TOEGANGSBEVEILIGING EN PUBLIEKE NETWERKEN

Een model voor een doelmatige en pragmatische aanpak

TOEGANGSBEVEILIGING EN PUBLIEKE NETWERKEN

Een model voor een doelmatige en pragmatische aanpak

A.D. (Ton) Swieb

9 mei 2005

status Final
versie 1.0
interne toets Steven Debets

Inhoudsopgave

Voorwoord

Rotterdam, 9 mei 2005

Deze scriptie is geschreven als afsluiting van het doctoraal examen van de studie Informatica & Economie aan de Erasmus Universiteit. Het schrijven van deze scriptie was een grote uitdaging en het voltooien hiervan heeft een hoop moeilijke momenten opgeleverd.
Gelukkig heb ik kunnen rekenen op de steun van een heleboel mensen die ieder op hun eigen manier hun bijdrage hebben geleverd. In het bijzonder zou ik willen bedanken:
Jan van den Berg en Steven Debets die als begeleiders mij ondanks de lange duur van mijn afstudeertraject bleven ondersteunen.
Mijn ouders voor het scheppen van de mogelijkheid om te kunnen studeren en voor hun onvoorwaardelijke steun bij te maken keuzes.
Suzanne voor de noodzakelijke mentale ondersteuning en het geduld.

Ton Swieb

1 Inleiding

Steeds vaker stellen organisaties hun informatievoorziening, via publieke netwerken, open voor externe partijen, zoals klanten of partners, of maken organisaties hun informatievoorziening toegankelijk voor medewerkers die zich elders bevinden. Voorbeelden hiervan zijn:

- Klanten die via het Internet orders kunnen plaatsen en de orderstatus van de door hun bestelde producten kunnen volgen.
- Partners die via het Internet informatie kunnen inzien en wijzigen van de door hun geleverde producten en diensten.
- Ambulante medewerkers die op locatie over dezelfde informatie moeten kunnen beschikken en toegang moeten hebben tot dezelfde informatiesystemen als hun collegae binnen de organisatie.

Echter, zodra organisaties de informatievoorziening toegankelijker gaan maken voor klanten, partners en medewerkers wordt deze informatievoorziening dit automatisch ook voor ongewenste partijen. Door middel van toegangsbeveiliging houdt men controle over wie wel en wie geen toegang krijgt tot de informatiesystemen van een organisatie. Toegangsbeveiliging lijkt eenvoudig om te realiseren, maar de praktijk leert dat dit niet het geval is. Er zijn hulpmiddelen om aspecten van toegangsbeveiliging, zoals identificatie, authenticatie en autorisatie, goed in te richten of te verbeteren, maar welke van deze middelen zijn zinvol om toe te passen? Welke aanpak op beheersmatig vlak is wenselijk?
Zijn de verschillende middelen en aanpakken in lijn met de organisatiedoelstellingen? Organisaties benaderen het onderwerp toegangsbeveiliging verschillend. We zien daarbij aanzienlijke verschillen in de autorisatiestructuur (van zeer eenvoudig tot rol gebaseerd), in de plaatsen waar toegangsbeveiliging wordt geïmplementeerd (besturingssystemen, database management systemen, applicaties, speciale toegangsbeveiliging 'raamwerken', firewalls etc.), in de inrichting van het proces om autorisatie te beheersen en ten slotte in de zwaarte en mate van standaardisatie van authenticatie middelen. De verschillen in aanpak van de verschillende organisaties suggereren dat verschillende situaties om verschillende inrichting van toegangsbeveiliging vragen. De verschillende aanpakken zijn echter niet duidelijk onderscheiden in literatuur en praktijk en de criteria om te kiezen voor de ene of de andere aanpak zijn ook niet helder.
In deze scriptie wordt geprobeerd een antwoord te geven op bovenstaande vragen. Deze vragen kunnen worden samengevat in een probleemstelling die in §1.3 wordt toegelicht. Allereerst wordt in het kort ingegaan op de ontwikkeling van ICT en de gevolgen die dit heeft voor de organisatie aangezien een aantal ontwikkelingen een grote invloed heeft op de inrichting van toegangsbeveiliging. Daarnaast wordt in het kort aangegeven waarom deze scriptie over toegangsbeveiliging gaat. Waarom is dit een interessant onderwerp voor een scriptie?

1.1 Ontwikkeling van de informatievoorziening en de gevolgen voor de organisatie

In de afgelopen decennia heeft de informatievoorziening van organisaties grote veranderingen ondergaan [1]:

- grotere organisaties stapten over van mainframes naar client-server omgevingen.
- kleinere organisatie begonnen met automatisering door de opkomst van de PC.

- organisatienetwerken, LAN's en WAN's, werden gecreëerd door het onderling koppelen van PC's binnen organisaties.
- wereldwijde netwerken werden gecreëerd, zoals het Internet, door het onderling koppelen van organisatienetwerken.
- de informatievoorziening van organisaties werd toegankelijk gemaakt over het Internet voor klanten, partners en medewerkers.

Organisaties hebben door bovenstaande ontwikkelingen veel meer mogelijkheden gekregen in de bedrijfsvoering. Zo ontstond door de invoering van de client-server omgeving binnen grote organisaties een flexibelere, goedkopere en toegankelijkere automatiseringsomgeving voor de medewerkers van de organisatie. De opkomst van de PC binnen kleinere organisaties stelden deze bedrijven in staat om tijdrovende processen te automatiseren. De opkomst van LAN's, WAN's en het Internet zorgden voor de mogelijkheid informatie uit te wisselen en informatie toegankelijker te maken. Als laatste zorgt het toegankelijk maken van de informatievoorziening via het Internet voor het gemakkelijker opnemen van informatie in processen van partners, leveranciers en klanten en kunnen ambulante medewerkers makkelijker beschikken over benodigde informatie.

Naast de voordelen hebben bovenstaande ontwikkelingen ook een hoop nadelen en risico's met zich meegebracht. Een aantal zal hier worden aangestipt:

Verandering van de rol van de informatievoorziening

De ontwikkelingen binnen de informatievoorziening zorgen voor een veranderende rol van de informatievoorziening ten aanzien van de organisatie. Waar in het verleden de informatievoorziening voornamelijk werd gebruikt door bepaalde afdelingen voor specifieke taken, wordt de informatievoorziening nu door de gehele organisatie gebruikt en in sommige gevallen zelfs door partners, klanten en leveranciers. Dit veroorzaakt:

- een intensiever gebruik van de informatievoorziening door de organisatie welke ook een grotere mate van afhankelijkheid van de informatievoorziening creëert. Deze toenemende afhankelijkheid wordt nog eens onderstreept door het feit dat de informatievoorziening steeds meer wordt gebruikt bij kritieke bedrijfsprocessen. Waar er in het verleden sprake was van ondersteuning aan het primaire proces, vormt de informatievoorziening nu steeds meer een onderdeel van het primaire proces.
- risico met betrekking tot de betrouwbaarheid van informatie. Doordat iedereen toegang heeft tot de informatievoorziening is het gevaar groot dat gebruikers toegang krijgen tot informatie die niet voor hen bedoeld is. Een nauwkeurig onderscheid naar welke informatie voor wie toegankelijk dient te zijn is noodzakelijk.

Explosief stijgende kosten voor de informatievoorziening

Het gebruik van de informatievoorziening door de gehele organisatie zorgt voor een toenemende kostenpost. Waar de informatievoorziening in het verleden het domein was van een groepje specialisten, heeft de informatievoorziening nu ook de aandacht van het management. Er dienen keuzes gemaakt te worden in welke onderdelen van de informatievoorziening wel en in welke onderdelen van de informatievoorziening niet wordt geïnvesteerd. Veelal blijven uitgaven voor informatiebeveiliging achter.

Toenemende complexiteit[1]

De groei van de informatievoorziening binnen organisaties werd voornamelijk beïnvloed door:

- Nieuwe ontwikkelingen op het gebied van de informatievoorziening
- Eisen van de gebruikers aan de informatievoorziening

Nieuwe ontwikkelingen werden veelal gekoppeld met de bestaande informatievoorziening. Hierdoor is binnen veel organisaties een informatievoorziening ontstaan die bestaat uit heterogene netwerken, systemen en applicaties. Deze heterogeniteit heeft gezorgd voor een toenemende complexiteit van de informatievoorziening:

- Sterke groei van het aantal gebruikers van de informatievoorziening.
- Gebruikers die voor elk systeem of elke applicatie apart moeten inloggen.
- Gegevens die op meerdere plaatsen en op verschillende manieren zijn vastgelegd.
- Netwerken, systemen en applicaties die op allerlei manieren met elkaar zijn gekoppeld.

Door deze toegenomen complexiteit zijn de beheerswerkzaamheden explosief toegenomen en veroorzaakt dit risico voor het in stand houden van de betrouwbaarheid van de informatievoorziening.

Van kasteel naar hotel [2]

De eerste netwerken van organisaties, LAN's en WAN's hadden als voornaamste doel de medewerkers van de organisatie toegang te geven tot de informatievoorziening. Met de opkomst van het Internet wordt de doelgroep van de informatievoorziening uitgebreid met klanten en partners. Hierdoor vervaagt de grens van het organisatienetwerk. Waar dit in het verleden een scherp afgebakend gebied was, LAN of WAN, omvat dit nu het gehele Internet. Dit brengt grotere risico's met zich mee betreffende de informatiebeveiliging. Er zijn meerdere toegangspunten naar het netwerk en de gebruiker is steeds vaker onbekend. Het organisatienetwerk uit het verleden kan gezien worden als een kasteel waarvan de toegangspoort zwaar beveiligd wordt en waar men (grotendeels) ongemoeid wordt gelaten zodra men zich binnen de kasteelmuren bevindt. Doordat steeds meer toegangspoorten naar de buitenwereld worden gecreëerd is dit een onhoudbare situatie. Het huidige netwerk zou meer gezien moeten worden als een hotel, waar mensen in en uit lopen. In zo'n "hotel" zijn bepaalde gebieden algemeen toegankelijk zijn en bepaalde gebieden niet, waarbij de gebruiker in de algemene gebieden veelal onbekend is. Zodra men zich wil bevinden in afgeschermd gebied, zoals een hotelkamer, dient men zich te registreren.

1.2 Actualiteit van toegangsbeveiliging

Uit de voorgaande paragraaf is gebleken dat de ontwikkelingen in de informatievoorziening en mogelijkheden die daarmee worden gecreëerd problemen en risico met zich meebrengen. Met behulp van toegangsbeveiliging kan een bijdrage geleverd worden aan het oplossen van deze problemen en het inperken van het risico. Door middel van toegangsbeveiliging kan namelijk bepaald worden wie wel en wie niet toegang krijgt tot bepaalde informatie. De techniek en de kennis voor goede toegangsbeveiliging is echter al geruime tijd voorhanden. Binnen bijna elke organisatie wordt toegangsbeveiliging gebruikt voor het beveiligen van de informatie. Is daarom het onderwerp toegangsbeveiliging nog wel actueel? Het antwoord op deze vraag blijkt uit het feit dat de techniek en de kennis voor goede toegangsbeveiliging al jaren beschikbaar is, maar organisatie er toch niet

in slagen om hun informatie optimaal te beschermen. Zo blijkt namelijk uit een onderzoek van de CSI en de FBI [3] uit 2003 dat 56% van de toen ondervraagde bedrijven ongeautoriseerd gebruik van de informatievoorziening in de afgelopen 12 maanden hadden geconstateerd. Verder blijkt uit een onderzoek van KPMG Information Risk Management [4], naar aanleiding van de vraag hoe organisaties omgaan met de toegang tot hun geautomatiseerde informatiesystemen, dat organisaties de toegang tot hun informatiesystemen onvoldoende beheren. In ruim de helft van de organisaties ontbreekt een actueel beeld van de toegangsrechten van medewerkers tot de verschillende systemen en vindt ook geen periodieke controle plaats. Bij een gering aantal organisaties wordt één centraal systeem gehanteerd waarin de autorisaties worden beheerd. Bij de meeste organisaties gebeurt dit echter in een veelvoud van systemen, waardoor het overzicht ontbreekt. Daarnaast wordt binnen 70% van de organisaties wachtwoorden en toegangspasjes door medewerkers gedeeld en 40% van de organisaties vindt dat de medewerkers over teveel autorisaties beschikken.
Het feit dat het merendeel van de organisaties hun toegangsbeveiliging niet op orde hebben of moeite hebben om hun toegangsbeveiliging op orde te krijgen, maakt toegangsbeveiliging een actueel onderwerp.

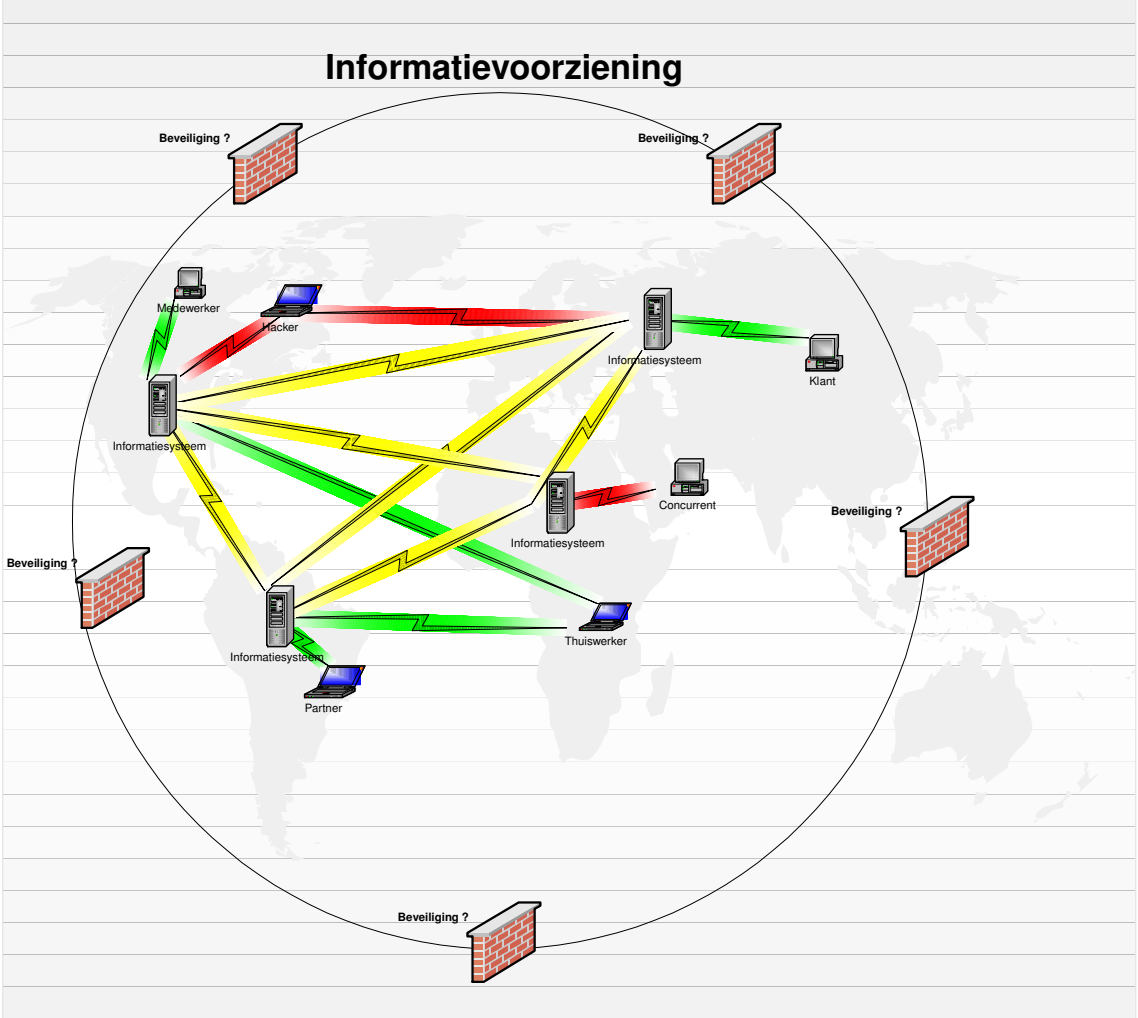
1.3 Probleemstelling

Er zijn meerdere oorzaken te bedenken waarom organisaties moeite hebben met het inrichten van hun toegangsbeveiliging. Greg Young van Gartner [5] geeft hiervoor onder andere als reden dat nieuwe technologie verstorend werkt. Omdat nieuwe technologieën elkaar in rap tempo opvolgen haalt men niet het gewenste niveau van beveiliging en neemt men genoegen met een lager niveau van beveiliging. Nieuwe technologieën worden vaak al geïntroduceerd voordat de beveiliging die daarvoor nodig is, volledig is uitgekristalliseerd. Tijd om vervolgens de beveiliging te optimaliseren is er niet omdat dan de volgende nieuwe technologie al weer zijn intrede doet die beveiligd moet worden. Nederlandse managers constateren dit nu ook zoals blijkt uit een onderzoek van de Giarte Media Group[6]. Zij zien de verandering in de IT-architectuur als een belangrijke factor voor verhoogde aandacht voor informatiebeveiliging van hun kant.

