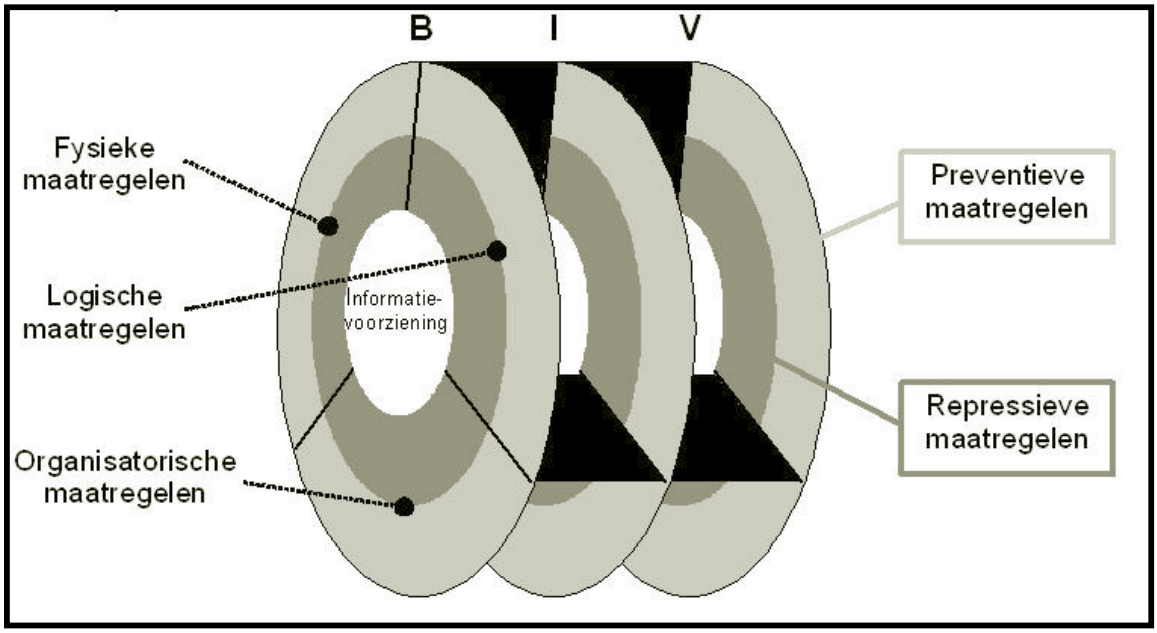
moeten de keuzes gemaakt worden. Het gaat om bedreigingen die vervelende gevolgen hebben, maar niet te voorkomen zijn. Door de juiste kennis van bedreigingen en de organisatie kunnen de juiste maatregelen genomen worden.

3.3.2.2 Beveiligingsmaatregelen

Binnen het onderzoek van Overbeek en anderen wordt er gesproken over de beveiligingsmaatregelen. Deze worden onderverdeeld in een drietal categorieën en worden als volgt omschreven:(16)

- Organisatorische maatregelen; hebben betrekking op de organisatie als geheel. Voorbeelden hiervan zijn: functiescheiding, interne controle of een portier bij de hoofdingang.
- Logische maatregelen; zijn geprogrammeerd en verwerkt in de programmatuur. Voorbeelden hiervan zijn: login- en wachtwoorden-authenticiteit in het besturingssysteem, encryptieprogrammatuur of een digitale handtekening in elektronische post.
- Fysieke maatregelen; zijn gebaseerd op apparatuur of andere materiële zaken zoals: noodstroomvoorziening, brandblussers of sloten.

De betrouwbaarheidsaspecten beschikbaarheid, integriteit en vertrouwelijkheid maken een belangrijk onderdeel uit van informatiebeveiliging. Binnen het onderzoek van Overbeek en anderen zijn de beveiligingsmaatregelen ingedeeld naar de manier waarop ze uitgevoerd worden binnen de betrouwbaarheidsaspecten.



Figuur 2: Beveiligingsmaatregelen ingedeeld naar de manier waarop ze uitgevoerd worden (16)

3.3.3 Statistische analyse

In de literatuur zijn er een aantal definities te vinden over wat statistische analyse is. Een van de definities definieert Statistiek in de praktijk en luidt als volgt:

Statistiek is de wetenschap, de methodiek en de techniek van het verzamelen, bewerken, interpreteren en presenteren van gegevens. Het is een onderdeel van de wiskunde. Statistici trachten informatie over een populatie (al dan niet abstract) te krijgen uit de waarneming van een (meestal) beperkt aantal elementen van die populatie, de steekproef.(20)

3.3.3.1 Steekproef en populatie

De groep individuen of objecten waarvan het kenmerk onderzocht gaat worden, wordt de populatie genoemd. Meestal is het onmogelijk om de gehele populatie te onderwerpen aan een onderzoek. Vaak wordt daarom een klein gedeelte van de populatie onderzocht, een steekproef.
De steekproef moet representatief zijn. Dat wil zeggen dat de steekproef een correct beeld moet geven van de verscheidenheid binnen de populatie, dat in de steekproef alle deelverzamelingen van de populatie evenredig vertegenwoordigd moeten zijn.
De steekproef moet aselect zijn. Dat betekent dat elk element van de populatie dezelfde kans heeft om opgenomen te worden in de steekproef.(20)

3.3.3.2 Onderverdelingen binnen de statistiek

Binnen de statistiek vinden er een aantal onderverdelingen plaats. Er worden een drietal onderverdelingen gemaakt. De eerste onderverdeling wordt verzamelende statistiek genoemd. Het verzamelen van de gegevens voor het onderzoek wordt gedaan via waarnemingen, tellingen of enquêtes bij de elementen van de steekproef.
De tweede onderverdeling wordt beschrijvende statistiek genoemd. De beschrijvende statistiek verzamelt gegevens en beschrijft de toestand door die gegevens te ordenen in tabellen, te verwerken, samen te vatten en grafisch voor te stellen. Ook worden gemiddelden, standaardafwijkingen, vormcoëfficiënten en eventuele correlaties (statistische verbanden) berekend.
De derde onderverdeling wordt verklarende statistiek genoemd. De verklarende statistiek steunt op de resultaten uit de beschrijvende statistiek en op de kanstheorie om uitspraken te doen over de ganse populatie.(20)

3.3.3.3 Aantal analyse technieken

Gemiddeld

Het rekenkundige gemiddelde van een reeks getallen wordt berekend door de getallen bij elkaar op te tellen en vervolgens het totaal te delen door het aantal getallen in de reeks. Bij een ongewogen gemiddelde wordt aan alle getallen eenzelfde gewicht toegekend. Wanneer er sprake is van een gewogen gemiddelde, worden verschillende gewichten toegekend aan de getallen. Dit wordt vaak toegepast om onderzoeksresultaten te corrigeren voor onder- en oververtegenwoordiging van bepaalde groepen in een steekproef. (21)(22)

Mediaan

De mediaan is de middelste waarde in een reeks getallen die gerangschikt zijn naar grootte. Dat wil zeggen dat 50% van de getallen onder de mediaan ligt en 50% van de getallen onder de mediaan. Het voordeel van een mediaan is dat deze minder gevoelig is voor uitbijters dan het gemiddelde. (21)(22)