Eén van die grote veranderingen in de IT-architectuur die van invloed is op toegangsbeveiliging is de overgang van een informatievoorziening die wordt gebruikt als een “kasteel” naar een informatievoorziening die wordt gebruikt als een “hotel”. Deze verandering in gebruik van de informatievoorziening dient vergezeld te worden van passende toegangsbeveiliging om de betrouwbaarheid van de informatie te kunnen blijven waarborgen. Waar in het “kasteel” model er maar enkele toegangspunten waren die beveiligd dienden te worden en de gebruiker veelal bekend was, is dit in het “hotel” model niet het geval. De gebruiker is, door de verweving van de informatievoorziening met het Internet, veelal onbekend, maar hij/zij wil toch toegang tot de informatievoorziening. Waar moet de inrichting van toegangsbeveiliging aan voldoen om zo’n soort omgeving goed te kunnen beveiligen en beheersen? Dat is het onderwerp van deze scriptie.
De probleemstelling is als volgt:

Wat is adequate toegangsbeveiliging voor een informatievoorziening die toegankelijk is via publieke netwerken?

Deze probleemstelling is grafisch weergegeven in figuur 1. Hierin is te zien dat het niet meer mogelijk is om een gebied af te bakenen waarbinnen alleen de informatievoorziening en alleen de gebruikers van deze informatievoorziening zich bevinden. Ook onbevoegde gebruikers bevinden zich vaak binnen dit gebied. Dit vraagt om een andere manier van beveiligen.



Figuur 1: grafische weergave van probleemstelling.

1.4 Opbouw scriptie

Het vinden van een antwoord op de bovenstaande probleemstelling is niet eenvoudig. Niet voor niets hebben organisaties nog steeds moeite met het goed inrichten van hun toegangsbeveiliging. Een hulpmiddel voor het vinden van een antwoord kan een model zijn. Een model dient om de weergave van de werkelijkheid enigszins te vereenvoudigen om zo makkelijker te komen tot een antwoord. In deze scriptie zal een model worden opgesteld dat als hulpmiddel kan dienen bij het vinden van een antwoord op de probleemstelling en dus organisaties kan helpen bij het inrichten van hun toegangsbeveiliging. Voordat dit model in hoofdstuk 5 wordt behandeld zal allereerst wat achtergrond informatie worden gegeven. In hoofdstuk 2 wordt uitgelegd wat informatiebeveiliging is. Het probleemgebied is een subonderdeel van informatiebeveiliging en in hoofdstuk 3 worden de

begrippen die hiermee te maken hebben toegelicht. In hoofdstuk 4 wordt vervolgens ingegaan op de noodzaak voor het opstellen van een model en wordt gekeken naar de randvoorwaarden voor het op te stellen model. In hoofdstuk 6 volgt een toetsing van het model aan de praktijk. Uiteindelijk worden in hoofdstuk 7 conclusies getrokken over de inzetbaarheid van het model.

2 Informatiebeveiliging

Het onderwerp van deze scriptie bevindt zich op het gebied van toegangsbeveiliging. Toegangsbeveiliging is een specifiek onderdeel van het meer omvattende gebied: informatiebeveiliging. Voor een goed begrip van toegangsbeveiliging wordt in dit hoofdstuk informatiebeveiliging behandeld. In dit hoofdstuk wordt uitgelegd waarom we informatie moeten beveiligen en misschien nog wel belangrijker hoe we informatie kunnen beveiligen.

2.1 Waarom informatie beveiligen?

Het werken met gegevens speelt een cruciale rol in elke organisatie. Voor tal van organisaties is het verwerken van gegevens zelfs het belangrijkste proces. Voorbeelden van relevante gegevens zijn:

- Personeelsgegevens
- Klantengegevens
- Leveranciersgegevens
- Financiële gegevens
- Marktgegevens
- Correspondentie

Gegevens zijn nodig voor het correct functioneren van diverse processen binnen een organisatie. Hierdoor hebben gegevens een bepaalde waarde voor een organisatie. Deze waarde hangt volgens Overbeek [7] onder andere af van:

- De *onmisbaarheid* van gegevens voor diverse processen. De mate waarin een proces afhankelijk is van de gegevens heeft invloed op de waarde van deze gegevens.
- Het *belang* van het proces voor de organisatie. Des te belangrijker het proces, des te meer waarde de gegevens hebben die voor dit proces noodzakelijk zijn.
- De *herstelbaarheid*: de mate waarin ontbrekende, incomplete, of onjuiste gegevens gereproduceerd, respectievelijk hersteld, kunnen worden.

Naast het belang van gegevens voor het correct functioneren van processen binnen een organisatie kan er ook een belang op een ander vlak uit de gegevens voortvloeien:

- Gegevens kunnen een belang vertegenwoordigen voor anderen, bijvoorbeeld persoongegevens.
- Gegevens kunnen concurrentiegevoelig zijn.

Gegevens, “een objectief waarneembare weerslag van feiten in een drager” [7], zijn waardevol voor een organisatie. De betekenis die de mens, aan de hand van bepaalde afspraken aan gegevens, toekent aan de informatie of de kennistoename die, door het verwerken van deze gegevens, ontstaat, is echter van een nog grotere waarde voor organisatie. Het verwerken van gegevens tot informatie kan met behulp van een informatiesysteem. “Een informatiesysteem (IS) is een samenhangende gegevensverwerkende functionaliteit die kan worden ingezet om één of meer bedrijfsprocessen te kennen, te ondersteunen, of te besturen. Een informatiesysteem kan de volgende componenten bevatten: apparatuur, programmatuur, gegevens, procedures en mensen.” [7] Alle informatiesystemen van de organisatie samen vormt de informatievoorziening (IV) van de organisatie.

Informatie wordt, naast kapitaal, grondstof en arbeid, ook wel gezien als de vierde productiefactor van een organisatie. Elke organisatie heeft informatie nodig voor de bedrijfsvoering. Informatie is nodig voor het nemen van beslissingen, het aansturen van de productie. Voor veel organisaties is het leveren van informatie zelfs hun kernactiviteit. Analoog aan het belang van gegevens voor de organisatie kan voor informatie over dezelfde belangen gesproken worden. Om deze belangen weer te geven, wordt in de informatiebeveiliging gebruik gemaakt van betrouwbaarheidskenmerken:

- *Beschikbaarheid* (B): De mate waarin informatie of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers.
- *Integriteit* (I): De mate waarin informatie of functionaliteit juist ingevuld is.
- *Vertrouwelijkheid* (V): De mate waarin de toegang tot informatie of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Deze betrouwbaarheidskenmerken zijn van toepassing op de gehele informatievoorziening. Deze kenmerken kunnen dus zoal betrekking hebben op informatiesystemen, informatie en gegevens. Het belang van de informatievoorziening voor een organisatie is groot. Echter de informatievoorziening is onderhevig aan bedreigingen. “Een *bedreiging* is een proces of een gebeurtenis die in potentie een verstorende invloed heeft op de betrouwbaarheid van een object. In het kader van informatiebeveiliging betreft het dan objecten van de informatievoorziening: apparatuur, programmatuur, gegevens, procedures en mensen.” [7] In welke mate de informatievoorziening gevoelig is voor bedreigingen hangt af van de kwetsbaarheid van de informatievoorziening voor een bepaalde dreiging. Zo is bijvoorbeeld een computer (het object), die verbonden is met het Internet, kwetsbaar voor het verkrijgen van toegang tot de computer via het Internet (de dreiging), terwijl een computer die niet met het Internet verbonden is hiervoor niet kwetsbaar is. De kwetsbaarheid van objecten voor diverse dreigingen is moeilijk kwantitatief weer te geven. Vaak is het wel mogelijk om een globale rangorde te maken van de diverse dreigingen, die een object ondervindt, op basis van de kwetsbaarheid. Doordat de informatievoorziening kwetsbaar is voor bepaalde dreigingen bestaat het gevaar dat deze kwetsbaarheden leiden tot verstoringen van de informatievoorziening waardoor de betrouwbaarheid van de informatievoorziening wordt aangetast. Doordat de betrouwbaarheid van de informatievoorziening wordt aangetast kan de organisatie schade ondervinden.

De schade kan al dan niet financieel van aard zijn en omvat:

- De directe schade aan rechtstreekse getroffenen, zoals personen, apparatuur, programmatuur, gegevensverzamelingen en gebouwen.
- De indirecte schade, oftewel de gevolgschade, zoals verstoring van bedrijfsprocessen, het overtreden van wetten, verlies van opdrachten en imagoschade.

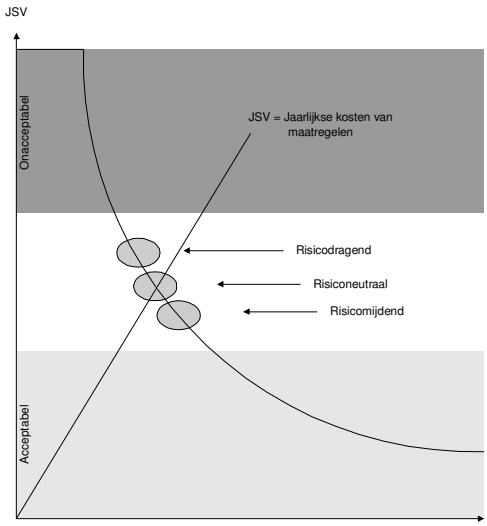
De “kans op schade” vermenigvuldigt met “de omvang van de schade” kan gezien worden als het risico dat de organisatie loopt.
Samengevat is het risico dat een organisatie loopt afhankelijk van:

- Het aantal dreigingen waarvoor de objecten van de informatievoorziening kwetsbaar zijn.
- De kans dat een bedreiging optreedt en een verstoring veroorzaakt.
- De verwachte schade die optreedt indien een verstoring plaatsvindt.

Het risico dat de organisatie loopt kan wel of niet wenselijk zijn. Door de informatievoorziening te beveiligen kan dit risico worden ingeperkt, maar hier zijn kosten aan verbonden.
De organisatie zal een evenwicht moeten vinden tussen de kosten die gemaakt moeten worden voor het beveiligen van de informatievoorziening en het risico dat men loopt. Zo kan de organisatie zich:

- risiconeutraal opstellen: men maakt evenveel kosten voor beveiliging dan dat men risico loopt.
- risicodragend opstellen: men maakt minder kosten voor beveiliging dan dat men risico loopt.
- risicomijdend opstellen: men maakt meer kosten voor beveiliging dan dat men risico loopt.

Dit is schematisch weergegeven in figuur 2.



Figuur 2: De relatie tussen schadeverwachting en kosten van maatregelen

2.2 Hoe informatie te beveiligen

Door middel van maatregelen kan men de informatievoorziening beveiligen. Er zijn diverse maatregelen die men kan toepassen. Het op goed geluk implementeren van maatregelen, levert zo goed als zeker een set maatregelen op die niet effectief is. Voor het vinden van een samenhangend pakket beveiligingsmaatregelen is inzicht nodig in de werking van maatregelen en de onderlinge relaties tussen maatregelen. In §2.2.1 wordt de verschillende werkingen van maatregelen en de onderlinge relaties tussen maatregelen toegelicht. Nadat een goede set maatregelen gevonden is, is men nog niet klaar. Zowel de organisatie als de omgeving van de organisatie is continue aan verandering onderhevig. Deze veranderingen hebben invloed op het risico dat de organisatie, met betrekking tot de informatievoorziening, loopt. Informatiebeveiliging is daarom een proces. De set met maatregelen dienen continue te worden bijgesteld. Het proces informatiebeveiliging wordt verder behandeld in §2.2.2. Aan het implementeren en continue bijstellen van maatregelen zitten kosten verbonden voor de organisatie. Nadat men bekend is met de werking van maatregelen en hun onderlinge relaties en bekend is met het proces informatiebeveiliging moet men overgaan tot het selecteren van een set maatregelen die geschikt is voor de desbetreffende organisatie. Dit is een moeilijke, tijdrovende en kostbare opgave en hiervoor zijn diverse hulpmiddelen ontwikkeld om organisatie te ondersteunen. Deze hulpmiddelen worden verder behandeld in §2.2.3.

2.2.1 Beveiligingsmaatregelen

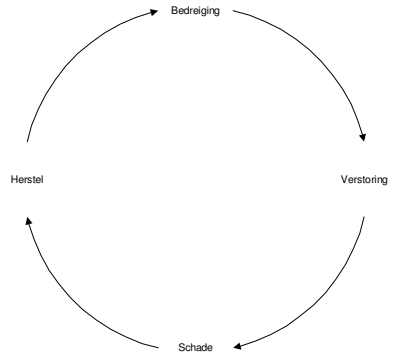
Overbeek [7] onderkent drie wegen waarlangs beveiligingsmaatregelen kunnen worden ingedeeld:

- Indeling op basis van de incidentcyclus
- Indeling naar de wijze waarop beveiligingsmaatregelen worden gerealiseerd.
- Indeling naar het aspect (beschikbaarheid, integriteit, vertrouwelijkheid) dat ze beveiligen.

Indeling op basis van de incidentcyclus

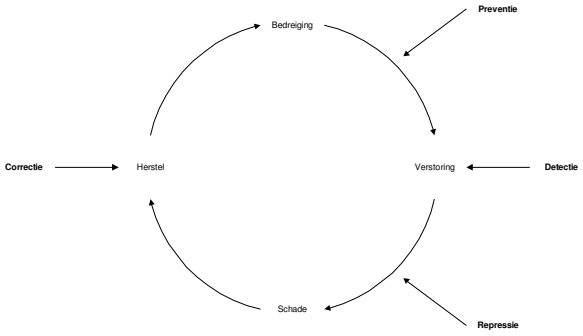
De incidentcyclus beschrijft de stappen die plaatsvinden rondom het optreden van een beveiligingsincident. De cyclus bestaat uit vier elkaar opvolgende stappen, zie figuur 3. Dit zijn:

- Bedreiging: iets dat zou kunnen gebeuren.
- Verstoring: een verwezenlijking van een bedreiging oftewel een beveiligingsincident.
- Schade: de gevolgen veroorzaakt door de verstoring.
- Herstel: het ongedaan maken van de schade.



Figuur 3: De incidentcyclus

Voor de indeling van de beveiligingsmaatregelen wordt op basis van de incidentcyclus een beveiligingscyclus afgeleid, zie figuur 4. Hierin staan de verschillende soorten beveiligingsmaatregelen ingedeeld naar waar zij aangrijpen in de incidentcyclus.



Figuur 4: De beveiligingscyclus

Dit zijn:

- **Preventieve maatregelen**[1][ADS1]
  Preventieve maatregelen zijn maatregelen die tot doel hebben te voorkomen dat bedreigingen tot een verstoring leiden. Preventieve maatregelen kunnen weer onderverdeeld worden in permanente maatregelen en getriggerde maatregelen. Permanente maatregelen zijn continue inwerking, zonder dat ze opgestart hoeven te worden, bijvoorbeeld de aanwezigheid van brandblusserinstallaties in computerruimtes. Getriggerde maatregelen treden pas in werking nadat een detectieve maatregel daartoe aanleiding geeft of nadat de maatregel handmatig in werking wordt gesteld.

- **Detectieve maatregelen**
  Detectieve maatregelen zijn op zichzelf niet werkzaam. Detectieve maatregelen kunnen alleen effectief zijn in combinatie met een of meer getriggerd-preventieve of repressieve maatregelen. Een voorbeeld van een detectieve maatregel is het gebruik van een IDS, Intrusion Detection System. De IDS slaat alarm zodra deze verdachte communicatie met de informatievoorziening waarneemt.

- **Repressieve maatregelen**
  Repressieve maatregelen zijn tweedelijns-maatregelen en hebben tot doel de negatieve invloed van een verstoring te minimaliseren, indien de preventieve maatregelen een verstoring niet hebben kunnen voorkomen. Bijvoorbeeld het opschonen van, met virussen, geïnfecteerde bestanden.

- **Correctieve maatregelen**
  Correctieve maatregelen richten zich op het herstel van de objecten die bij een incident beschadigd zijn. In feite zijn dit geen beveiligingsmaatregelen, maar onderhoudsmaatregelen.

Indeling naar de wijze waarop beveiligingsmaatregelen worden gerealiseerd

Beveiligingsmaatregelen kunnen op verschillende manieren worden gerealiseerd en werkzaam zijn op verschillende objecten. Aan de hand hiervan kunnen de beveiligingsmaatregelen worden ingedeeld in:

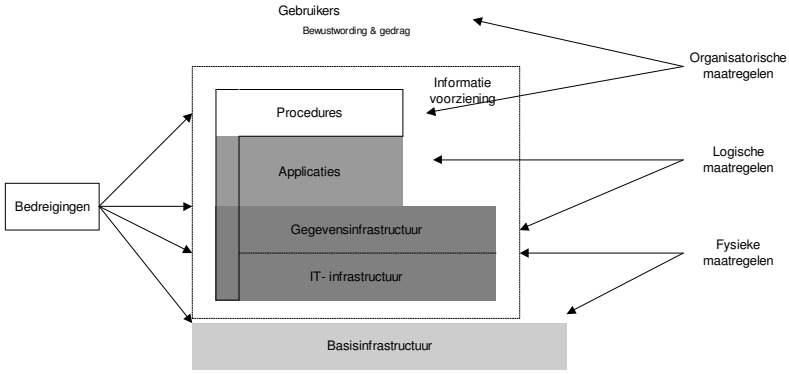
- **Organisatorische maatregelen**
  Organisatorische maatregelen zijn maatregelen die betrekking hebben op de organisatie als geheel en werkzaam zijn op menselijke en organisatorische zaken. Hieronder vallen het formuleren van het beveiligingsbeleid, richtlijnen en procedures.

- **Logische maatregelen**
  Logische maatregelen zijn maatregelen die geprogrammeerd zijn in programmatuur en werkzaam zijn op gegevensverzamelingen en programmatuur, zoals applicaties en de programmatuurdelen van infrastructuren.

[1] Wat een repressieve maatregel is voor het ene incident kan weer een preventieve maatregel zijn voor het andere incident.

- **Fysieke maatregelen**
  Fysieke maatregelen zijn maatregelen die gebaseerd zijn op apparatuur of andere materiele zaken en werkzaam zijn op de apparatuurdelen van de infrastructuur.

Het bovenstaande is schematisch weergegeven in figuur 5.



Figuur 5: Beveiligingsmaatregelen en hun werkingsgebied

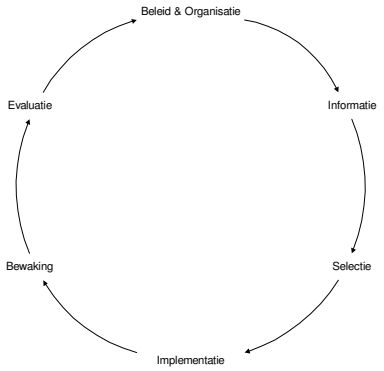
Indeling naar het aspect dat ze beveiligen

Informatiebeveiliging draait in essentie om de aspecten beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Elke beveiligingsmaatregel moet dus betrekking hebben op één of meer van deze aspecten. Indelen van beveiligingsmaatregelen naar deze aspecten is dus niet onlogisch.

2.2.2 Het proces informatiebeveiliging

Informatiebeveiliging is een proces dat kan worden opgedeeld in een aantal elkaar opvolgende stappen (zie figuur 6):

- Het formuleren van een beleid ten aanzien van informatiebeveiliging en het inrichten van de organisatie die verantwoordelijk is voor informatiebeveiliging.
- Het opsporen van onacceptabele risico's en het zoeken van maatregelen die de risico's kunnen reduceren.
- Het selecteren van een pakket maatregelen.
- Het implementeren van de geselecteerde maatregelen.
- Het evalueren van het effect dat met de getroffen maatregelen bereikt wordt.



Figuur 6: De informatiebeveiligingscyclus

De omgeving waarop informatiebeveiliging zich richt is voortdurend aan verandering onderhevig. Zo kunnen de risico's veranderen evenals de eisen en randvoorwaarden die de organisatie aan informatiebeveiliging stelt. Informatiebeveiliging is daarom een continue terugkerend proces. De cirkel, zoals weergegeven in figuur 6, dient dus telkens opnieuw te worden doorlopen.

2.2.3 Hulpmiddelen voor het inrichten van informatiebeveiliging

Informatie representeert waarde voor een organisatie. Dit dient beschermd te worden tegen allerlei dreigingen. Voor het inschatten van risico's die ondervonden worden, wordt gebruik gemaakt van een risicoanalyse. Risicoanalyses zijn er in verschillende soorten en maten. Diverse risicoanalyse methodes en hun verschillen zijn het onderwerp van deze paragraaf.
Grofweg kunnen de risicoanalyse methodes in twee groepen worden ingedeeld. Aan de ene kant zijn er de methodes op basis van de standaardbenadering en aan de andere kant zijn er de methodes gebaseerd op een maatwerkbenadering. Elk met hun eigen voor- en nadelen.

Risicoanalyse methodes op basis van een standaardbenadering

Deze methodes zijn veel gebaseerd op checklists waarin een lijst met standaard maatregelen is opgenomen. Het geheel van standaard maatregelen vormt samen de beveiligingsnorm die door de checklist wordt nagestreefd. In de eenvoudigste vorm is de nagestreefde norm een externe norm en wordt de risicoanalyse methode een *quick scan* genoemd. In een wat uitgebreidere vorm is de nagestreefde norm een intern opgestelde norm, eventueel afgeleid van een externe norm, en spreekt men van een *baseline checklist*.
Voordelen van deze risicoanalyse methodes zijn:

- Checklists zijn makkelijk en goedkoop toe te passen.
- Het toepassen van checklist geeft een vergelijkingskader.

Nadelen van deze risicoanalyse methodes zijn:

- Te algemeen en dus niet op alles en iedereen toepasbaar.
- De ontwikkelingen in de ICT staan niet stil, dus de checklists verouderen snel.

Risicoanalyse methodes op basis van een maatwerkbenadering

Deze methodes zijn niet gebaseerd op standaard lijstjes, maar op grondig onderzoek van de afhankelijkheid en kwetsbaarheid van een object. Aangezien haast geen enkel object dezelfde risico's ondervindt, wordt door middel van een maatwerkbenadering de risico's veel nauwkeuriger bepaald. Het bepalen van het risico kan in het eenvoudigste geval gebeuren door gebruik te maken van een kwalitatieve analyse en in het uitgebreidste geval door gebruik te maken van kwantitatieve analyse. Bij kwantitatieve analyse wordt getracht om voor elk object het risico te berekenen waar bij kwalitatieve analyse volstaan wordt met een schatting.
Een groot voordeel van deze vorm van risicoanalyse is:

- Een nauwkeurigere inschatting van de risico's is mogelijk.

Nadelen van deze vorm van risicoanalyse zijn:

- Het uitvoeren van deze vorm van analyse is complex, duur en tijdrovend.
- Er kan een overvloed aan informatie ontstaan op basis waarvan het management beslissingen moet nemen.

De standaard risicoanalyse benadert het informatiebeveiligingsprobleem dus door middel van het nastreven van een norm. Hierbij wordt niet gekeken naar de individuele afhankelijkheden en kwetsbaarheden van de diverse objecten. Het gevolg is dat de objecten in kwestie voldoen aan een norm, maar het blijft natuurlijk de vraag of die norm goed gesteld is. Indien de norm te hoog gesteld is worden er onnodige investeringen gedaan in informatiebeveiliging en indien de norm te laag gesteld is wordt er onnodig risico gelopen. De risicoanalyse op maat heeft dit probleem echter niet.

Focus van de risicoanalyse

Naast te kijken naar het soort risicoanalyse dat wordt toegepast is het net zo van belang om te kijken wat de focus van de risicoanalyse is. Een risicoanalyse kan namelijk op verschillende objecten worden uitgevoerd. Zo kan een risicoanalyse zich meer richten op de bedrijfsprocessen of juist meer op de techniek. Objecten die onderwerp van risicoanalyse kunnen worden, zijn bijvoorbeeld:

- De organisatie
- Het bedrijfsproces
- Het informatiesysteem
- De applicatie

Afhankelijk van het soort object dat onderwerp is van de risicoanalyse zullen bepaalde risicoanalyse methodes meer of minder geschikt zijn. Zo kan bij een organisatie een checklist een goed middel zijn om het beveiligingsniveau van een organisatie op een hoger peil te brengen. Met eventueel als tweede stap het onderzoeken van de kritieke bedrijfsprocessen met behulp van maatwerk risicoanalyse. Echter de gehele organisatie doorlichten met behulp van maatwerk risicoanalyse is minder geschikt. De meeste bedrijfsprocessen binnen organisaties zijn redelijk standaard en zijn terug te vinden binnen meerdere organisaties. Een algemene norm/checklist die deze bedrijfsprocessen behandelt is dan vaak voldoende.

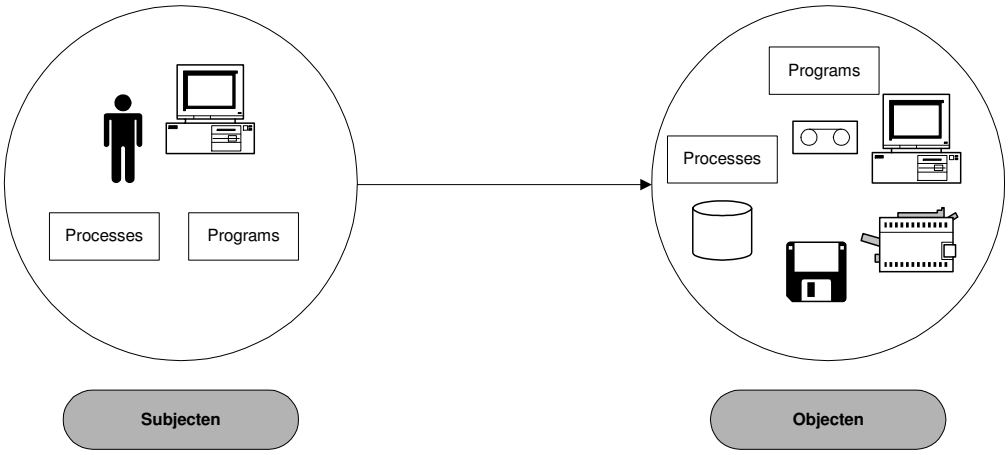
3 Toegangsbeveiliging

Informatiebeveiliging, zo is gebleken uit het vorige hoofdstuk, is een uitgebreide discipline. Het omvat het opstellen, uitvoeren en evalueren van een grote set aan maatregelen op basis van een informatiebeveiligingsbeleid. De maatregelen die hierbij aanbod komen variëren van fysieke maatregelen, zoals het installeren van brandblusserinstallaties, tot logische maatregelen, zoals het scannen op virussen, tot organisatorische maatregelen, zoals het opstellen van richtlijnen en procedures. Toegangsbeveiliging is een onderdeel van informatiebeveiliging dat, analoog aan bovenstaande, ook kan worden onderverdeeld in fysieke, logische en organisatorische maatregelen. Zo hebben fysieke toegangsbeveiligingsmaatregelen betrekking op het reguleren van de toegang naar fysieke objecten zoals: gebouwen, werkkamers, kluizen, kasten, etc. Logische toegangsbeveiligingmaatregelen hebben betrekking op het reguleren van toegang tot digitaal opgeslagen informatie, door middel van in software en hardware geprogrammeerde regelen en organisatorische toegangsbeveiligingsmaatregelen bevatten de regels, richtlijnen en procedures voor het beheren van toegangsbeveiliging.
Toegangsbeveiliging in de context van deze scriptie draait om het beveiligen van de toegang tot informatie die via digitale weg kan worden verkregen. De focus ligt hierbij dus op logische toegangsbeveiligingsmaatregelen en de daarbij behorende organisatorische maatregelen. Uiteraard hebben logische toegangsbeveiligingsmaatregelen vrijwel geen nut zonder fysieke toegangsbeveiligingsmaatregelen en in mindere mate hebben fysieke toegangsbeveiligingsmaatregelen geen nut zonder logische toegangsbeveiligingsmaatregelen. In dit hoofdstuk wordt echter niet verder ingegaan op fysieke toegangsbeveiligingsmaatregelen maar beperken we ons tot logische toegangsbeveiligingmaatregelen en de bijbehorende organisatorische logische maatregelen. Waar in het vervolg van de deze scriptie gesproken wordt over toegangsbeveiliging worden de logische maatregelen en bijbehorende organisatorische maatregelen bedoeld.
In de hierna volgende paragrafen worden de diverse soorten beveiligingsmaatregelen van toegangsbeveiliging behandeld en vervolgens wordt gekeken naar het probleem van het selecteren van de juiste toegangsbeveiligingsmaatregelen. Hoe bepaalt men welke toegangsbeveiligingsmaatregelen moeten worden gebruikt en kan hiervoor een standaardmodel worden gebruikt of niet?

3.1 Wat is toegangsbeveiliging?

In de vorige paragraaf hebben we al aangegeven dat toegangsbeveiliging bestaat uit maatregelen op het fysiek, logische en organisatorische vlak. Echter voor een beter afgebakende omschrijving van toegangsbeveiliging in de context van deze scriptie dient eerst een aantal andere dingen helder te zijn, zoals: wanneer spreken we over toegang en aan wie wordt er toegang verstrekt.
Toegang is de stroom van informatie tussen een subject en een object, waarbij een subject een actieve entiteit is die toegang vraagt tot een object of tot de data in een object en een object een passieve entiteit is die data bevat. Een actieve entiteit kan zowel een gebruiker, een programma of een proces zijn. Een passieve entiteit kan zowel een computer, een database, een bestand of een computerprogramma zijn. De verhouding tussen subjecten en objecten is in figuur 7 weergegeven. Het reguleren van de stroom van informatie tussen een subject en een object gebeurt door middel van beveiligingsmaatregelen die zijn vastgelegd in software of hardware. Aan het vastleggen van

deze maatregelen gaat een heel proces vooraf. Zo moet er bepaald worden welke subjecten toegang krijgen tot welke informatie van een bepaald object. Dit proces vindt plaats aan de hand van opgestelde regels, richtlijnen en procedures. Oftewel aan de hand van organisatorische maatregelen. Zo kan men stellen dat voor elke fysieke of logische beveiligingsmaatregel aanvullend één of meer organisatorische maatregelen nodig zijn [7].



Figuur 7: Subjecten zijn actieve entiteiten die objecten benaderen; objecten zijn passieve entiteiten

Niet voor niets wordt vaak gezegd dat informatiebeveiliging voor 80% bestaat uit regels, richtlijnen en procedures en voor 20% uit technische middelen.
Voor toegangsbeveiliging is dit niet anders, hoewel er in de meeste literatuur, als het over toegangsbeveiliging gaat, wordt gesproken over technische middelen. Echter al deze technische middelen zijn zinloos indien deze niet ingebed zijn in een goede organisatorische structuur met heldere regels en procedures. Zo kan bijvoorbeeld een financiële instelling een kluis aanschaffen die absoluut niet te kraken is, maar als de sleutel voor iedereen voor het grijpen ligt heeft de hele dure kluis weinig zin. Hetzelfde geldt voor toegangsbeveiliging.

Samenvattend zouden we informatiebeveiliging kunnen definiëren als [8]:

"Het reguleren van de stroom van informatie tussen subjecten en objecten aan de hand van logische maatregelen, die zijn ingebed als regels in hardware en software, aan de hand van organisatorische beveiligingsmaatregelen, die regels, richtlijnen en procedures omvatten voor de mensen in de organisatie, en aan de hand van diverse technische middelen die ondersteuning bieden aan de diverse beveiligingsmaatregelen."