Standaardafwijking

De standaardafwijking of standaarddeviatie, is een maat voor de spreiding van een variabele, gedefinieerd als de wortel uit de variantie. Er moet daarbij onderscheid gemaakt worden of het gaat om een populatie of een steekproef. Voor een steekproef is de variantie (ongeveer) het gemiddelde van de kwadraten van de afwijking van de metingen ten opzichte van het gemiddelde van de gegevens. Bij een populatie is de variantie de verwachte kwadratische afwijking van de verwachtingswaarde. De standaardafwijking wordt gebruikt om de spreiding, (de mate waarin de waarden onderling verschillen) van een verdeling aan te geven. De standaarddeviatie is de gemiddelde afwijking van het gemiddelde. Een verschil tussen standaardafwijking en variantie is dat de standaardafwijking in dezelfde eenheid wordt uitgedrukt als de verwachtingswaarde of het gemiddelde, waardoor het zinnig wordt te spreken over het gemiddelde plus of min een aantal malen de standaardafwijking.(21)(22)

Bij normale verdelingen wijkt van de mogelijke waarden:

- 68,3% ten hoogste 1 keer de standaardafwijking af van de verwachtingswaarde (het midden van de verdeling)
- 95,4% ten hoogste 2 keer de standaardafwijking af van de verwachtingswaarde
- 99,7% ten hoogste 3 keer de standaardafwijking af van de verwachtingswaarde

Voor de berekening van standaarddeviatie voor oorspronkelijke, ongegroepeerde gegevens in een datamatrix ga je als volgt te werk:

- Bereken het gemiddelde van de variabele.
- Trek iedere waarde van het gemiddelde af.
- Kwadrateer de verschillen: dit gebeurt omdat anders positieve verschillen tegen negatieve zouden wegvallen: het totaal van de afwijkingen zou dan nul zijn!
- Tel de gekwadrateerde verschillen op.
- Standaardafwijking: deel het totaal van de gekwadrateerde verschillen door het aantal waarnemingen. Trek de wortel hieruit. De standaardafwijking wordt hierdoor weer in vergelijkbare hoeveelheden gegeven als het gemiddelde.

Correlatie

De correlatie is een getal tussen -1 en 1, dat aangeeft hoe sterk het verband tussen twee variabelen is. Een correlatie van 0 betekent dat er geen verband is. Een positieve correlatie (groter dan 0), betekent dat hogere waarden op de ene variabele samen gaan met hogere waarden op de andere variabele. Een negatieve correlatie betekent dat hogere waarden op de ene variabele samen

gaan met lagere waarden op de andere variabele. Hoe verder de correlatie van 0 af zit, hoe sterker het verband is. Op basis van toeval zal de correlatie altijd wel iets van 0 afwijken. Maar met de p-waarde wordt beoordeeld of het verband significant is. Bij een p-waarde die kleiner is dan 0.05, is een verband statistisch significant.
Een correlatie kan alleen berekend worden voor variabelen die getallen als uitkomst hebben. De getallen moeten van interval meetniveau zijn, dat wil zeggen dat ze A) een volgorde hebben en dat B) de afstand tussen getallen dezelfde betekenis heeft op verschillende punten van de schaal. De variabele leeftijd is bijvoorbeeld van interval meetniveau: A) een hoger aantal jaren betekent dat de persoon in kwestie ouder is en B) het verschil tussen 5 jaar en 10 jaar is net zo groot als het verschil tussen 65 jaar en 70 jaar. De correlatie meet een lineair verband, dat betekent dat de relatie tussen de variabelen voor alle waarden van de variabelen hetzelfde moet zijn. (20)(21)(22)

- Bereken correlatiecoëfficiënt $R(x,y) = \frac{Cov(x,y)}{\sigma_x \cdot \sigma_y}$
- Hier staat *Cov*(*x, y*) voor de covariantie van *x* en *y*.
- Bereken het gemiddelde m_x van de *x*-waarden en het gemiddelde m_y van de *y*-waarden.
- Bereken voor elk getal x_i de deviatie $d_{xi} = x_i - m_x$ en bereken voor elk getal y_i de deviatie $d_{yi} = y_i - m_y$.
- Bereken de produkten van de deviaties, dus $(x_i - m_x)(y_i - m_y)$.
- Bereken het gemiddelde van die produkten.

Waarden	Sterkte samenhang
0	Geen samenhang
0,25	Zwakke samenhang
0,50	Matig sterk samenhang
0,75	Sterk samenhang
1	Volledige samenhang

Variantie-analyse

Variantie-analyse, een begrip uit de statistiek, vaak aangeduid als ANOVA (van het Engelse 'Analysis of variance'), is een toetsingsprocedure om na te gaan of de populatiegemiddelden van twee of meer groepen van elkaar verschillen. Er wordt gesproken van een significant verschil bij waarden van 0,05 en lager. De term variantie-analyse verwijst naar de uiteenlegging (analyse) van de totale variantie van de gemeten grootheid in twee delen, de variantie binnen de groepen en de variantie tussen de groepen die met elkaar vergeleken worden. (20)(22) Voor de berekening van variantie voor oorspronkelijke, ongegroepeerde gegevens in een datamatrix ga je als volgt te werk:

- Bereken het gemiddelde van de variabele.
- Trek iedere waarde van het gemiddelde af.
- Kwadrateer de verschillen: dit gebeurt omdat anders positieve verschillen tegen negatieve zouden wegvallen: het totaal van de afwijkingen zou dan nul zijn!
- Tel de gekwadrateerde verschillen op.
- Variantie: deel het totaal van de gekwadrateerde verschillen door het aantal waarnemingen.

4. Methode

In dit onderdeel van het onderzoeksplan is beschreven wat de onderzoeksfunctie is en wat de structuur van het onderzoek inhoudt (deelvragen). Daarnaast wordt het onderzoek geoperationaliseerd (onderzoekseenheden, variabelen, indicatoren, validiteit, dataverzameling en data-analyse). De modellen (tussenmodel en empirisch model) die bij deze operationalisatie horen, zijn te vinden onder het onderdeel operationalisatie.

4.1 Onderzoeksfunctie

Dit onderzoek kan gekenschetst worden als een vergelijkend onderzoek. Op basis van een vermoeden zal er gezocht worden naar het bestaan van verband tussen het opleidingstype en het bewustzijn van het belang van informatiebeveiliging onder de studenten van Radboud Universiteit Nijmegen? Vier willekeurige opleidingstypen zullen vergeleken worden met het opleidingstype informatiekunde. Hierin zal gekeken worden of de studenten, die tijdens hun opleiding niet te maken hebben gehad met informatiebeveiliging, even hoge scores behalen met betrekking tot informatiebeveiligingsbewustzijn als de studenten van informatiekunde.