De focus van deze scriptie ligt bij de organisatorische maatregelen van toegangsbeveiliging. Echter voor een goed begrip van toegangsbeveiliging wordt in dit hoofdstuk in het kort ingegaan op logische maatregelen van toegangsbeveiliging.

3.2 Logische maatregelen

De logische toegangsbeveiligingsmaatregelen kan men onderverdelen in drie elkaar opvolgende stappen [7]:

- Het specificeren van toegang: dit omvat het opstellen van regels voor het verlenen van toegang.
- Het verlenen van toegang: dit omvat het daadwerkelijk geven van toegang conform de specificatie
- Het bewaken van toegang: dit omvat het controleren of de verleende toegang of de te verlenen toegang correspondeert met de gespecificeerde toegang.

3.2.1 Het specificeren van toegang

Het specificeren van toegang omvat het opstellen van regels aan de hand waarvan toegang wordt verleend. In de programmatuur dient, aan de hand van regels, te worden vastgelegd aan wie toegang moet worden verleend, tot diverse objecten.
Er zijn meerdere methodes op basis waarvan systemen toegang verlenen, dit zijn:

DAC (Discretionary Access Control)

DAC is een mechanisme waarbij de eigenaar van een bepaald object de toegang voor anderen tot dit object kan verlenen of ontzeggen. Een DAC mechanisme is in het algemeen gebaseerd op een toegangsmatrix waarin aangegeven wordt wie welke toegangsrechten heeft tot een object of tot een groep van objecten.

MAC (Mandatory Access Control)

MAC is een mechanisme waarbij de gebruikers zelf geen invloed hebben op het verlenen of ontzeggen van toegang tot informatie. Zowel gebruikers als informatie wordt geclassificeerd, bijvoorbeeld van zeer geheim tot vrij toegankelijk. Hierbij heeft een gebruiker slechts toegang tot informatie uit zijn eigen classificatie of tot informatie uit een lagere classificatie, maar niet tot informatie uit een hogere classificatie.

RBAC (Role Based Access Control)

RBAC is een mechanisme waarbij toegang wordt verleend op basis van rollen. Aan elke rol, zoals de rol financieel medewerker, zijn toegangsrechten verbonden. Rollen worden vervolgens toegekend aan gebruikers.

3.2.2 Het verlenen van toegang

Het verlenen van toegang gebeurt op basis van de gespecificeerde toegangsregels die zijn vastgelegd via één van de hierboven beschreven methodes. Voor het verlenen van toegang worden de volgende stappen doorlopen [7]:

- Identificatie: Het bepalen van een identiteit.
- Authenticatie: Het verifiëren van de geclaimde identiteit.
- Autorisatie: Het toekennen van de rechten.

Identificatie

Identificatie wordt gebruikt voor het bepalen van de identiteit van een subject. Indien anoniem gebruik van de informatievoorziening niet is toegestaan dient de identiteit te worden vastgesteld alvorens een subject toegang krijgt tot de informatievoorziening. Voor dit doel beschikt het subject over een identiteit waaronder het subject bij de informatievoorziening bekend staat. De opgegeven

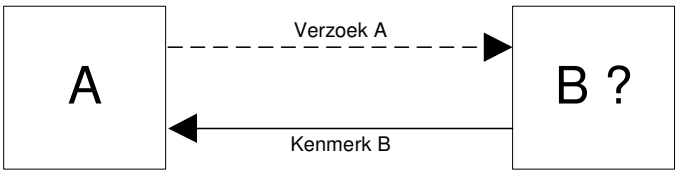
identiteit van het subject wordt vergeleken met alle identiteiten die binnen de informatievoorziening bekend zijn. Indien de opgegeven identiteit in de lijst gevonden wordt, is het subject geïdentificeerd. Voor het informatiesysteem is nu duidelijk welke identiteit van het systeem gebruik wil maken. Het probleem hierbij is dat het vaak erg gemakkelijk is om een andere identiteit op te geven. Het is dus nodig dat de identiteit niet alleen bepaald, maar vervolgens ook geverifieerd wordt. Een voorbeeld van identificatie is het intypen van een gebruikersnaam, de identiteit, om een persoon, het subject, ten overstaan van een computersysteem te identificeren.

Single Sign On

Door de wildgroei van applicaties en informatiesystemen is de complexiteit voor de gebruiker voor het verkrijgen van toegang enorm toegenomen. Elke informatiesysteem of applicatie heeft meestal zijn eigen systeem om toegang te verlenen binnen de eigen grenzen. Doordat gebruikers vaak toegang moeten hebben tot meerdere applicaties en informatiesystemen moeten zij meerdere keren een identificatie proces doorlopen. Single Sign On is een techniek waarmee dit probleem wordt ondervangen. Het doel van Single Sign On is dat een gebruiker zich maar een keer hoeft te identificeren waarna hij toegang heeft tot alle applicaties en systemen waarop toegang voor deze gebruiker is gespecificeerd. De manier waarop Single Sign On wordt geïmplementeerd verschilt per omgeving, maar dit ligt verder buiten het bereik van deze scriptie.

Authenticatie

Door middel van authenticatie kan de identiteit van een subject met enige zekerheid worden vastgesteld. Hierbij wordt gebruik gemaakt van een uniek kenmerk, dat specifiek verbonden is aan de identiteit die geverifieerd wordt. In figuur 8 is het principe van authenticatie schematisch weergegeven. A wil vaststellen of B degene is waar hij zich voor uitgeeft. Daartoe dient B een kenmerk naar A te sturen, op basis waarvan A voldoende vertrouwen heeft in de identiteit van B. Dit kan al dan niet gebeuren op initiatief van A, die daarvoor dan een verzoek naar B stuurt.



Figuur 8: Schematische weergave van authenticatie

Voor elke authenticatie is een kenmerk nodig. Bij authenticatie van een persoon bestaat dat uit een of meer persoonsgebonden gegevens. De gegevens die we daarbij kunnen onderscheiden zijn ingedeeld in drie gebieden, Overbeek[7]:

- Iets dat de persoon weet, bijvoorbeeld een wachtwoord.
- Iets dat de persoon bezit, bijvoorbeeld een sleutel, token of smartcard.
- Iets dat deel uitmaakt van de persoon / Iets dat de persoon is, bijvoorbeeld biometrische gegevens zoals een handtekening, vingerafdruk of een irisscan.

Sterke authenticatie

Voor authenticatie kan volstaan worden door één element te kiezen uit één van de drie gebieden. Dit wordt ook wel één factor authenticatie genoemd. Het vertrouwen in het authenticatiemiddel bij

één factor authenticatie mag echter niet echt groot te noemen zijn. Namelijk iets dat je weet kan misschien iemand anders ook wel te weten komen, iets dat hebt kan je kwijtraken of kan gestolen worden en iets dat je bent is op het eerste gezicht moeilijker te misbruiken, maar zeker niet onmogelijk, zie de discussie van biometrie hieronder. Er bestaat een hele range aan authenticatie middelen, waarbij sommige moeilijker zijn te misbruiken dan andere, zie de discussie van authenticatie middelen hieronder. Echter bij één factor authenticatie hoeft je maar één kenmerk te bemachtigen om vervolgens toegang te krijgen tot de informatievoorziening onder een andere identiteit. Daarom wordt, indien men zekerder wil zijn dat de identiteit gebruikt wordt door de rechthebbende, vaak gebruik gemaakt authenticatie op basis van ten minste twee kenmerken uit verschillende gebieden. Dit wordt ook wel sterke authenticatie genoemd. Een voorbeeld van sterke authenticatie is bijvoorbeeld de bankpas waarbij twee factoren worden gebruikt uit verschillende authenticatie gebieden: je bankpas (iets dat je hebt) en je pincode (iets dat je weet). Iemand die geld wil opnemen bij de geldautomaat moet zowel beschikken over de bankpas als over de pincode. Een gestolen bankpas is waardeloos zonder een bijbehorende pincode. Iemand die de pincode te weten is gekomen heeft niks aan deze pincode zonder de bijbehorende bankpas. Geld opnemen bij de bank onder een andere identiteit wordt hiermee bemoeilijkt. De bank en de klant, waartoe de identiteit behoort, hebben meer zekerheid dat alleen de klant in staat is om geld op te nemen namens deze klant.

Toelichting op authenticatie middelen

Het scala aan authenticatie middelen is zeer uitgebreid. Hieronder worden in het kort een aantal authenticatie middelen aangestipt. Dit zijn het challenge-response principe en biometrie. Het challenge-response principe omdat dit een belangrijk middel is voor authenticatie in een “open” omgeving en biometrie omdat de kracht hiervan nogal eens overschat wordt.

Challenge-response: Een van de meest toegepaste vormen van authenticatie is het gebruik van wachtwoorden. Aan wachtwoorden kleven velen nadelen. Een nadeel dat hierbij speelt in open netwerkomgevingen is de mogelijkheid tot het afluisteren van het wachtwoord dat verstuurd wordt als kenmerk van het B naar A (zie figuur 8). Om dit te ondervangen wordt in open omgevingen veel gebruik gemaakt van challenge-response systemen. Hierbij wordt het wachtwoord niet verstuurd, maar het systeem waarmee de gebruiker contact wil, genereert eerst een code (challenge). De gebruiker moet dan antwoorden met de juiste antwoordcode (response). De gebruiker heeft hiertoe een (geautomatiseerd) algoritme tot zijn beschikking om de response af te leiden uit de challenge. De juistheid van de response wordt binnen het systeem gecontroleerd met hetzelfde algoritme als de gebruiker heeft.

Biometrie: Biometrie omvat onderscheidende eigenschappen van een persoon, zoals zijn vingerafdruk, irisscan, handschrift, etc. De kracht van biometrie wordt nog al eens overschat. Voornamelijk omdat voor de implementatie van biometrie als authenticatie middel een aantal concessies moet worden gedaan waardoor biometrie veiliger is dan het lijkt. Bij een biometrisch systeem wordt namelijk gebruik gemaakt van een permanent opgeslagen afdruk van de biometrische eigenschap die vergeleken wordt met een live scan van de biometrische eigenschap. Om iemand te authenticeren moet de live scan binnen bepaalde marges overeenkomen met de opgeslagen afdruk. Een biometrische eigenschap kan namelijk onderhevig zijn aan verandering en wordt daarnaast niet altijd op dezelfde manier aangeboden aan de scanner. Om het aantal

incidenten te minimaliseren waarbij personen ten onrechte niet worden geauthentiseerd worden deze marges gebruikt. Doordat bepaalde marges worden aangehouden is het mogelijk een onjuiste persoon te authenticeren of om een juiste persoon niet te authenticeren. Het eerste geval wordt weergegeven door de FAR, False Acceptance Rate, en laatste geval wordt weergegeven door de FRR, False Rejection Rate. Zodra de live scan en de permanent opgeslagen afdruk binnen bepaalde marges met elkaar overeen komen wordt de gebruiker geauthentiseerd. Er moet bij biometrie dus gebruik gemaakt worden van tolerantie marges wat het vertrouwen in de identiteit niet ten goede komt.

Autorisatie

Autorisatie is het toekennen van het recht aan geidentificeerde en geauthenticeerde subjecten om toegang te krijgen tot (bepaalde) informatie van een object. Autorisatie gebeurt op basis van de rechten die in een eerder stadium zijn gespecificeerd in het systeem via een model zoals DAC of MAC.

3.2.3 Het bewaken van toegang

Het bewaken van toegang omvat het detecteren van inbreuken op de toegangsregels en het registreren ervan en het registreren van verleende toegang aan geautoriseerde subjecten.
Bij het detecteren van inbreuken op de toegangsregels kunnen we onderscheid maken in:

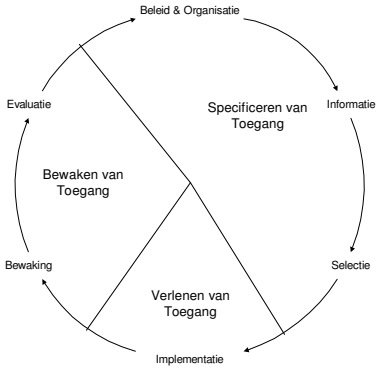
- Een feitelijke inbreuk, waarbij de toegangsbeheersing gefaald heeft.
- Een potentiële inbreuk, waarbij een niet gelukte inbreukpoging gedetecteerd is.

3.3 Organisatorische maatregelen

Analoog aan de stappen die onderkend worden bij de logische maatregelen kan men dezelfde stappen onderkennen bij de organisatorische maatregelen. Dit zijn [7]:

- Het specificeren van toegang: dit omvat het opstellen van regels voor het verlenen van toegang.
- Het verlenen van toegang: dit omvat het daadwerkelijk geven van toegang.
- Het bewaken van toegang: dit omvat het controleren of de verleende toegang of de te verlenen toegang correspondeert met de gespecificeerde toegang.

Bij organisatorische maatregelen gaat het echter niet meer over software –en hardwarematige configuraties en principes, maar om processen die zich afspelen binnen een organisatie ten behoeve van het goed verlopen van toegangsbeveiliging. Analoog aan de informatiebeveiligingscyclus uit hoofdstuk 2 kan hiervoor een toegangsbeveiligingscyclus worden opgesteld, zie figuur 9.



Figuur 9: De toegangsbeveiligingscyclus

De onderdelen van de toegangsbeveiligingscyclus worden in de hierop volgende paragrafen verder uitgewerkt.

3.3.1 Het specificeren van toegang

Bij het specificeren van toegang worden een aantal stappen doorlopen om uiteindelijk te komen tot een informatiebeveiligingsplan voor toegangsbeveiliging. Dit zijn:

Opstellen informatiebeveiligingsbeleid (Beleid & Organisatie)

Analoog aan het informatiebeveiligingsbeleid voor de gehele organisatie, of als onderdeel daarvan, dient het management de eisen en randvoorwaarden die gesteld worden aan toegangsbeveiliging te formuleren en te documenteren. Men dient aan te geven hoe men wenst om te gaan met risico's:

- Moeten de kosten van beveiliging in evenwicht zijn met de potentiële schade (risiconeutraal)
- Neemt men juist wat meer risico (risicodragend)
- Of neem men juist zo min mogelijk risico (risicomijdend)

Daarnaast dient men in het beleid aan te geven welke standaarden en richtlijnen er gelden voor het uitvoeren van risicoanalyses en voor het selecteren, implementeren en evalueren van beveiligingsmaatregelen.

Inventariseren van risico's (Informatie)

De informatievoorziening bestaat uit objecten die kwetsbaar zijn voor bedreigingen. Uitgaande van de betrouwbaarheid die gesteld wordt aan de informatievoorziening is te bepalen of de organisatie risico loopt of niet. Het management dient te bepalen hoeveel risico de organisatie mag lopen zodat te grote risico's kunnen worden ingeperkt met beveiligingsmaatregelen.

Opstellen informatiebeveiligingsplan (Selectie)

Om de risico's in te perken dient er een pakket beveiligingsmaatregelen te worden opgesteld. Afhankelijk van de aard en omvang van de risico's kunnen toegangsbeveiligingsmaatregelen hierbij een rol spelen. De keuze voor toegangsbeveiligingsmaatregelen kunnen zich zowel fysieke, logische als organisatorisch van aard zijn.

3.3.2 Het verlenen van toegang

Het verlenen van toegang omvat maatregelen en richtlijnen voor het uitgeven en beheren van:

- identiteiten: identiteit management
- authenticatiemiddelen: authenticatie management
- autorisatie: autorisatie management

Voordat deze maatregelen en richtlijnen worden behandeld dient eerst een ander probleem te worden aangestipt, namelijk de relatie tussen entiteiten en identiteiten in de reële wereld en identiteiten in de abstracte wereld van computers.