4.2 Onderzoeksstructuur

De onderzoeksvraag is opgesplitst in drie deelvragen. Met behulp van de resultaten van deze deelvragen kan de onderzoeksvraag beantwoord worden. Om er achter te komen wat het bewustzijn is van de studenten van een bepaald opleidingstype, moet het volgende worden onderzocht:

- Mening
- Kennis
- Gedrag

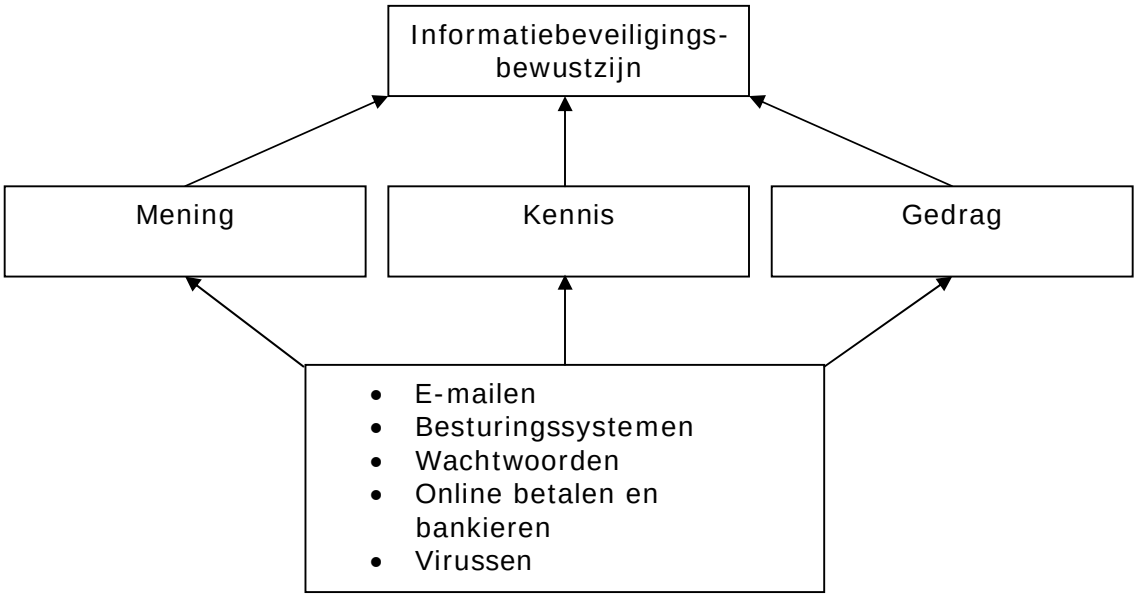
Elk van de bovenstaande dimensies wordt vervolgens onderverdeeld in een vijftal aandachtsgebieden. Dit is besproken binnen het theoretisch kader. De aandachtsgebieden richten zich alle op organisaties. Omdat dit onderzoek niet wordt uitgevoerd binnen een organisatie zijn een aantal aandachtsgebieden niet van toepassing. De volgende aandachtsgebieden zullen binnen dit onderzoek onderzocht worden:

- E-mailen en surfen
- Besturingssystemen
- Wachtwoorden
- Online betalen en bankieren
- Virussen

Op basis van de vijf bovenstaande punten zijn de volgende drie deelvragen opgesteld:

- Hoe kijken de studenten tegen informatiebeveiliging aan? Mening
- Hoe zouden de studenten reageren in bepaalde situaties met bettrekking tot informatiebeveiliging? Gedrag

- Hoever reikt de kennis van de studenten over informatiebeveiliging? Kennis



4.3 Antwoord op de onderzoeksvraag

Door dit onderzoek uit te voeren wordt er een antwoord gegeven op of er een verband is tussen het opleidingstype en het bewust zijn van het belang van informatiebeveiliging onder de studenten van Radboud Universiteit Nijmegen. Als uit de resultaten van het onderzoek blijkt dat er geen verband is tussen deze twee variabelen, dan is het antwoord op de onderzoeksvraag duidelijk. Er is geen verband als er geen significante verschillen van bewustzijn worden waargenomen tussen de studenten van de verschillende opleidingstypen. Als echter blijkt dat er wel een verband is tussen opleidingstype en bewust zijn van het belang van informatiebeveiliging, dan zal ook worden aangegeven wat dit verband inhoudt: zijn de studenten van een bepaalde opleidingstype juist meer of minder bewust van het belang van informatiebeveiliging en waar zitten de verschillen tussen de verschillende opleidingstypen (mening, kennis, gedrag)? Er wordt vastgesteld dat er een verband is tussen het opleidingstype en het bewustzijn als van minstens één van de drie indicatoren van bewustzijn er significante verschillen worden waargenomen tussen de studenten van de verschillende opleidingstypen. Er wordt gesproken van een significant verschil als er een verschil wordt waargenomen van 0,6 of hoger.
Het is belangrijk om op te merken dat het daadwerkelijke gedrag van de ondervraagden niet nauwkeurig gemeten kan worden door alleen gebruik te maken van een vragenlijst. Dit komt omdat de ondervraagden niet noodzakelijk de waarheid hoeven te vertellen wanneer er over hun gedrag vragen worden gesteld. Aan de andere kant moet ook erkend worden dat niet alle respondenten zullen liegen over hun gedrag met betrekking tot informatiebeveiliging. Daarom zal de vragenlijst een indicatie geven over het niveau van de respondenten wat betreft hun gedrag met betrekking tot informatiebeveiliging.

Een aantal voorbeeldvragen om de deelvragen te kunnen beantwoorden.

- Mening; Ik vind het gebruik van meerdere email adressen ….

zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig

- Gedrag; Tijdens het online bankieren controleer ik of ik gebruik maak van een veilige internetverbinding

  nooit, soms, regelmatig, vaak, altijd

- Kennis; In hoeverre weet je wat brute force aanval betekent en inhoudt?

  onvoldoende, matig, voldoende, goed, zeer goed

4.4 Operationalisatie

De operationalisatie van dit onderzoek komt aan bod in het empirisch model. Dit model is hieronder uitgewerkt en toegevoegd.

Specifiek Universum (Steekproefkader)

Met dit onderzoek wordt een representatieve uitspraak gedaan die geldt voor alle studenten van de Radboud Universiteit Nijmegen die een opleiding volgen op de Radboud Universiteit Nijmegen. Om dit te realiseren, worden de respondenten gekozen uit vier verschillende opleidingstypen en het opleidingstype informatiekunde.

- Onderzoekselementen
  - Studenten van de Radboud Universiteit -> SRU
  - Studenten die een opleiding volgen aan de RU uit vier verschillende opleidingstypen en opleidingstype informatiekunde.
- Indicatoren
  - Informatiebeveiligingsbewustzijn
    - Kennis: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
    - Meetniveau: interval
    - Mening: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
    - Meetniveau: interval
    - Gedrag: SRU -> {nooit, soms, regelmatig, vaak, altijd}
    - Meetniveau: interval
  - Opleidingstype
    - Opleidingstype: SRU -> {informatiekunde, wiskunde, natuurkunde, biologie}
    - Meetniveau: ordinaal
- Empirische variabele
  - Kennis:
    - Kennis spam: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
    - Kennis phishing: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
    - Kennis patch: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}

- Kennis open source: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
- Kennis veilig wachtwoord: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
- Kennis brute force aanval: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
- Kennis virus: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
- Kennis firewall: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
- Kennis veilig internetverbinding: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
- Kennis keylogging: SRU -> {onvoldoende, matig, voldoende, goed, zeer goed}
- Meetniveau voor alle empirische variabelen is interval.

o Mening
- Meerdere email adressen: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Vercijferen email: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Gebruik verouderde besturingssysteem: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Back-up maken: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Kiezen voor de hand liggende wachtwoorden: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Gebruik dezelfde wachtwoord: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Nemen anti-virus maatregelen: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Gebruik anti-spyware software: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Opletten bankzaken publieke computer: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Doorgeven opvallende transacties: SRU -> {zeer onverstandig, onverstandig, neutraal, verstandig, zeer verstandig}
- Meetniveau voor alle empirische variabelen is interval.

o Gedrag
- Openen email: SRU -> {nooit, soms, regelmatig, vaak, altijd}
- Invullen persoonlijke gegevens: SRU -> {nooit, soms, regelmatig, vaak, altijd}
- Installeren updates: SRU -> {nooit, soms, regelmatig, vaak, altijd}
- Maken back-up: SRU -> {nooit, soms, regelmatig, vaak, altijd}
- Doorgeven van wachtwoord: SRU -> {nooit, soms, regelmatig, vaak, altijd}

- Verzinnen complex wachtwoord: SRU -> {nooit, soms, regelmatig, vaak, altijd}
- Controleren veilige internetverbinding: SRU -> {nooit, soms, regelmatig, vaak, altijd}
- Controleren afschrift: SRU -> {nooit, soms, regelmatig, vaak, altijd}
- Computer scannen virusscanner: SRU -> {nooit, soms, regelmatig, vaak, altijd}
- Update virusscanner: SRU -> {nooit, soms, regelmatig, vaak, altijd}
- Meetniveau voor alle empirische variabelen is interval.

4.5 Steekproefkader

Met dit onderzoek wordt er een uitspraak gedaan die geldt voor studenten van verschillende opleidingen aan het Radboud Universiteit Nijmegen. Om dit te realiseren worden de respondenten gekozen uit vijf verschillende opleidingstypen. De gewenste steekproefgrootte voor dit onderzoek is 70 studenten. Dit zou leiden tot een verdeling van 14 studenten per opleidingstype. De steekproefgrootte van 70 studenten is gebaseerd op een populatie van 1750 studenten binnen de vijf opleidingstypen. De steekproefgrootte is gebaseerd op een foutmarge van 10% en een betrouwbaarheidspercentage van 91%. Dit betekent dat in 91% van de gevallen de proportie binnen het universum 10% onder of boven de gevonden steekproefverhouding ligt. Deze percentages zijn berekend op basis van de populatie studenten binnen vijf opleidingstypen van Radboud Universiteit Nijmegen.
De steekproef is gestratificeerd select. Er worden van de vijf verschillende opleidingstypen even veel respondenten gekozen. Vier ervan zijn willekeurig en de vijfde is informatiekundestudenten. Daarnaast is de steekproef ook gestratificeerd naar geslacht.

Het variabele bewustzijn wordt vastgesteld door de volgende drie indicatoren:

- Mening
- Kennis
- Gedrag

Het variabele opleidingstype wordt vastgesteld door de volgende indicator:

- De huidige opleiding die gevolgd wordt op het Radboud Universiteit Nijmegen

Er wordt gekeken of er een relatie bestaat tussen het opleidingstype dat gevolgd wordt (onafhankelijk) en mening (afhankelijk), gedrag (afhankelijk) en kennis (afhankelijk) ten aanzien van informatiebeveiliging.

4.6 Interne validiteit

De interne validiteit van dit onderzoek wordt gewaarborgd door het feit dat de indicatoren die er gebruiken worden om het bewustzijn vast te stellen in eerdere onderzoeken naar bewustzijn van het belang van informatiebeveiliging ook gebruikt zijn om het bewustzijn vast te stellen (zie theoretisch kader). Dit betekent dat de indicatoren valide zijn. Daarnaast zijn de vragen gesteld die te

maken hebben met beschikbaarheid, integriteit en vertrouwelijkheid (zie theoretisch kader).
Om te voorkomen dat er bij het verzamelen van data systematische afwijkingen voorkomen, wordt een vragenlijst opgesteld met vragen die voldoen aan de TAP criteria (topic, applicability & perspective). Binnen de vragenlijst is er voor gekozen om de onderdelen uit de categorieën in te laten vullen aan de hand van een 5-punts Likert schaal, omdat deze schriftelijke methode er voor zorgt dat moeilijk te kwantificeren gegevens toch kunnen worden ondervraagd. Dit zorgt er voor dat de respondent gemakkelijker een passend antwoord kan vinden op een vraag, wat resulteert in betrouwbaardere resultaten. Daarnaast wordt de vragenlijst anoniem afgenomen om er voor te zorgen dat de resultaten hiervan zo betrouwbaar mogelijk zijn.

4.7 Externe validiteit

De externe validiteit wordt gewaarborgd door het feit dat het steekproefkader zo is opgesteld dat een uitspraak gedaan kan worden die geldt voor studenten van het Radboud Universiteit Nijmegen. Het steekproefkader bestaat uit vier willekeurige opleidingstypen en het opleidingstype informatiekunde die worden gegeven aan het Radboud Universiteit Nijmegen. De opleidingstypen worden alle door evenveel respondenten vertegenwoordigd (gestratificeerd select). Daarnaast is de steekproef gestratificeerd naar geslacht om te voorkomen dat de resultaten beïnvloed worden door het geslacht.

4.8 Dataverzameling

Zoals al eerder is aangegeven, is het informatietype van de variabelen die in dit onderzoek aan bod komen feitelijke informatie. De methode van dataverzameling die gebruikt wordt, is een formele gestructureerde situatie (gesloten zelfinvul-vragenlijst). De vragenlijst zal bestaan uit 30 vragen om kennis, gedrag en mening te onderzoeken over de vijf aandachtsgebieden. Bij het samenstellen van de vragenlijst is er gebruik gemaakt van de website digibewust.nl. De vragenlijst dient te zijn opgesteld volgens de TAP-criteria (topic, applicability, perspective) om er zo zeker van te zijn dat elke vraag een juiste en concrete vraagstelling heeft. Omdat de drie deelvragen van het onderzoek nauw met elkaar gerelateerd zijn, zal de dataverzameling voor alle deelvragen plaatsvinden aan de hand van één enquête, waarin vragen gesteld worden die bijdragen aan het beantwoorden van alle drie de deelvragen.
Om er voor te zorgen dat er geen onsystematische afwijkingen plaatsvinden, zal de dataverzameling gestandaardiseerd zijn; alle respondenten zullen voor zover mogelijk op dezelfde manier respons geven, waardoor de resultaten betrouwbaar zullen zijn.
Om de non-respons zo laag mogelijk te houden zal de onderzoeker langs de verschillende opleidingstypen gaan met de vraag aan de respondenten om de vragenlijst in te vullen. Hierdoor zal het beoogde aantal respondenten, dat nodig is voor het onderzoek, behaald worden. Daarnaast zal er geen item non-respons plaatsvinden omdat de onderzoeker ter plekke kan controleren of alle vragen ingevuld zijn.