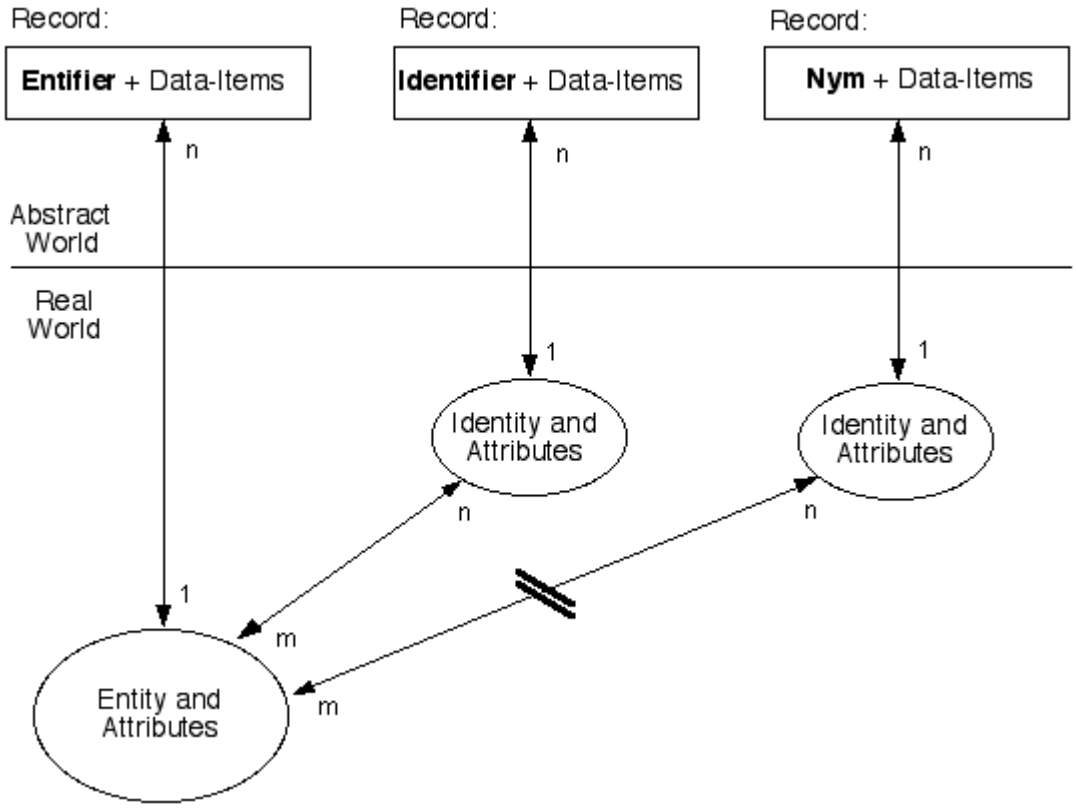
Entiteiten versus Identiteiten

In de reële wereld hebben we te maken met entiteiten en de daarbij behorende identiteiten. Een entiteit kan bijvoorbeeld zijn een mens en de bijbehorende identiteit kan dan bijvoorbeeld zijn de naam van deze persoon. Soms zijn identiteiten vrij formeel, zoals de identiteit die iemand heeft volgens zijn paspoort. Soms zijn deze minder formeel, zoals een schuilnaam of koosnaam. Hierbij dient dus te worden opgemerkt dat een mens niet per definitie beschikt over een enkele identiteit. Zelfs niet over een enkele formele identiteit. Mensen kunnen in het dagelijks leven beschikken over meerdere identiteiten. Zo kan iemand bijvoorbeeld over twee staatsburgerschappen beschikken en dus twee paspoorten hebben. Daarnaast is het niet ongewoon dat mensen in het dagelijks leven meerdere rollen aannemen waarbij dezelfde persoon in elke rol onder een andere naam bekend staat. Hierbij is het mogelijk dat aan elke rol een andere identiteit verbonden is.
Naast het feit dat een entiteit meerdere identiteiten kan aannemen kan een enkele identiteit ook aangenomen worden door meerdere personen (entiteiten). Dit kan bewust gebeuren, bijvoorbeeld een persoon neemt een andere persoon zijn identiteit aan om hier misbruik van te maken, of dit kan onbewust gebeuren. Zo kunnen er binnen een bepaalde context twee identiteiten bestaan die beide naar een ander persoon (entiteit) wijzen, maar vanwege beperkingen binnen de context exact hetzelfde zijn gedefinieerd. Bijvoorbeeld de voornaam van een persoon.
Entiteiten en identiteiten zijn begrippen die zich in de reële wereld bevinden, echter voor toegangscontrole is het nodig dat de entiteiten en identiteiten in een informatiesysteem kunnen worden vastgelegd. Zodra deze in een informatiesysteem zijn vastgelegd kunnen deze gebruikt worden om te controleren wie toegang tot informatie of tot een systeem verlangt en of dit dient te worden verleend.

Model van Clarke

De relatie tussen menselijke entiteiten, identiteiten en de manier waarop deze in een systeem worden vastgelegd is weergegeven in een artikel geschreven door Clarke [9] en is in figuur 10 schematisch weergegeven. Entiteiten in de reële wereld kunnen door middel van "entifiers" in de abstracte wereld, de wereld van informatiesystemen, uniek van elkaar worden onderscheiden. Een "entifier" kan van alles aan een mens zijn, of een combinatie daarvan, wat onderscheidend is. Gedacht kan worden aan fysieke uiterlijke kenmerken, sociaal gedrag, bio-dynamiek (geschreven handtekening,karakteristieken van de stem), natuurlijke fysiografie(vingerafdruk,gebit gegevens,botbreuken) en opgelegde fysieke kenmerken. In de praktijk echter worden entiteiten zo niet vastgelegd, maar zit er in de reële wereld een "laag" tussen: de identiteit. Zoals in de vorige paragraaf al was aangegeven, kan een entiteit beschikken over meerdere identiteiten en kan een identiteit worden gebruikt door de verschillende entiteiten. Identiteit worden in de abstracte wereld door middel van "identifiers" uniek van elkaar onderscheiden. Gedacht kan worden aan bijvoorbeeld een gebruikersnaam die bij de identiteit hoort.

Zowel entiteiten als identiteiten kunnen meerdere verschijningen hebben in de abstracte wereld. Het is dus mogelijk dat bijvoorbeeld een identiteit meerdere keren is vastgelegd in een bepaald informatiesysteem echter elke keer via een andere "identifier". Zodra een "identifier" van een identiteit in een informatiesysteem is vastgelegd en deze identiteit is niet te herleiden, of moeilijk te herleiden tot een entiteit spreekt men niet van een "identifier", maar van een "nym". Dit is het geval bij een pseudoniem of anonimiteit en is in figuur 10 weergegeven door de twee parallel getrokken strepen door de m staat tot n relatie tussen een entiteit en een identiteit.



Figuur 10: Een model voor menselijke entiteiten en identiteiten [9].

Identiteit Management

Identiteit management omvat het uitgeven en beheren van identifiers, identiteiten in de abstracte wereld van computers. Identifiers worden gebruikt om personen (entiteiten) toegang te verschaffen tot de informatievoorziening van die organisatie. Belangrijk hierbij is dat alleen de personen die onderdeel vormen van de organisatie toegang krijgen via identifiers die voor de persoon in kwestie bedoeld zijn. Zo moet voorkomen worden dat iemand zich als een andere persoon voordoet en zo de beschikking krijgt over bepaalde identifiers, bijvoorbeeld gebruikersnamen voor een computersysteem, die eigenlijk voor een andere persoon bedoeld is.
Het primaire doel van identiteit management wordt daarom gedefinieerd als:

Beheren van identifiers en zekerheid verkrijgen over de terugvoerbaarheid van deze identifiers tot entiteiten.

Om dit doel te bereiken moeten er beveiligingsmaatregelen genomen worden.
Het secundaire doel van identiteit management is:

Beheersbaar maken van de vele "identifiers" behorende bij een identiteit en de vele identiteiten behorende bij een entiteit.

Welke maatregelen er precies genomen moeten worden om de doelen van identiteit management te verwezenlijken komt aan bod in hoofdstuk 5.

Authenticatie Management

Authenticatie management omvat het beheer van authenticatie middelen. Authenticatie middelen dienen om te verifiëren dat een gebruikte identifier behoort tot de persoon die via deze identifier toegang tot het systeem probeert te verkrijgen. Het beheer omvat uitgifte van authenticatie middelen aan de juiste personen, inname van authenticatie middelen. Met andere woorden: Het beheer van de gehele levenscyclus van een authenticatie middel. Belangrijk hierbij is dat authenticatiemiddelen niet gebruikt worden door personen waarvoor deze niet zijn bedoeld.
Het doel van authenticatie management is daarom:

Zekerheid verkrijgen in de betrouwbaarheid van de gehele levenscyclus van een authenticatie middel.

Door middel van de juiste informatiebeveiligingsmaatregelen kan dit doel worden gehaald. Dit wordt behandeld in hoofdstuk 5.

Autorisatie Management

Autorisatie management omvat het beheren van rechten die subjecten hebben tot de informatie van objecten. Deze rechten moeten afgestemd zijn op de handelingen die door een subject moeten worden verricht. Zodra subjecten meer rechten hebben dan ze nodig hebben brengt dit extra risico's met zich mee. Zodra subjecten minder rechten hebben dat ze nodig hebben wordt het functioneren van die subjecten bemoeilijkt. Het doel van autorisatie management is daarom:

Het beheren van op maat gesneden rechten van subjecten tot objecten

Door middel van de juiste informatiebeveiligingsmaatregelen kan dit doel worden gehaald. Dit wordt behandeld in hoofdstuk 5.

3.3.3 Het bewaken van toegang

De laatste fase in de informatiebeveiligingscyclus omvat het bewaken van de toegang. In eerdere fases is de gewenste toegang gespecificeerd en verleend. Deze fase dient ter controle of de nagestreefde doelen zoals gesteld in het informatiebeveiligingsbeleid en in het informatiebeveiligingsplan worden gehaald.
Dit gebeurt door middel van controle en evaluatie waarna het informatiebeveiligingsbeleid of het informatiebeveiligingsplan kan worden bijgesteld, indien nodig.
Het geheel van controle en evaluatie ligt echter buiten de scope van deze scriptie en wordt hier niet verder behandeld.

4 Modelleren van toegangsbeveiliging

Het inrichten van toegangsbeveiliging is een grote opgave. Er dienen regels en richtlijnen te worden opgesteld voor de organisatie, er dienen regels en richtlijnen te worden vastgelegd in hardware en software en de juiste technische hulpmiddelen dienen aanwezig te zijn. Het geheel van regels, richtlijnen en hulpmiddelen dient goed op elkaar te zijn afgestemd, de ketting is immers zo sterk als de zwakste schakel. Voor een goed toegangsbeveiligingsbeleid moeten dus diverse keuzes gemaakt worden op uiteenlopende vlakken. Deze keuzes werden in het verleden voornamelijk genomen door aparte informatiebeheerafdelingen. Hierbij redeneerden deze afdelingen iets te vaak vanuit de technologische kant, met maximale beveiliging in het achterhoofd, zonder echt goed te kijken naar de organisatie. Hierdoor ontstond toegangsbeveiligingsbeleid dat wellicht niet helemaal aansloot op de organisatie. Elke organisatie is namelijk uniek in het bepalen van hun doelstellingen en in het bepalen van de risico's die de organisatie daarbij wil lopen.
Met bovenstaande dient in het toegangsbeveiligingsbeleid rekening gehouden te worden. Informatiebeheerafdelingen zijn hier vaak niet toe in staat aangezien dit strategische keuzes omvat die gemaakt moeten worden door het management. Het management bepaalt de lange termijn doelstellingen van een organisatie en maakt hierbij afwegingen met betrekking tot te verwachten risico's: de mate waarin bepaalde risico's wel of niet door middel van maatregelen dienen te worden afgedekt. Echter waar het management deze maatregelen op allerlei gebieden neemt, ontwijkt zij dit vaak voor het informatiebeveiligingsbeleid in z'n algemeen en het toegangsbeveiligingsbeleid in het bijzonder. Dit heeft een aantal redenen:

- Gebrek aan interesse voor het onderwerp
- Gebrek aan kennis over het onderwerp

Hierdoor komt het vaak niet tot een goed afgestemd toegangsbeveiligingsbeleid.
De toegangsbeveiligingscyclus, zie §3.3, bevat de stappen die het management moet nemen. Volgens de toegangsbeveiligingscyclus begint het management met het opstellen van het informatiebeveiligingsbeleid. Hierin stelt het management, aan de hand van de eisen en randvoorwaarden die aan de informatie voorziening gesteld worden, beleid op ten aanzien van toegangsbeveiliging. Vervolgens worden de risico's geanalyseerd en wordt aangegeven welke risico's onacceptabel zijn. Waarna kan worden overgegaan tot het opstellen en implementeren van een pakket passende maatregelen. Het volgen van de stappen uit de toegangsbeveiligingscyclus geeft echter de volgende problemen:

- Het is een tijdrovend proces waarin veel organisaties geen zin hebben
- Voor het goed uitvoeren van bepaalde stappen is expertkennis nodig die vaak binnen de organisatie niet aanwezig is.

Een uitkomst voor deze problemen zou het gebruik van een model zijn, waarbij men aan de hand van een aantal, voor managers, begrijpbare criteria tot een set met maatregelen komt. Modellering betekent veelal dat stappen worden vereenvoudigd. De essentie van een complexe stap wordt vereenvoudigd weergegeven of verborgen. In het geval van de toegangsbeveiligingscyclus kan men zo het tijdrovende proces van het doorlopen van de stappen vermijden en is er geen expertkennis nodig.

4.1.1 Randvoorwaarden aan een model voor toegangsbeveiliging

Een model kan een uitkomst zijn bij het oplossen van een bepaald vraagstuk. Echter niet elk model zal toepasbaar zijn op elk vraagstuk. In deze scriptie wordt het vraagstuk weergegeven door de probleemstelling uit §1.3 en deze wordt hier voor de volledigheid nog even herhaald:

Wat is adequate toegangsbeveiliging voor een informatievoorziening die toegankelijk is via publieke netwerken?

De kern van het vraagstuk bestaat uit het specificeren van toegang voor een “web-enabled” informatievoorziening. Hiervoor moet analoog aan de toegangsbeveiligingscyclus:

- Risico’s worden geïnventariseerd.
- Betrouwbaarheidseisen worden geïnventariseerd.
- Afwegingen gemaakt worden of bepaalde risico’s wel of niet acceptabel zijn.
- Een pakket maatregelen worden opgesteld die in overeenstemming zijn met de gewenste risico’s.

Dit alles rekening houdend met het feit dat de informatievoorziening door zijn “web-enabled” karakter in essentie toegankelijk kan zijn voor iedereen.
De bovenstaande stappen kunnen echter niet zo uitgebreid worden uitgevoerd als wanneer men deze stappen doorloopt aan de hand van de toegangsbeveiligingscyclus. Een model is nu eenmaal een vereenvoudiging van de werkelijkheid. Dit heeft als nadeel dat dit ten koste gaat van bepaalde details, maar als voordeel dat een oplossing makkelijker te vinden is. Dit zou voor het inventariseren van de risico’s en betrouwbaarheidseisen bijvoorbeeld kunnen betekenen dat deze per groep worden geïnventariseerd of van toepassing zijn op een groep van organisaties. Hetzelfde zou gezegd kunnen worden voor het maken van de afwegingen en het kiezen van een pakket met maatregelen. Deze zullen overeenkomen kunnen komen met de afwegingen die binnen een standaard organisatie worden gemaakt en met de maatregelen die binnen een standaard organisatie worden gebruikt. Dit alles afhankelijk van het model dat gaat worden gebruikt.

Bovenstaande schept de volgende randvoorwaarden voor een model voor toegangsbeveiliging van de informatievoorziening in een “web-enabled” omgeving:

- Risico’s voor een organisatie dienen globaal te worden geïnventariseerd
- Betrouwbaarheidseisen voor een organisatie dienen globaal te worden geïnventariseerd
- Een gestandaardiseerde set met maatregelen dient te volgen uit de geïnventariseerde set met risico’s en betrouwbaarheidseisen.
- Het model dient makkelijk toepasbaar te zijn door het management zonder enige vorm van expertkennis.