4.9 Data analyse

Aan de hand van de verkregen resultaten zijn de data verwerkt en geanalyseerd. Er is gekeken naar de onderlinge scores van informatiebeveiligingsbewustzijn per opleidingstype. Hierdoor kon er waargenomen worden of er verschillen zitten in de drie facetten van informatiebeveiligingsbewustzijn (kennis, mening en gedrag) per opleidingstype. De verzamelde vragenlijsten zijn voor de verwerking eerst gestructureerd per opleidingstype. Dit zorgde ervoor dat tijdens de dataverwerking er conclusies konden worden getrokken uit de resultaten van de vragenlijst.
De antwoorden op de vragenlijst hebben een score opgeleverd tussen 0 en 4, waarmee werd bepaald hoe hoog de respondenten scoren van de verschillende opleidingstypen.

Bij het samenstellen van de vragenlijst is als schaallengte 5 punt Linkertschaal gebruikt. De reden hiervoor is dat door het gebruik van Linkertschaal mogelijk is om moeilijk te kwantificeren gegevens toch kunnen worden ondervraagd en geanalyseerd. Hierbij vond een puntentoekenning plaats van 0 tot en met 4. Per indicator worden er 10 vragen gesteld.

	Aantal punten	Weegfactor in %
Kennis	0 - 4	30
Mening	0 - 4	20
Gedrag	0 - 4	50

Het is hier belangrijk om op te merken dat alle aandachtsgebieden (zie 4.2 Onderzoeksstructuur) een even zware wegingsfactor hebben.

Met behulp van statistische methodes kunnen uit de verkregen scores conclusies getrokken worden over informatiebeveiligingsbewustzijn per opleidingstype en over de drie afzonderlijke facetten van informatiebeveiligingsbewustzijn (kennis, mening en gedrag) per opleidingstype. De eerste resultaten zullen een score opleveren tussen 0 en 4 per opleidingstype. Aan de hand hiervan worden er vergelijkingen gemaakt tussen de verschillende opleidingstypen.

Als tweede zal er gekeken worden of er correlatie bestaat tussen kennis/mening kennis/gedrag en mening/gedrag. Om te bepalen of er een significant verband is tussen kennis/mening, kennis/gedrag en mening/gedrag zal er een p-waarde uitgerekend worden. Hierbij is uitgegaan van een standaard significantieniveau van 0,05 (zie 3.3.3.3 Aantal analyse technieken). Dit betekent indien de p-waarde 0,05 of lager is dat we dan te maken hebben met een statistisch significant verband tussen de variabelen. Om te bepalen hoe sterk het verband is tussen de variabelen, is er gebruik gemaakt van Pearsons correlatiecoëfficiënt. Er wordt uitgegaan van een sterk verband indien er een correlatie is van 0,60 of hoger.

Tot slot is er met behulp van variantieanalyse gekeken of de populatiegemiddelden van de groepen echt van elkaar verschillen. Ook hier is uitgegaan van een standaard significantieniveau van 0,05 (zie 3.3.3.3 Aantal

analyse technieken). Dit betekent dat indien er een score van 0,05 en lager uitkomt, er gesproken kan worden van significante verschillen tussen de verschillende opleidingstypen.

Dit zal uiteindelijk het antwoord opleveren op de vraag of er een relatie bestaat tussen het informatiebeveiligingsbewustzijn en opleidingstypen. Met de verkregen resultaten komen we te weten of informatiebeveiligingsbewustzijn daadwerkelijk wordt beïnvloed door het opleidingstypen en waar de verschillen zitten tussen de verschillende opleidingstypen.

5. Conclusie en discussie

Dit onderzoek was een vergelijkend onderzoek. De conclusie en discussie bestaat dus uit het gedeelte vergelijken. Hierin worden de verschillende deelvragen beantwoord. Hierna wordt de onderzoeksvraag beantwoord en worden er voorstellen gedaan voor toekomstig onderzoek.

5.1 Vergelijken

De volgende deelvragen hebben betrekking op het gedeelte vergelijken van de conclusie en discussie:

- Hoe kijken de studenten tegen informatiebeveiliging aan? Mening
- Hoe zouden de studenten reageren in bepaalde situaties met betrekking tot informatiebeveiliging? Gedrag
- Hoe ver reikt de kennis van de studenten over informatiebeveiliging? Kennis

Om deze deelvragen te kunnen beantwoorden zijn er met behulp van een vragenlijst 70 studenten ondervraagd. Dit heeft geleid tot een verdeling van 14 studenten per opleidingstype. De steekproefgrootte is gebaseerd op een foutmarge van 10% en een betrouwbaarheidspercentage van 91%. Dit betekent dat in 91% van de gevallen de proportie binnen het universum 10% onder of boven de gevonden steekproefverhouding ligt.
De hierboven genoemde deelvragen worden hieronder afzonderlijk beantwoord.

Hoe kijken de studenten tegen informatiebeveiliging aan? Mening

Er zijn in totaal 70 studenten ondervraagd. Het opleidingstype informatiekunde behaalt een score van 3,5 van maximaal 4 punten. Het opleidingstype rechten behaalt een score van 2,7 van maximaal 4 punten. De opleidingstypen natuurkunde, wiskunde en biologie behalen respectievelijk 2,6 2,6 en 2,2 punten van maximaal 4 punten. Opmerkelijk is dat de opleidingstypen rechten, natuurkunde, wiskunde en biologie op het onderdeel besturingssystemen een stuk lager scoren in vergelijking met het opleidingstype informatiekunde. Bij dit onderdeel is er een score behaald van 1,5 door alle vier de opleidingstypen terwijl informatiekunde 3,5 scoort. De twee vragen die hierbij werden gesteld, gingen over het back-up maken van de gegevens en gebruik maken van verouderde besturingssystemen. Op het onderdeel virussen is door alle opleidingstypen het hoogst gescoord. Bij het onderdeel virussen ging het om het gebruik maken van anti-spyware en het nemen van antivirus maatregelen. De scores die hierbij behaald werden, variëren van 3,0 tot 3,7 van maximaal 4 punten. Deze scores vallen hoger uit dan het gemiddelde dat per opleidingstype in totaal werd behaald op het onderdeel mening.

Hoe zouden de studenten reageren in bepaalde situaties met bettrekking tot informatiebeveiliging? Gedrag

Op het gebied van gedrag scoort het opleidingstype informatiekunde het hoogst. Het opleidingstype informatiekunde behaalt een score van 3,5 van maximaal 4 punten. De opleidingstypen rechten en natuurkunde behalen een score van 2,9

en de opleidingstypen wiskunde en biologie behalen een score van 2,8. Opmerkelijk hier is dat de vier opleidingstypen in vergelijking met informatiekunde een stuk lager scoren op het onderdeel besturingssystemen. Bij dit onderdeel wordt er een score behaald van 1,5 terwijl het opleidingstype informatiekunde een score behaalt van 3,5. De twee vragen die hierbij werden gesteld gingen over het updaten van besturingssystemen en een back-up maken van de gegevens. Op de onderdelen virussen en e-mailen/surfen is door de alle opleidingstypen hoog gescoord. De twee vragen die hierbij werden gesteld gingen over het openen van email van een onbekende afzender en het invullen van persoonlijke gegevens tijdens het surfen. De scores die bij het onderdeel e-mailen en surfen werden behaald, variëren van 3,5 tot 4,0 van maximaal 4 punten. Het opmerkelijke is dat het opleidingstype rechten een maximale score van 4 behaald heeft. Bij het onderdeel virussen zijn er scores behaald tussen 3,2 en 3,4. Hierbij werden vragen gesteld over het scannen van de computer met een virusscanner en up to date houden van een virusscanner. Opmerkelijk hierbij is dat de opleidingstypen wiskunde en biologie even hoog scoren in vergelijking met informatiekunde. Alle drie de opleidingen behalen een score van 3,4.

Hoever reikt de kennis van de studenten over informatiebeveiliging?
Kennis

Ook op het gebied van kennis scoort het opleidingstype informatiekunde het hoogst. Een score van 3,6 van maximaal 4 punten is hierbij behaald. De opleidingstypen natuurkunde en biologie behalen een score van 2,3. Het opleidingstype rechten behaalt een score van 2,5 en wiskunde 2,2. Bij het onderdeel online betalen en bankieren zijn de laagste scores behaald in vergelijking tot het opleidingstype informatiekunde. De scores die hierbij behaald zijn 1,1 door het opleidingstype natuurkunde, 1,8 door rechten en 1,9 door wiskunde en biologie. De score die door het opleidingstype informatiekunde werd behaald is 3,3. Bij het onderdeel online betalen en bankieren ging het om in hoeverre de ondervraagden weten wat keylogging en veilige internetverbinding betekent en inhoudt. Op het onderdeel virussen is door vier van de vijf opleidingstypen het hoogst gescoord. De twee vragen die hierbij werden gesteld, gingen over in hoeverre de ondervraagden weten wat virus en firewall betekent en inhoudt. De hierbij behaalde scores zijn 3,4 door het opleidingstype informatiekunde, 3,1 door de opleidingstypen rechten en biologie en 2,9 door het opleidingstype natuurkunde. Opmerkelijk hierbij is dat het opleidingstype wiskunde een score behaald heeft van 0,6 punten van in totaal 4 punten. Aan de andere kant heeft het opleidingstype wiskunde een score van 3,5 behaald op het onderdeel e-mailen en surfen wat even hoog is in vergelijking tot het opleidingstype informatiekunde.

5.2 Antwoord op de onderzoeksvraag

Dit onderzoek is uitgevoerd om antwoord te geven op de volgende onderzoeksvraag;

- Is er een verband tussen het opleidingstype en het bewust zijn van het belang van informatiebeveiliging?

Uit de antwoorden op de deelvragen kan er geconcludeerd worden dat er een verband bestaat tussen het opleidingstype en het bewust zijn van het belang van informatiebeveiliging. Op alle drie de indicatoren kennis, gedrag en mening is door het opleidingstype informatiekunde een hogere score behaald in vergelijking met andere opleidingstypen. Een van de redenen voor de hoge score kan de hoeveelheid aandacht voor informatiebeveiliging tijdens de studie zijn. Van het opleidingstype informatiekunde antwoordde 71% dat er veel aandacht aan informatiebeveiliging besteed is tijdens de studie en 29% antwoordde dat er heel veel aandacht besteed is aan informatiebeveiliging. Bij de andere opleidingstypen antwoordde 80% van de ondervraagden dat er helemaal geen aandacht besteed is aan informatiebeveiliging tijdens hun studie en 20% antwoordde dat er weinig aandacht besteed is aan informatiebeveiliging.

De verschillen die waargenomen zijn tussen de opleidingstypen zijn significant. Op de indicator kennis is er een verschil van 1,1 punt tussen de opleidingstypen informatiekunde en rechten, 1,3 punt tussen informatiekunde en de opleidingstypen biologie en natuurkunde en 1,4 punt tussen de opleidingstypen informatiekunde en wiskunde.
Op de indicator gedrag is er een verschil van 0,6 punt tussen de opleidingstypen informatiekunde, natuurkunde en rechten. Tussen de opleidingstypen informatiekunde, wiskunde en biologie is er een verschil van 0,7 punt berekend.
Op de indicator mening is er een verschil van 0,9 punt tussen de opleidingstypen informatiekunde, natuurkunde en wiskunde. Tussen de opleidingstypen informatiekunde en rechten is er een verschil van 0,8 punt berekend. Een verschil van 1,3 punt is berekend tussen de opleidingstypen informatiekunde en biologie.

Bij een verschil van 0,6 punt of hoger mag er geconcludeerd worden dat er een significant verschil is tussen de opleidingstypen. Aangezien het opleidingstype informatiekunde op alle indicatoren een score behaalt dat minimaal 0,6 hoger is dan dat de andere opleidingstypen behalen, mag er geconcludeerd worden dat er inderdaad een verband is tussen het opleidingstype en bewust zijn van het belang van informatiebeveiliging.
Bij alle indicatoren is een significantieniveau van 0,00 behaald. Omdat deze lager uitvalt dan 0,05 hebben we te maken met statistisch significante verschillen tussen de indicatoren en dus ook verschillende opleidingstypen.

Naast het verband tussen het opleidingstype en bewust zijn van het belang van informatiebeveiliging is er een sterk verband tussen de indicatoren gedrag en mening. Er is een correlatie berekend van 0,71 tussen deze twee indicatoren. Door het berekenen van de p-waarde is vastgesteld dat de bovenstaande uitkomst van 0,71 significant is. De berekende p-waarde bedroeg 0,004. Omdat deze lager uitvalt dan 0,05 hebben we te maken met statistisch significant verband tussen de indicatoren. Tussen de indicatoren kennis, mening en kennis, gedrag is er een matig verband geconstateerd. De hierbij berekende waarden

zijn 0,43 tussen de indicatoren kennis en mening en 0,41 tussen de indicatoren kennis en gedrag. De p-waarde die hierbij uitgekomen is, is 0,11 en 0,14. Aangezien beide van deze p-waarden hoger zijn dan 0,05 kan er niet gesproken worden van statistisch significant verband tussen deze indicatoren.

5.3 Mogelijkheden voor toekomstig onderzoek

Uit de conclusie is gebleken dat het opleidingstype informatiekunde de hoogste scores behaalt op het gebied van informatiebeveiligingsbewustzijn. Wat we niet weten is waarom het opleidingstype informatiekunde de hoogste scores behaalt ten opzichte van andere opleidingen. Een van de redenen kan de hoeveelheid voorlichting zijn die ze tijdens hun studie hebben gehad. Maar het is goed denkbaar dat de informatiekundestudenten al voor hun studie interesse hebben ontwikkeld voor informatiebeveiliging en juist daarom gekozen hebben om het opleidingstype informatiekunde te volgen.

In dit onderzoek is er geprobeerd om informatiebeveiligingsbewustzijn onder verschillende opleidingstypen in kaart te brengen. Er is een vergelijking gemaakt tussen het opleidingstype informatiekunde en een aantal andere opleidingstypen. Nu kan er geïmpliceerd worden dat er een verband bestaat tussen informatiebeveiligingsbewustzijn en het opleidingstype informatiekunde. Dit zou verder onderzocht kunnen worden door een enquête te houden om achter de redenen te komen waarom het opleidingstype informatiekunde de hoogste scores behaalt. Hierdoor zou geconcludeerd kunnen worden in hoeverre het gevonden verband tussen informatiebeveiligingsbewustzijn en het volgen van opleidingstype informatiekunde hier aan toe te schrijven is.