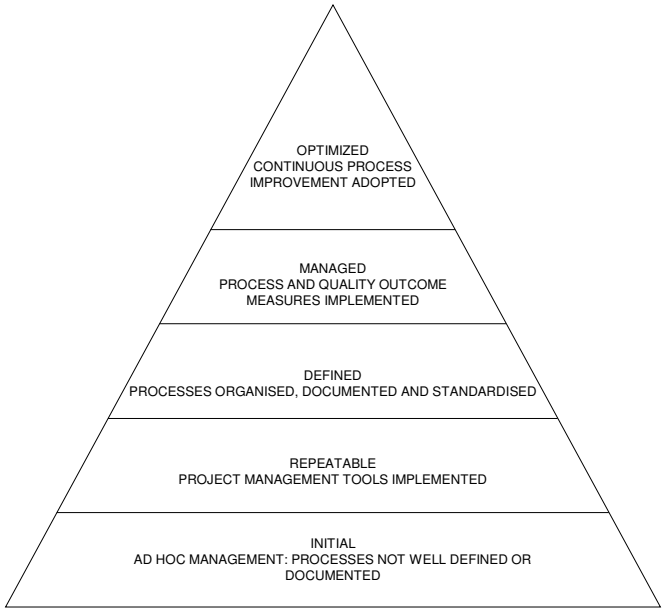
4.1.2 Bestaande modellen

In de vorige paragraaf zijn de randvoorwaarden opgesteld waaraan een model moet voldoen. Een model dat naadloos aansluit op deze randvoorwaarden is echter niet gevonden. Tijdens de zoektocht naar een geschikt model zijn we modellen tegengekomen die nuttig waren bij het opstellen van een nieuw model. Bepaalde modellen hebben aspecten die bruikbaar blijken te zijn bij het opstellen van een nieuw model en andere modellen scheppen randvoorwaarden die hierboven nog niet zijn genoemd. Dit omvat de volgende modellen:

- Capability Maturity Model
- De basisconfiguraties van mintzberg

Capability Maturity Model

Het Capability Maturity Model (CMM) [10] geeft inzicht in het ontwikkelingsniveau of de volwassenheid van een organisatie die zich richt op softwareontwikkeling. Het model beschrijft de wijze waarop binnen de organisatie wordt omgegaan met de bedrijfsprocessen en onderscheidt hiertoe vijf niveaus, zie figuur 11. Het model is opbouwend en definieert concrete stappen en activiteiten om van het ene naar het andere niveau te komen. Belangrijk hierbij is dat de organisatie de softwareontwikkeling moet kunnen dragen.



Figuur 11: Capability Maturity Model

Alhoewel dit model oorspronkelijk was opgezet voor softwareontwikkeling kan uit dit model genoeg wijze lessen worden afgeleid voor andere situaties. Het CMM geeft duidelijk aan dat je eerst moet kunnen kruipen voordat je kan beginnen met lopen. Hierdoor schept dit model een duidelijke randvoorwaarde waaronder het op te stellen model, voor toegangsbeveiliging, bruikbaar is. Het op te stellen model is voornamelijk bedoeld voor organisaties die niet zelfstandig in staat zijn om de stappen uit de informatiebeveilgingscyclus te doorlopen. Hiermee wordt automatisch een bovengrens gesteld aan de bruikbaarheid van het op te stellen model. Een model als het CMM kan helpen bij het vaststellen van die bovengrens.

De basisconfiguraties van Mintzberg

Met de basisconfiguraties van Mintzberg [11] kunnen organisaties gecategoriseerd en getypeerd worden. Het organisatiemodel dat Mintzberg als uitgangspunt neemt, kent zes onderdelen: de strategische top, het middenkader, de uitvoerende kern, de technostructuur, de ondersteunende staf en de ideologie. Op basis van deze onderdelen bouwt Mintzberg zeven zogenaamde basisconfiguraties:

- De ondernemersorganisatie
- De professionele organisatie
- De machineorganisatie
- De innovatieve organisatie
- De gediversifieerde organisatie
- De zendingsorganisatie
- De politieke organisatie

Deze organisaties verschillen van elkaar: onder meer in dominantie van een bepaald onderdeel, in primair coördinatiemechanisme en in vorm en mate van decentralisatie. Zo is in de ondernemersorganisatie de strategische top het belangrijkste, directe toezicht het primaire coördinatiemechanisme en is er sprake van centralisatie. In de professionele organisatie staan hier respectievelijk de uitvoerende kern, standaardisatie van vaardigheden en verticale en horizontale decentralisatie tegenover. Op basis van de categorie waarin een organisatie thuishoort, kunnen de problemen worden aangepakt aangezien verschillende organisaties om verschillende aanpakken van problemen vragen. De werkwijze die Mintzberg hanteert is bruikbaar voor het op te stellen model: op basis van een aantal kenmerken een organisatie categoriseren waarna de problemen binnen zo'n categorie op dezelfde manier kunnen worden aangepakt. De indeling die Mintzberg hanteert is echter te algemeen en niet onderscheidend genoeg om hieraan dreigingen en kwetsbaarheden en noodzakelijke betrouwbaarheidseisen toe te kennen. Hiervoor is een uitgebreidere indeling in categorieën nodig.

5 Toegangsbeveiligingsmaatregelen model

In het vorige hoofdstuk is gesproken over het modelleren van toegangsbeveiliging, het nut van modelleren en de randvoorwaarden voor toepassing van een model op het vraagstuk van deze scriptie. Het hoofddoel van het model is om op een makkelijke en snelle manier een set met toegangsbeveiligingsmaatregelen toe te kennen aan een organisatie. Bekende methodes om tot deze set met toegangsbeveiligingsmaatregelen te komen zijn:

- risicoanalyses, maar deze zijn te uitgebreid, deze methodes hebben expertkennis nodig en vragen veel tijd.
- het gebruik van “best practices”. Deze “best practices” zijn snel en makkelijk toe te passen, maar zijn te algemeen toepasbaar.

De methode die wij zoeken voor het vraagstuk van deze scriptie ligt precies tussen bovenstaande twee uitersten in. De methode moet snel en makkelijk, zonder expertkennis, toepasbaar zijn, maar moet ook weer niet te algemeen zijn. De methode moet enigszins rekening houden met de organisatie in kwestie.
Een methode die aan deze eisen voldoet hebben we niet gevonden. Daarom wordt in dit hoofdstuk een model geïntroduceerd dat naar aanleiding van het vraagstuk van deze scriptie, met in achtneming van de gestelde randvoorwaarden, is opgesteld. Dit is het toegangsbeveiligingsmaatregelen model en is grafisch weergegeven in figuur 12.
We willen een model hebben dat maatregelen voorschrijft op basis van de organisatie zonder dat dit omslachtig is en hiervoor expertkennis voor nodig is.. Het model dient daarom een koppeling te maken tussen organisaties enerzijds en toegangsbeveiligingsmaatregelen anderzijds. Voor het vinden van deze koppeling zijn een aantal paden bewandeld voordat we uiteindelijk zijn uitgekomen bij het model zoals dit is weergegeven in figuur 12. De diverse mogelijkheden voor een model die onderzocht zijn worden hieronder kort toegelicht.

Categoriseren van organisaties naar soort

Voor het vinden van een koppeling tussen organisaties enerzijds en maatregelen anderzijds wilden we in eerste instantie organisaties indelen naar hun soort. De gedachte was dat er een indeling in categorieën is te maken waarbij elke categorie een soort organisatie bevat die correspondeert met een bepaalde set met toengangsbeveiligingsmaatregelen. Als uitgangspunt hiervoor zijn in eerste instantie de basisconfiguraties van Mintzberg [11] genomen. Dit betreft een indeling van organisaties in zeven categorieën. Hoewel de basisconfiguraties van Mintzberg heel helder diverse type organisaties onderscheidt bleek deze indeling niet onderscheidend genoeg om toepasbaar te zijn voor dit probleem. Elke organisatie heeft te maken met toegangsbeveiliging. De ene organisatie wat meer dan de andere, maar dit onderscheid valt niet te maken door te kijken naar het type organisatie.

Categoriseren van organisatie naar onderscheidende kenmerken

Hoewel in eerste instantie duidelijk was geworden dat indelen van organisatie naar type niet nuttig is voor het vinden van een koppeling, was er nog steeds de gedachte dat organisaties op één of andere manier van elkaar verschillen en dat deze verschillen zich zouden laten vertalen naar toegangsbeveiligingsmaatregelen. Deze verschillen zouden dan niet te vinden zijn in de kenmerken

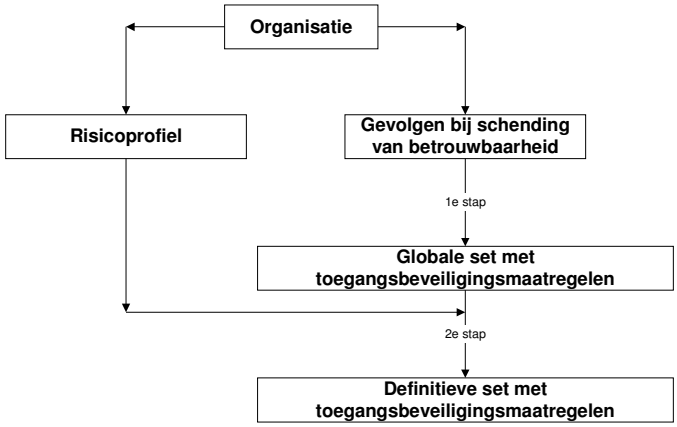
die Mintzberg hanteert, maar te vinden zijn in kenmerken die een duidelijkere link hebben met toegang tot de informatievoorziening. Om de onderscheidende kenmerken te achterhalen zijn interviews afgenomen met medewerkers van diverse organisaties, zoals banken, multinationals en overheidsinstellingen, die verantwoordelijk zijn voor de inrichting van toegangsbeveiliging binnen hun organisatie. Door middel van de interviews is geprobeerd te achterhalen op basis waarvan bepaalde toegangsbeveiligingsmaatregelen zijn genomen. Dit leverde echter geen noemenswaardige onderscheidende kenmerken op om een koppeling te maken tussen organisaties en toegangsbeveiligingsmaatregelen. Veelal wisten deze medewerkers geen kenmerken van hun organisatie aan te geven die verband hielden met bepaalde maatregelen, nog vaker waren bepaalde maatregelen gewoon genomen omdat de IT-afdeling dat nodig vond.

Categoriseren naar betrouwbaarheidseisen en organisatiekenmerken

Noch naar aanleiding van literatuur, noch naar aanleiding van expertkennis was een indeling te maken van organisaties naar sets met toegangsbeveiligingsmaatregelen. Daarom was in derde instantie de gedachte dat betrouwbaarheidseisen en organisatiekenmerken zouden leiden tot de sets met toegangsbeveiligingsmaatregelen. Analoog aan risicoanalyse zouden de betrouwbaarheidseisen de afhankelijkheid van de organisatie van de informatievoorziening weergeven en de organisatiekenmerken de kwetsbaarheden van de informatievoorziening, waarna deze gezamenlijk het risico zouden bepalen aan de hand waarvan maatregelen genomen zouden worden, echter dit alles op een veel beknoptere en makkelijkere manier dan wanneer een volledige risicoanalyse zou worden uitgevoerd.
Categoriseren naar betrouwbaarheideisen brengt echter een aantal problemen met zich mee. De betrouwbaarheidseisen representeren het door de organisatie gewenste niveau van betrouwbaarheid van de informatievoorziening. In principe zou elke organisatie wel willen beschikken over een zeer betrouwbare informatievoorziening, maar hier zijn echter kosten aan verbonden die niet elke organisatie bereid is te dragen of kan dragen. Organisaties moeten een kosten afweging maken tussen enerzijds de kosten die zij zullen ondervinden van de gevolgen die ontstaan als de informatievoorziening de gewenste betrouwbaarheid niet haalt en anderzijds de kosten die gemaakt moeten worden om de gewenste betrouwbaarheid te garanderen, zoals kosten voor informatiebeveiliging.

Categoriseren naar gevolgen bij schending van de betrouwbaarheid en risicoprofielen

In het uiteindelijke model wordt, om de problemen uit de vorige stap te vermijden, gebruik gemaakt van de gevolgen bij schending van de betrouwbaarheid en van risicoprofielen om te komen tot een set van toegangsbeveiligingsmaatregelen. Door gebruik te maken van “gevolgen bij schending van betrouwbaarheid” in plaats van betrouwbaarheidseisen kan het bedrijfskundig belang van een betrouwbare informatievoorziening voor een organisatie beter in het model worden meegenomen. Door gebruik te maken van risicoprofielen worden de organisatiekenmerken die de risico’s veroorzaken gebundeld waardoor het model overzichtelijker wordt voor de gebruiker.
Het afleiden van de set met toegangsbeveiligingsmaatregelen gebeurt in twee stappen, zie figuur 12:



Figuur 12: Toegangsbeveiligingsmaatregelen model

- in de eerste stap wordt op basis van de *gevolgen bij schending van de betrouwbaarheid* een globale set met toegangsbeveiligingsmaatregelen samengesteld. Hierbij zijn de *gevolgen bij schending van de betrouwbaarheid* een graadmeter voor de omvang van de gevolgen indien bepaalde betrouwbaarheidseisen van de informatievoorziening worden geschonden en dus in welke mate maatregelen nodig zijn om de betrouwbaarheid te kunnen blijven waarborgen. Dit levert een globale set met maatregelen op. In §5.2 wordt het begrip *gevolgen bij schending van de betrouwbaarheid* en de verschillende gradaties die hierin onderkend worden verder uitgewerkt, in §5.5 wordt uitgelegd hoe de koppeling gelegd is tussen de *gevolgen bij schending van de betrouwbaarheid* en een globale set met toegangsbeveiligingsmaatregelen en in §5.4 worden toegelicht uit welke maatregelen de diverse set met maatregelen, die uitkomst zijn van deze eerste stap, bestaan.

- in de tweede stap wordt op basis van de gekozen set met toegangsbeveiligingsmaatregelen en het risicoprofiel van de organisatie een definitieve set met toegangsbeveiligingsmaatregelen samengesteld. Het risicoprofiel neemt kenmerken van organisaties, die dreigingen representeren, mee in de uiteindelijke keuze voor een set met maatregelen. In §5.3 wordt ingegaan op de verschillende risicoprofielen die van toepassing kunnen zijn op een organisatie en uit welke organisatiekenmerken deze risicoprofielen bestaan, in §5.5 wordt uitgelegd hoe de koppeling gelegd is tussen de globale set met maatregelen, uit de eerste stap, het risicoprofiel en de definitieve set met maatregelen en in §5.4 wordt toegelicht uit welke maatregelen de diverse sets met maatregelen, die uitkomst zijn van deze tweede stap, bestaan.

5.2 Gevolgen bij schending van betrouwbaarheid

Voor het optimaal functioneren van een organisatie is het van belang dat de organisatie kan vertrouwen op de informatievoorziening: de informatievoorziening dient betrouwbaar te zijn.
Zo kan bijvoorbeeld de organisatie de informatievoorziening zo inrichten dat bepaalde informatie slechts toegankelijk is voor een beperkte groep gebruikers, de organisatie classificeert daarmee bepaalde informatie als vertrouwelijk. De organisatie moet er dan vervolgens van op aan kunnen dat de vertrouwelijkheid van die informatie door de informatievoorziening gewaarborgd blijft. Hetzelfde geldt voor het waarborgen van de integriteit en beschikbaarheid van informatie door de informatievoorziening. De organisatie moet er op kunnen vertrouwen dat een bepaalde mate van integriteit en beschikbaarheid door de informatievoorziening wordt gewaarborgd. Om dit te bereiken

stelt de organisatie betrouwbaarheidseisen op. Op basis van deze betrouwbaarheidseisen neemt de organisatie maatregelen, waaronder toegangsbeveiligingsmaatregelen, zodat de betrouwbaarheid van de informatievoorziening gewaarborgd blijft. De grote vraag blijft natuurlijk welke en hoeveel maatregelen genomen moeten worden om de gewenste betrouwbaarheid te kunnen waarborgen. Indien het nemen van maatregelen kosteloos is dan zou men gewoon alle maatregelen kunnen nemen die bekend zijn. Echter dit is niet het geval. Organisaties moeten kiezen hoeveel en welke maatregelen men wilt nemen en welke maatregelen men wel en welke maatregelen men niet wil nemen. Indien men deze afweging op bedrijfskundig gronden maakt dan moet er een afweging gemaakt worden tussen:

- welke kosten gemoeid zijn met het nemen van maatregelen.
- welke kosten voorkomen kunnen worden met het nemen van maatregelen.