6. Literatuur

- (1) Zembla, Wij weten alles van u, November 2008.
- (2) U.S. Department of Juistice, Cybercrime against Businesses, September 2008.
- (3) Eleonora, Cybercrime bij internetbankieren, Juni 2008.
- (4) Tweede Kamer der Staten Generalen, Bestrijding cybercriminaliteit en de mogelijke digitale aanslag in Almere, Oktober 2007.
- (5) Het College bescherming persoonsgegevens & de Inspectie voor de Gezondheidszorg, Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm, 2008.
- (6) ANP, Experts slaan handen ineen tegen cybercrime, 2009.
- (7) Dr. Marcel E.M. Spruit, Informatiebeveiliging en bewustzijn, 2004.
- (8) Killmeyer J., Information security architecture: an integrated approach to security in the organization, 2006.
- (9) Information Security Forum, Effective Security Awareness, Information Security Forum, 2002.
- (10) Neys C., IT'ers, regels en Security Awareness, Referaat postdoctorale opleiding MSIT, 2003.
- (11) de Vries R., Dolfsma R., Het meten van informatiebeveiligings-bewustzijn, Informatiebeveiliging, 2007.
- (12) Krugera H.A., Kearney W.D., A prototype for assessing information security awareness, Elsevier Ltd. vol. 25, 2006.
- (13) Basten N.F.H., Security awareness, Informatiebeveiligingsjaarboek 2003/2004, 2003.
- (14) Jentjens V.L.M., Graaf M.C. de, Geïntegreerde informatiebeveiliging: de sleutel tot succesvolle implementatie, 2004.
- (15) Nederlands Normalisatie-instituut, Code voor informatiebeveiliging, 2002.
- (16) Overbeek P.L., Roos Lindgreen E., Spruit M.E.M., Informatiebeveiliging onder controle, Pearson Education: Financial Times / Prentice Hall, 2005.
- (17) Looijen M., Beheer van informatiesystemen, Ten HageStam, 2004.
- (18) Dr. Marcel E.M. Spruit, Waardevol maakt kwetsbaar: het belang van informatiebeveiliging, 2003.
- (19) Dam M, Wessels K, The human firewall of behavioral information security, Master Thesis Informatiekunde, 2008.

7. Bijlage

7.1 Totaal score kennis, mening en gedrag

Informatiekunde	Gemiddelde aantal punten per dimensie				Maximaal score
	3,6	3,5	3,5	**3,5**	4,0
Focus area					
Emailen & surfen	3,6	3,9	3,0	3,6	4,0
Besturingssystemen	3,9	3,5	3,5	3,6	4,0
Wachtwoorden	3,8	3,2	3,8	3,5	4,0
Virussen	3,4	3,4	3,7	3,5	4,0
Online bankieren en betalen	3,3	3,6	3,8	3,5	4,0
	Kennis 30%	Gedrag 50%	Mening 20%	Totaal	

Rechten	Gemiddelde aantal punten per dimensie				Maximaal score
	2,5	2,9	2,7	**2,7**	4,0
Focus area					
Emailen & surfen	3,0	4,0	3,0	3,5	4,0
Besturingssystemen	2,5	1,5	1,5	1,8	4,0
Wachtwoorden	2,1	2,4	3,5	2,5	4,0
Virussen	3,1	3,2	3,1	3,2	4,0
Online bankieren en betalen	1,8	3,2	2,4	2,6	4,0
	Kennis 30%	Gedrag 50%	Mening 20%	Totaal	

Natuurkunde	Gemiddelde aantal punten per dimensie				Maximaal score
	2,3	2,9	2,6	**2,7**	4,0
Focus area					
Emailen & surfen	3,0	3,8	2,6	3,3	4,0
Besturingssystemen	2,1	1,5	1,5	1,7	4,0
Wachtwoorden	2,2	3,0	3,4	2,9	4,0
Virussen	2,9	3,2	3,0	3,1	4,0
Online bankieren en betalen	1,1	3,1	2,4	2,4	4,0
	Kennis 30%	Gedrag 50%	Mening 20%	Totaal	

Wiskunde	Gemiddelde aantal punten per dimensie				Maximaal score
	2,2	2,8	2,6	**2,6**	4,0
Focus area					
Emailen & surfen	3,5	3,5	2,6	3,3	4,0
Besturingssystemen	2,5	1,5	1,5	1,8	4,0
Wachtwoorden	2,4	3,4	3,3	3,1	4,0
Virussen	0,6	3,4	3,1	2,5	4,0
Online bankieren en betalen	1,9	2,2	2,4	2,2	4,0
	Kennis 30%	Gedrag 50%	Mening 20%	Totaal	

Biologie	Gemiddelde aantal punten per dimensie				Maximaal score
	2,3	2,8	2,2	**2,5**	4,0
Focus area					
Emailen & surfen	2,7	3,5	2,2	3,0	4,0
Besturingssystemen	1,4	1,5	1,5	1,5	4,0
Wachtwoorden	2,3	3,4	2,8	2,9	4,0
Virussen	3,1	3,4	3,1	3,3	4,0
Online bankieren en betalen	1,9	2,1	1,5	1,9	4,0
	Kennis 30%	Gedrag 50%	Mening 20%	Totaal	

7.2 Correlatie en p-waard

Correlatie	Kennis	Mening	Correlatie	Kennis	Gedrag	Correlatie	Gedrag	Mening
Informatiekunde	102	83	Informatiekunde	102	109	Informatiekunde	109	83
	110	99		110	97		97	99
	106	106		106	89		89	106
	95	103		95	96		96	103
	93	105		93	100		100	105
Rechten	83	83	Rechten	83	112	Rechten	112	83
	71	42		71	41		41	42
	58	98		58	66		66	98
	87	88		87	89		89	88
	49	67		49	90		90	67
Natuurkunde	84	73	Natuurkunde	84	105	Natuurkunde	105	73
	60	42		60	41		41	42
	61	95		61	85		85	95
	81	84		81	89		89	84
	30	67		30	88		88	67
Wiskunde	98	73	Wiskunde	98	98	Wiskunde	98	73
	71	43		71	42		42	43
	66	93		66	94		94	93
	16	88		16	96		96	88
	54	67		54	62		62	67
Biologie	76	61	Biologie	76	98	Biologie	98	61
	38	43		38	42		42	43
	63	77		63	94		94	77
	88	86		88	96		96	86
	53	43		53	58		58	43
Totaal correlatie		0,4364929	Totaal correlatie		0,412698	Totaal correlatie		0,7125415
P-waarde		0,118749	P-waarde		0,142610	P-waarde		0,004442