De kosten die voorkomen kunnen worden, door het nemen van maatregelen, bestaan uit kosten die verband houden met de gevolgen die ontstaan doordat de gestelde betrouwbaarheid niet wordt gehaald. Deze gevolgen kunnen bestaan uit:

- juridische gevolgen.
- publicitaire gevolgen.
- financiële gevolgen.
- operationele gevolgen.

Indien de kosten, die een organisatie logischerwijs kan verwachten, te hoog zijn in relatie tot wat een organisatie wil en kan dragen, moet de organisatie hiertegen maatregelen nemen. Het nemen van maatregelen beperkt de kans dat er te veel kosten ontstaan doordat de informatievoorziening de gewenste betrouwbaarheid niet haalt, maar aan het nemen van deze maatregelen zijn ook kosten verbonden. Het treffen van kostbare maatregelen om een gewenst niveau van betrouwbaarheid te halen is verspilling van schaarse middelen indien het niet halen van het gewenste niveau van betrouwbaarheid bijna geen directe of indirecte financiële gevolgen heeft of indien de financiële gevolgen die dit heeft de kosten van de maatregelen niet overtreffen. Andersom is het niet treffen van kostbare maatregelen uit bedrijfskundig oogpunt onverstandig indien de gevolgen, vertaald naar kosten, vele malen groter zijn dan de kosten die gemoeid zijn met het nemen van deze maatregelen.
Cruciaal voor het bepalen van het aantal maatregelen dat een organisatie moet nemen is dus de kostenafweging op basis van de gewenste betrouwbaarheid, maar niet de gewenste betrouwbaarheid op zichzelf.
Organisaties moeten zich, om te bepalen welke en hoeveel maatregelen genomen moeten worden, bijvoorbeeld afvragen of het niet halen van de gewenste betrouwbaarheid:

1. de continuïteit van de organisatie in gevaar brengt.
2. het imago van de organisatie onherstelbaar beschadigd wordt.
3. de financiële gevolgen groot zijn in relatie tot de begroting van de organisatie.

In het model worden de gevolgen bij schending van betrouwbaarheid gebruikt voor het afleiden van een set met maatregelen. Hiervoor is voor elke betrouwbaarheidscomponent (vertrouwelijkheid, integriteit en beschikbaarheid) die geschonden kan worden een classificatie tabel opgezet. Deze classificatie dient als input voor het model. Het classificeren van de gevolgen bij schending van

vertrouwelijkheid en integriteit gaat voor beide kenmerken op dezelfde manier. De mogelijke classificaties zijn in tabel 1 opgesomd. Deze classificatiecriteria zijn in overleg met adviseurs van Verdonck, Klooster & Associates (VKA) gekozen op basis van hun expertkennis.

Classificatie	**Gevolgen bij schending van vertrouwelijkheid en integriteit**
Groot	Het voortbestaan van de organisatie wordt ernstig in gevaar gebracht.
Gemiddeld	Er wordt grote schade toegebracht aan het bereiken van de bedrijfsdoelstellingen. Financiële gevolgen en gevolgen voor het imago zijn groot.
Klein	Er wordt beperkte schade toegebracht aan het bereiken van de bedrijfsdoelstellingen. Financiële gevolgen of gevolgen voor het imago zijn beperkt.

Tabel 1: Classificatie van de gevolgen bij schending van vertrouwelijkheid en integriteit.

Uit tabel 1 kunnen de eerste twee benodigde invoerwaarden voor het model worden afgelezen. Het classificeren van de gevolgen bij schending van beschikbaarheid, de derde invoer van het model, gaat niet op dezelfde manier. Bij de eerste twee kenmerken is de daadwerkelijk schending de veroorzaker van de gevolgen. Bij schending van beschikbaarheid hoeft dit niet het geval te zijn. Bij schending van beschikbaarheid speelt de duur van de schending een veel belangrijkere rol dan de schending zelf. Het classificatie criterium van gevolgen bij schending van beschikbaarheid bestaat daarom uit de duur van een schending die nodig is om:

- grote schade toe te brengen aan het bereiken van de bedrijfsdoelstellingen
- grote financiële schade te veroorzaken
- grote schade toe te brengen aan het imago

De mogelijke classificatiecriteria zijn opgesomd in tabel 2. Deze classificatiecriteria zijn in overleg met adviseurs van VKA gekozen op basis van hun expertkennis.

Classificatie	**Gevolgen zijn groot bij onbeschikbaarheid na**
Groot	Eén dag
Gemiddeld	Eén week
Klein	Eén maand

Tabel 2: Classificatie van de maximale tijdsduur voordat grote gevolgen optreden bij onbeschikbaarheid.

5.3 Risicoprofielen

Het vaststellen van de financiële consequenties en overige consequenties voor de organisatie die optreden indien de gewenste betrouwbaarheid van de informatievoorziening niet wordt gehaald, is een goede graadmeter voor de noodzaak voor het implementeren van een set met maatregelen. Echter een organisatie opereert niet in een vacuüm. Een organisatie heeft continue interactie met

zijn omgeving, zowel binnen de grenzen van de organisatie als daarbuiten. Het optreden van financiële consequenties is dan wel afhankelijk van het wel of niet halen van de gewenste betrouwbaarheid en de gevolgen die door de schending van de betrouwbaarheidseisen ontstaan, maar het wel of niet halen van de gewenste betrouwbaarheid is vervolgens weer afhankelijk van de omgeving van de organisatie en dus de informatievoorziening. Zo heeft een organisatie met een openbaar toegankelijke informatievoorziening een groter kans dat de gewenste betrouwbaarheidseisen niet worden gehaald dan een organisatie met dezelfde informatievoorziening, echter meer gesloten, en gewenste betrouwbaarheidseisen. De informatievoorziening heeft namelijk minder toegangspunten waarlangs deze kan worden benaderd. Hiermee wordt dus de groep van mogelijke veroorzakers kleiner en dus ook de kans dat de betrouwbaarheid van de informatievoorziening wordt aangetast.
Naast de financiële en overige consequenties die optreden bij schending van de betrouwbaarheid moet dus ook goed worden gekeken naar de omgeving van de organisatie wanneer men nadenkt over de noodzaak voor het nemen van maatregelen. Het is dus belangrijk om te bepalen welke omgeving een grotere kans geeft op het niet halen van de betrouwbaarheideisen. Vervolgens kan op basis van deze informatie bepaalt worden welke set met maatregelen een organisatie moet implementeren.
Elke omgeving brengt een kans met zich mee dat de gewenste betrouwbaarheidseisen niet worden gehaald. Het is echter belangrijk om te identificeren welke omgevingen een grotere of kleinere kans veroorzaken, zodat niet te weinig of te veel maatregelen worden genomen. Het identificeren van de kans op schending van betrouwbaarheid binnen een bepaalde omgeving kan met behulp van een risicoanalyse. Hiermee wordt bepaald voor welke dreigingen de informatievoorziening kwetsbaar is en welk risico dit veroorzaakt ten aanzien van het instant houden van de gewenste betrouwbaarheidseisen. Het uitvoeren van een risicoanalyse is maatwerk en is daarom zeer tijdrovend en kostbaar. Daarnaast moet deze, om een goed resultaat te krijgen, worden uitgevoerd door een expert. Binnen de overheid wordt A&K analyse [12] veelvuldig toegepast[2]. Binnen de bancaire wereld wordt gebruik gemaakt van de SPRINT-analyse [13] welke is ontwikkeld door een aantal bancaire instellingen.
Één van de randvoorwaarden voor dit model is dat het verkrijgen van een set met maatregelen snel en zonder de hulp van experts kan plaatsvinden. Daarom is het uitvoeren van bovenstaande risicoanalyses niet geschikt. In dit model wordt het risico bepaald aan de hand van een aantal makkelijk identificeerbare organisatiekenmerken. Om overzicht te houden over welke kenmerken of combinatie van kenmerken een groter of kleinere kans met zich meebrengen, ten aanzien van het instant houden van de betrouwbaarheidseisen, zijn deze ingedeeld in drie risicoprofielen:

- een profiel met een laag risico.
- een profiel met een normaal risico.
- een profiel met een hoog risico.

De kenmerken die van toepassing zijn op een organisatie, bepaalt het risicoprofiel waarin een organisatie wordt ingedeeld. Risicoprofielen met bijbehorende organisatiekenmerken verwoorden op een begrijpelijkere manier de kwetsbaarheid voor bepaalde dreigingen die een verstoring van de informatievoorziening kunnen veroorzaken. Hierdoor wordt het bepalen van het risico. Er zijn echter geen standaardlijsten met organisatiekenmerken, die concrete dreigingen vertegenwoordigen, in de

[2] De K-analyse, kwetsbaarheids analyse, van de A&K analyse is bedoeld voor het onderzoeken van de risico's.

literatuur te vinden. Daarom zijn de volgende stappen doorlopen om een lijst met relevante organisatiekenmerken samen te stellen.:

1) de lijsten met dreigingen uit de SPRINT-analyse en de BSI[14] zijn bekeken.
2) bij elke dreiging worden, indien mogelijk, de organisatiekenmerken bepaald die deze dreiging veroorzaken.
3) de kwetsbaarheid van de informatievoorziening voor deze dreiging wordt bepaald en indien deze groot is wordt het organisatiekenmerk aan de lijst met organisatiekenmerken voor het model toegevoegd.

Bij het samenstellen van de lijst met organisatiekenmerken is gebruik gemaakt SPRINT en BSI. Uiteraard zijn er meerdere risicoanalyse methodieken en toegangsbeveiligingsstandaarden die een lijst met dreigingen voorschrijven op basis waarvan bovenstaande stappen doorlopen kunnen worden. Er is echter gekozen om één gangbare risicoanalyse methodiek te nemen, SPRINT, en één gangbare beveiligingsstandaard te raadplegen, BSI, omdat die uitgebreid genoeg zijn om alle dreigingen te bevatten. Het doornemen van meerdere risicoanalyse methodieken en toegangsbeveiligingsstandaarden zouden voor het grootste gedeelte alleen maar meer van hetzelfde opleveren. Bijlage B bevat een gedetailleerd overzicht van hoe de lijst met organisatiekenmerken tot stand is gekomen.
De lijst met organisatiekenmerken zijn onderverdeeld, op basis van waarop deze kenmerken betrekking hebben, in vier groepen:

- groep 1: toegang tot de informatie van buiten de organisatie.
- groep 2: toegang tot de informatie binnen de organisatie.
- groep 3: beheersbaarheid van het verstrekken van toegang tot de informatie.
- groep 4: positie van de organisatie in de maatschappij.

De organisatiekenmerken uit de vier groepen worden hieronder verder toegelicht. Hierbij wordt tevens aangegeven wanneer een bepaald kenmerk op een organisatie van toepassing is of niet.

5.3.1 Groep 1: Toegang tot de informatie van buiten de organisatie

Ambulante medewerkers

Ambulante medewerkers hebben steeds vaker de mogelijkheid om op locatie te beschikken over (gevoelige) informatie van de organisatie. Dit wordt veelal bereikt door het meebrengen van draagbare computermiddelen of door op locatie verbinding te maken met het netwerk van de organisatie. Hierdoor neemt de kans toe dat de betrouwbaarheid van de informatie wordt geschonden. De draagbare computermiddelen kunnen namelijk verloren raken of worden gestolen en de mogelijkheid om op locatie een verbinding te maken met het netwerk van de organisatie kan worden misbruikt door derden.
Criterium: Indien medewerkers buiten de panden van de organisatie toegang kunnen krijgen tot (gevoelige) informatie van de organisatie is dit kenmerk van toepassing op de organisatie.

Communicatie over onbeveiligde netwerken

Door het communiceren over onbeveiligde netwerken kan gevoelige informatie in handen komen van derden.

Criterium: Indien er communicatie plaats vindt met de organisatie over onbeveiligde netwerken dan is dit kenmerk van toepassing op de organisatie.

Geografische spreiding

Door de geografische spreiding van een organisatie, dient de digitale communicatie plaats te vinden over eventueel aanwezige netwerken tussen de diverse locaties. Dit kan zowel publieke als private netwerken betreffen. In het geval van publieke netwerken heeft dit invloed op de toegangsbeveiliging omdat ook derde een poging kunnen ondernemen om via deze publieke netwerken toegang te krijgen tot de informatie of informatievoorzieningen. Er worden namelijk meer toegangspaden gecreëerd, waarlangs ook derde toegang tot de informatievoorziening kunnen bemachtigen. De toegang langs deze paden dient zwaarder beveiligd te zijn.
Critierium: Indien de organisatie verdeeld is over meerdere fysiek gescheiden locaties is dit kenmerk op de organisatie van toepassing.

Toegang van partners/service providers tot kritieke informatie/informatiesystemen

De mate waarin partners, leveranciers of serviceproviders toegang hebben tot (gevoelige) informatie heeft invloed op de mate waarin zij de betrouwbaarheid van (gevoelige) informatie kunnen aantasten. Indien zij vergaande toegang hebben is het kanaal waarover deze toegang plaats vindt en de controle op het gebruik van deze toegang belangrijk.
Criterium: Indien partners / service-providers toegang hebben tot kritieke informatie / informatiesystemen is dit kenmerk op de organisatie van toepassing.

5.3.2 Groep 2: Toegang tot de informatie binnen de organisatie

Gebruik van Internet door de medewerkers

Door gebruik van Internet vanuit het bedrijf worden computersystemen blootgesteld aan virussen en trojans. In situaties waarbij medewerkers toegang hebben het internet dienen de rechten strak geregeld te zijn en goed gecontroleerd te worden.
Criterium: Indien medewerkers toegang hebben tot Internet is dit kenmerk van toepassing op de organisatie.

Legacy systemen

Legacy systemen worden vaak niet meer ondersteund door de leverancier. Zij hebben vaak een eigen beheersstructuur die moeilijk te integreren is met een overkoepelende beheersstructuur. Dit bemoeilijkt het uitvoeren van identiteit management.
Criterium: Indien ten minste 25% van de informatiesystemen als legacy systemen worden aangemerkt, de systemen zitten in de vervangingsfase, is dit kenmerk op de organisatie van toepassing.

5.3.3 Groep 3: Beheersbaarheid van het verstrekken van toegang tot de informatie

Aantal medewerkers (grootte van organisatie)

In grote organisaties met veel medewerkers is de beheersoverhead voor het voeren van identiteit management en het verstrekken van autorisatie groter. Sterke identiteit management en gebruik van rollen kunnen deze overhead reduceren.
Criterium: Indien het aantal medewerkers van de organisatie groter is dan 500 is dit kenmerk op de organisatie van toepassing.

Instroom / Doorstroom van medewerkers

Veel medewerkers verlaten na een korte periode het bedrijf en worden vervangen door nieuwe medewerkers of medewerkers stromen door intern binnen het bedrijf en blijven dus niet lang op dezelfde functie zitten. Door deze grote instroom, uitstroom of doorstroom nemen de beheerswerkzaamheden voor het beheren van identiteiten, het uitgeven van authenticatie middelen en het verstrekken van autorisatie toe. Deze toename in beheerswerkzaamheden kan met behulp van een sterke identiteit management en gebruik van rollen worden teruggedrongen.
Criterium: Indien de instroom van medewerkers groter is dan 10% van het totaal aantal medewerkers en/of de doorstroom is groter dan 20% van het totaal aantal medewerkers dan is dit kenmerk op de organisatie van toepassing.

Organisatievorm (structuur)

Geografische spreiding kan niet los gezien worden van de manier waarop de organisatie is gestructureerd. Zijn de afzonderlijke locaties, divisies, vrij autonoom of wordt alles centraal aangestuurd? De organisatiestructuur heeft invloed op de beheersbaarheid van de identiteiten van medewerkers.
Criterium: Indien het beleid niet geheel centraal wordt bepaald, is dit kenmerk op de organisatie van toepassing.

Sociale controle

Sociale controle is vaak in kleine bedrijven zeer hoog. In grotere bedrijven vervaagt de sociale controle omdat het voor medewerkers moeilijker is in te schatten wie er nu allemaal werkzaam zijn bij de organisatie en wie niet. Daarom moeten uitgifte processen van rechten en authenticatie middelen met meer controle zijn omgegeven.
Criterium: Indien onbekende mensen binnen de organisatie kunnen rondlopen zonder te worden aangesproken, is dit kenmerk op de organisatie van toepassing.