7.3 Variantieanalyse

Kennis

(I) Kennis	(J) Kennis	Mean Difference (I-J)	Sig.
Biologie	Informatiekunde	-13,429*	,000
	Natuurkunde	,143	,838
	Rechten	-1,929*	,007
	Wiskunde	,929	,188
Informatiekunde	Biologie	13,429*	,000
	Natuurkunde	13,571*	,000
	Rechten	11,500*	,000
	Wiskunde	14,357*	,000
Natuurkunde	Biologie	-,143	,838
	Informatiekunde	-13,571*	,000
	Rechten	-2,071*	,004
	Wiskunde	,786	,264
Rechten	Biologie	1,929*	,007
	Informatiekunde	-11,500*	,000
	Natuurkunde	2,071*	,004
	Wiskunde	2,857*	,000
Wiskunde	Biologie	-,929	,188
	Informatiekunde	-14,357*	,000
	Natuurkunde	-,786	,264
	Rechten	-2,857*	,000

Gedrag

(I) Gedrag	(J) Gedrag	Mean Difference (I-J)	Sig.
Biologie	Informatiekunde	-7,357*	,000
	Natuurkunde	-1,429*	,021
	Rechten	-,714	,243
	Wiskunde	-,286	,639
Informatiekunde	Biologie	7,357*	,000
	Natuurkunde	5,929*	,000
	Rechten	6,643*	,000
	Wiskunde	7,071*	,000
Natuurkunde	Biologie	1,429*	,021
	Informatiekunde	-5,929*	,000
	Rechten	,714	,243
	Wiskunde	1,143	,064
Rechten	Biologie	,714	,243
	Informatiekunde	-6,643*	,000

	Natuurkunde	-,714	,243
	Wiskunde	,429	,482
Wiskunde	Biologie	,286	,639
	Informatiekunde	-7,071*	,000
	Natuurkunde	-1,143	,064
	Rechten	-,429	,482

Mening

(I) Mening	(J) Mening	Mean Difference (I-J)	Sig.
Biologie	Informatiekunde	-13,286*	,000
	Natuurkunde	-3,643*	,000
	Rechten	-4,857*	,000
	Wiskunde	-3,857*	,000
Informatiekunde	Biologie	13,286*	,000
	Natuurkunde	9,643*	,000
	Rechten	8,429*	,000
	Wiskunde	9,429*	,000
Natuurkunde	Biologie	3,643*	,000
	Informatiekunde	-9,643*	,000
	Rechten	-1,214*	,050
	Wiskunde	-,214	,725
Rechten	Biologie	4,857*	,000
	Informatiekunde	-8,429*	,000
	Natuurkunde	1,214*	,050
	Wiskunde	1,000	,104
Wiskunde	Biologie	3,857*	,000
	Informatiekunde	-9,429*	,000
	Natuurkunde	,214	,725
	Rechten	-1,000	,104

7.4 Vragenlijst

Kennis

Kruis aan in hoeverre je weet wat de volgende tien begrippen betekenen en inhouden?

	Onvoldoende	Matig	Voldoende	Goed	Zeer goed
Email					
1. Spam					
2. Phishing					
Besturingssystemen					
3. Patch					
4. Open source software					
Wachtwoorden					
5. Veilig wachtwoord					
6. Brute force aanval					
Virussen					
7. Virus					
8. Firewall					
Online bankieren en betalen					
9. Veilige internetverbinding					
10. Keylogging					

Gedrag

E-mailen en surfen

1. Je krijgt een e-mail binnen van XXENAXX@zasar.org. Zou jij een email openen waarvan je de persoon en de organisatie niet kent om inhoud ervan te bekijken.

   nooit, soms, regelmatig, vaak, altijd

2. Je bent aan het surfen op het internet, opeens verschijnt een scherm waarin je wordt meegedeeld dat je een prijs hebt gewonnen. Enige wat je daarvoor moet doen is een aantal van je persoonlijke gegevens invullen.

   Daar doe ik … aan mee.

   nooit, soms, regelmatig, vaak, altijd

Besturingssystemen

3. Je wordt gewaarschuwd dat er nieuwe updates beschikbaar zijn voor je besturingssysteem (Windows XP, Vista, Linux). Wat doe je?

   Ik installeer … updates voor mijn besturingssysteem.

   nooit, soms, regelmatig, vaak, altijd

4. Ik maak … een back-up van mijn gegevens.

   nooit, soms, regelmatig, vaak, altijd

Wachtwoorden

5. Ik ben er van bewust dat je nooit je wachtwoord moet geven aan een ander desondanks heb ik mijn wachtwoord aan een vriend(in) gegeven om even mijn email te controleren of een werkstuk van school door te sturen als ik het zelf niet kan.

   Ik geef mijn wachtwoord … aan een ander.

   nooit, soms, regelmatig, vaak, altijd

6. Bij het verzinnen van een complex wachtwoord zorg ik ervoor dat die bestaat uit minimaal 8 karakters, waarvan er minimaal 4 cijfers, 1 hoofdletter en 1 vreemd teken zijn.

   Bij het verzinnen van een complex wachtwoord hou ik hier … rekening mee.

   nooit, soms, regelmatig, vaak, altijd

Online betalen en bankieren

7. Tijdens het online bankieren controleer ik of ik gebruik maak van een veilige internetverbinding.

   nooit, soms, regelmatig, vaak, altijd

8. Je hebt via internet bankieren een rekening betaald. Controleer je na een online transactie jouw afschrift om te kijken of het juiste bedrag is afgeschreven?

   Ik controleer … mijn afschrift na een online transactie.

   nooit, soms, regelmatig, vaak, altijd

Virussen

9. Ik scan … , met een virusscanner, mijn hele computer op virussen.

   nooit, soms, regelmatig, vaak, altijd

10. Ik zorg … ervoor dat mijn virusscanner up-to-date is.

    nooit, soms, regelmatig, vaak, altijd

Mening

Kruis aan wat je vindt van de volgende 10 onderdelen

	Zeer onverstandig	Onverstandig	Neutraal	Verstandig	Zeer verstandig
Email					
1. Het gebruik van meerdere email adressen.					
2. Het vercijferen van je email zodat anderen je digitale post niet kunnen lezen.					
Besturingssystemen					
3. Het gebruik van verouderde besturingssysteem zoals Windows 2000 die niet meer worden ondersteund door de leverancier.					
4. Back-up maken van mijn gegevens.					
Wachtwoorden					
5. Het kiezen van voor de hand liggende wachtwoorden zoals je geboortedatum					
6. Overal gebruik maken van één dezelfde wachtwoord					
Virussen					
7. Het nemen van anti-virus maatregelen zoals installeren van een firewall					
8. Het gebruik maken van anti-spyware software					
Online bankieren en betalen					
9. Extra goed opletten wanneer je je bankzaken online regelt op een publieke computer					
10. Het direct doorgeven van opvallende transacties aan je bank					

Opleiding:

Studiejaar:

Leeftijd:

Geslacht: Man / Vrouw

Ik maak … uur per week gebruik van een computer.

- o 0 tot 2 uur
- o 3 tot 5 uur
- o 6 tot 9 uur
- o 10 tot 19 uur
- o 20 of meer uur

Mijn kennis en vaardigheden ten aanzien van Informatie- en Communicatietechnologie beoordeel ik met het rapportcijfer:

- o (1) (2) (3) (4) (5) (6) (7) (8) (9) (10)

In hoeverre is aandacht besteed aan informatiebeveiliging tijdens je studie?

- o Heel veel
- o Veel
- o Voldoende
- o Weinig
- o Helemaal niet