5.3.4 Groep 4: Positie van de organisatie in de maatschappij

Doelgroep

De doelgroep die een organisatie probeert aan te spreken heeft invloed op de toegangsbeveiliging. Want door zich op bepaalde doelgroepen te richten kan een organisatie gevoeliger worden voor aanvallen op de informatie en informatievoorziening en deze dient dus zwaarder beveiligd te zijn. Doordat bijvoorbeeld een organisatie zich richt op de consument, krijgt de organisatie een grotere naamsbekendheid onder het grote publiek en zal deze dus eerder als doelwit worden gekozen.
Criterium: Indien de doelgroep onder andere bestaat uit de consument, is dit kenmerk op de organisatie van toepassing.

Omstreden activiteiten

Bedrijven waarbij de activiteiten liggen op een vlak die door bepaalde groepen in de maatschappij worden afgekeurd, zijn extra gevoelig voor sabotage van deze groepen. Toegangsbeveiliging van gevoelige informatie moet voor dit soort bedrijven dus op een hoog niveau zitten.
Criterium: Indien een organisatie “omstreden activiteiten” heeft, is dit kenmerk van toepassing op de organisatie.

Wet & Regelgeving

Organisaties die niet gebonden zijn aan Wet & Regelgeving op het gebied van security hoeven hier dus ook minder aandacht aan te besteden of besteden hier ten onrechte minder aandacht aan.
Criterium: Indien een organisatie in grote mate onderhevig is aan specifieke Wet & Regelgeving is dit kenmerk van toepassing op de organisatie.

5.4 Toegangsbeveiligingsmaatregelen

De financiële en overige consequenties die optreden bij schending van de betrouwbaarheid en het risicoprofiel van een organisatie bepaalt de noodzaak tot het nemen van maatregelen. Er zijn veel maatregelen die een organisatie kan toepassen. Sommige zijn kostbaar om te implementeren andere wat minder. Daarnaast zijn losse maatregelen vaak niet effectief. Het totaal aan maatregelen moet een coherent geheel zijn.
Het model verdeelt de noodzaak tot het nemen van maatregelen in drie niveau’s. Voor elk niveau moet een bijpassende set maatregelen beschikbaar zijn. Het samenstellen van het pakket maatregelen per niveau is gedaan in overleg met adviseurs van VKA op basis van hun expertkennis. Dit had als resultaat een set met: lichte maatregelen, middelmatige maatregelen en zware maatregelen. De maatregelen uit de verschillende sets zijn opgebouwd uit de drie kerngebieden van toegangsbeveiliging. Binnen een kerngebied is weer een onderverdeling gemaakt naar drie subgebieden. De drie kerngebieden met hun subgebieden zijn:

- Identiteit Management
    - Informatie & Controle
    - Traceerbaarheid
    - Beheersbaarheid
- Authenticatie Management
    - Sterkte authenticatie
    - Controle uitgifte proces
    - Incident management
- Autorisatie Management
    - Granulariteit (rollen en content)
    - Toekenningproces (Controle & Functiescheiding)
    - Controle gebruik

Bij elk subgebied hoort tenminste één lichte, één middelmatige en één zware toegangsbeveiligingsmaatregel die correspondeert met de lichte, middelmatige of zware set met maatregelen. Hieronder worden de maatregelen per kerngebied en subgebied behandeld.

5.4.1 Identiteit Management

Het gebied identiteit management is onderverdeeld in drie subgebieden:

- Informatie & Controle
- Traceerbaarheid
- Beheersbaarheid

Informatie & Controle

Informatie samen met de controle van deze informatie moet vertrouwen creëren in het feit dat een identiteit te herleiden is tot een bepaalde entiteit. Er moet genoeg informatie worden aangedragen die vervolgens gecontroleerd dient te worden op juistheid zodat het gewenste niveau van vertrouwen bereikt kan worden. De eisen aan de informatie die gebruikers aandragen en de controle die hierop plaats vindt zal niet voor elke groep gebruikers hetzelfde zijn. Bij klanten en partners zal de aangedragen informatie veelal anders van aard zijn en de controle hierop veelal uitgebreider omdat bij deze groep gebruikers het "face to face" contact meestal ontbreekt, dit in tegenstelling tot de medewerkers van een bedrijf.

Traceerbaarheid

Bij traceerbaarheid draait het om het herleiden van gedane handelingen naar een identiteit. Hierbij is het belangrijk dat een gebruiker uniek wordt geïdentificeerd en dat de handelingen die worden verricht ook worden vastgelegd.

Beheersbaarheid

Beheersbaarheid omvat de mate waarin de identiteiten en de bijbehorende identifiers correct en efficiënt te beheren zijn. Van invloed hierop zijn:

- hoe en waar de identifiers (login-accounts) beheerd worden. Mogelijke voorbeelden zijn: decentraal per applicatie, centraal per applicatie of centraal voor de geïntegreerde informatievoorziening.
- de mate waarin Single Sign On binnen een organisatie is doorgevoerd.
- hoe wordt omgegaan met identiteiten die binnen een organisatie meerdere rollen hebben, zoals een medewerker die ook klant van een organisatie is of een medewerker die zowel gebruiker van een systeem is als beheerder van een systeem.

Voor de bovenstaande subgebieden zijn de maatregelen op zwaar, middelmatig en licht niveau weergegeven in onderstaande tabel:

	Licht	Middelmatig	Zwaar
Informatie & Controle	Geen controle	Vertrouwen in afgeleide identificatie	Directe identificatie + controle onafhankelijke informatiebron
Traceerbaarheid	Functionele id	Uniek user-id	Uniek user-id + logging
Beheersbaarheid	Decentraal per applicatie	Centraal per applicatie	Centraal voor de geïntegreerde informatievoorziening
	Geen SSO	Geen SSO	SSO

Tabel 3: Lichte, middelmatige en zware maatregelen voor de subgebieden van identiteit management

5.4.2 Authenticatie management

Het gebied authenticatie management is onderverdeeld in drie subgebieden:

- Sterkte authenticatie
- Controle uitgifte proces
- Incident management

Sterkte authenticatie

Het authenticatie middel moet er voor zorgen dat alleen de persoon die behoort bij een bepaalde identiteit, gebruik maakt van deze identiteit. Door te variëren in de sterkte van het authenticatiemiddel kan men meer of minder vertrouwen hebben dat de identiteit alleen door de rechthebbende wordt gebruikt.

Controle uitgifte proces

Controle op het uitgifte proces van authenticatie middelen moet er voor zorgen dat alleen entiteiten authenticatie middelen voor bepaalde voorzieningen krijgen die daar recht op hebben. Door een strenger uitgifte proces in te stellen kan met een grotere zekerheid worden bepaald of iemand recht heeft op toegang tot bepaalde middelen.

Incident management

Incident management moet zorgen voor een groter vertrouwen in de levenscyclus van het authenticatiemiddel. Door adequaat incident management kan voorkomen worden dat authenticatie middelen in verkeerde handen komen en misbruikt kunnen worden.

Voor de bovenstaande subgebieden zijn de maatregelen op zwaar, middelmatig en licht niveau weergegeven in onderstaande tabel:

	Licht	Middelmatig	Zwaar
Sterke authenticatie	één factor	Sterke één factor, bijvoorbeeld wachtwoord dat aan veel eisen moet voldoen	twee factor
Controle uitgifte proces	Niet	Bevestigd	Bewezen
Incident management	Niet	Periodiek (batch)	In het proces

Tabel 4: Lichte, middelmatige en zware maatregelen voor de subgebieden van authenticatie management

5.4.3 Autorisatie management

Het gebied autorisatie management is onderverdeeld in drie subgebieden:

- Granulariteit (rollen en content)
- Toekenning proces (Controle & Functiescheiding)
- Controle gebruik

Granulariteit (rollen en content)

Met granulariteit wordt bedoeld de mate van fijnmazigheid. Hoe groter/fijner de granulariteit des te nauwkeuriger iets ingedeeld kan worden. Voor rollen betekent dit dat bij een fijnere granulariteit er meer rollen zijn waarlangs een gebruiker kan worden ingedeeld en dus de rol die een gebruiker krijgt toegewezen beter bij het profiel van de gebruiker past. Voor content geldt hetzelfde, de content kan bij een grotere granulariteit beter worden geclassificeerd waardoor beter kan worden bepaald wie toegang tot de data krijgt.

Toekenning proces (Controle & Functiescheiding)

De manier waarop rechten aan gebruikers worden toegekend bepaalt de zekerheid waarmee de juiste rechten aan de juiste gebruikers worden toegekend. Door controle uit te oefenen op het uitgeven van rechten of door functiescheiding toe te passen bij het uitgeven van rechten kan voorkomen worden dat gebruikers verkeerde rechten krijgen toegewezen of dat rechten worden toegekend terwijl men daartoe niet bevoegd was.

Controle gebruik

Controle op het gebruik zorgt ervoor dat de rechten die een gebruiker heeft continue in balans zijn met zijn werkzaamheden. Gebruikers switchen namelijk nog wel eens van functie binnen een organisatie en bij elke functie horen weer andere rechten. Hierdoor kan ontstaan dat gebruikers in de loop der tijd rechten gaan verzamelen die ze allang niet meer nodig hebben.

Voor de bovenstaande subgebieden zijn de maatregelen op zwaar, middelmatig en licht niveau weergegeven in onderstaande tabel:

Maatregelen	Licht	Middelmatig	Zwaar
Granulariteit	Alles of niet	Grof	Fijn
Toekenningproces (Controle & Functie scheiding)	Geen	Controle of functie scheiding	Controle en functie scheiding
Controle gebruik	Niet	Periodiek	Proces

Tabel 5: Lichte, middelmatige en zware maatregelen voor de subgebieden van autorisatie management

5.5 Koppeling tussen organisaties en maatregelen

Om de juiste set met maatregelen te kunnen bepalen voor een organisatie moet er een koppeling komen tussen de gevolgen die optreden bij schending van de betrouwbaarheid, de organisatiekenmerken, in vorm van een risicoprofiel, en de drie sets met maatregelen.
De gevolgen die optreden bij schending van de betrouwbaarheid zijn onderverdeeld naar de gevolgen die optreden indien het gewenste niveau van:

- vertrouwelijkheid niet wordt gehaald op een schaal van laag / middelmatig / hoog.
- integriteit niet wordt gehaald op een schaal van laag /middelmatig / hoog.
- beschikbaarheid niet wordt gehaald op een schaal van laag /middelmatig / hoog.

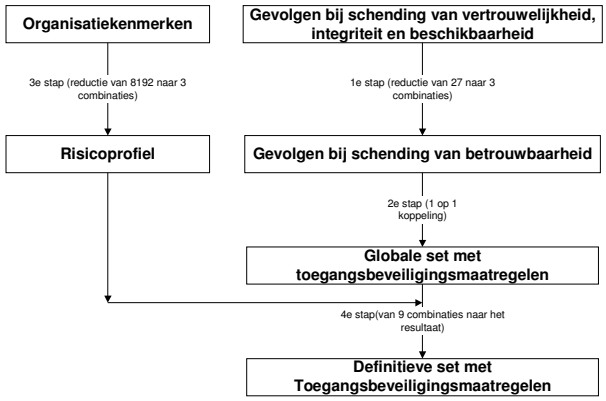
Zie hiervoor ook §5.2. De gevolgen bij schending van de betrouwbaarheid geven dus 3^3 (27) combinaties die van toepassing kunnen zijn op een organisatie.

De organisatiekenmerken, die het risico inventariseren, worden samengevat in drie risicoprofielen, zie hiervoor ook §5.3. Er kunnen totaal 13 relevante organisatiekenmerken onderscheiden worden die elk wel of niet van toepassing zijn op een organisatie. Dit geeft dus 2^{13} combinaties van organisatiekenmerken die van toepassing kunnen zijn op een organisatie.
Om de juiste set met maatregelen te bepalen voor een organisatie moet het model dus een koppeling leggen tussen de mogelijke combinaties van betrouwbaarheidseisen en organisatiekenmerken enerzijds en de drie set met maatregelen anderszijds. Dit geeft uiteindelijk 3^3 x 2^{13} (221184) combinaties. Elke combinatie van betrouwbaarheidseisen en organisatiekenmerken heeft dus één corresponderende set met maatregelen en aan elke set met maatregelen kunnen dus verbonden zijn met meerdere combinaties van betrouwbaarheidseisen en organisatiekenmerken.

Het direct leggen van 221174 koppelingen geeft een model dat, misschien wel feitelijk juist, niet te begrijpen is door de gebruiker of ontwerper van het model. Zo'n model maakt de koppeling tussen de organisatie en de maatregelen niet inzichtelijk en is dus ook niet controleerbaar.
In het toegangsbeveiligingsmodel zijn een aantal tussenstappen ingevoerd zodat er een koppeling blijft bestaan tussen alle combinaties van betrouwbaarheidseisen en organisatiekenmerken en dat het model begrijpbaar en controleerbaar is voor gebruiker en ontwerper van het model. Deze tussenstappen zijn:

1) het samenvoegen van de drie variabelen: gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid tot één variabele: "gevolgen bij schending van betrouwbaarheid" op een schaal van laag / middelmatig / hoog. Dit reduceert het aantal combinaties met een factor negen.
2) het koppelen van de drie mogelijke waardes, laag /middelmatig /hoog, van "gevolgen bij schending van betrouwbaarheid" aan een corresponderende set met maatregelen.
3) het opstellen van drie risicoprofielen op basis 13 organisatiekenmerken. Dit reduceert het aantal combinaties van 2^{13} tot drie.
4) de gekozen set met maatregelen uit de eerste stap aanscherpen op basis van het risicoprofiel uit de 2^e stap.

Bovenstaande tussenstappen worden na elkaar uitgevoerd en zorgen ervoor dat er nog maar 9 combinaties van "gevolgen bij schending van betrouwbaarheid" en risicoprofielen direct worden gekoppeld aan een set met maatregelen waardoor het model inzichtelijker en begrijpelijker wordt. Het nadeel hiervan is uiteraard dat er keuzes gemaakt moeten worden hoe bepaalde informatie moet worden geaggregeerd. Hierdoor gaat informatie verloren.
De diversen stappen zijn in figuur 13 weergegeven.



Figuur 13: De stappen van het toegangsbeveiligingsmodel gedetailleerd weergegeven.

In het begin van hoofdstuk 5 wordt echter gesproken over twee stappen, in plaats van vier, zoals ook blijkt uit figuur 12. Daar wordt namelijk voor de eenvoud stap één en twee samengenomen tot de eerste stap van het model en stap drie en vier samengenomen tot de tweede stap van het model. Een nauwkeurigere indeling in stappen is namelijk voor het gebruik van het model niet noodzakelijk en werkt verwarrend, maar om het model te kunnen doorgronden is het noodzakelijk om onderscheid te maken tussen deze vier stappen.
Hieronder worden de stappen één voor één toegelicht. Hierbij worden stap 1 en 2 gezamenlijk besproken omdat in stap 2 geen informatie wordt samengevoegd. In stap 2 is namelijk sprake van een één op één koppeling van “gevolgen bij schending van betrouwbaarheid” naar een set met maatregelen en andersom.

5.5.1 Stap 1 en 2

De éérste twee stappen leggen de koppeling tussen de 27 mogelijke combinaties van “gevolgen bij schending van de betrouwbaarheid” en de diverse sets met maatregelen. Voor het maken van deze tussenstap is een algoritme nodig op basis waarvan bepaald wordt hoe de 27 combinaties tot drie combinaties worden gereduceerd. Deze drie combinaties worden vervolgens één op één gekoppeld aan een set met maatregelen met hetzelfde classificatieniveau. In dit model is gekozen om te kijken naar de meerderheid van stemmen. Hierbij wordt begonnen om allereerst te bepalen welke combinaties als hoog worden geclassificeerd om vervolgens te bepalen welke combinaties als middelmatig worden geclassificeerd. De overgebleven combinaties worden dan vervolgens als laag geclassificeerd. Deze volgorde van classificeren zorgt ervoor dat bij een meerderheid van stemmen een combinatie eerder te hoog wordt geclassificeerd dan te laag wordt geclassificeerd. Vooral vanuit het oogpunt van informatiebeveiliging kan men beter iets te veel beveiligen dan iets te weinig beveiligen.
Samengevat worden de combinaties als volgt geaggregeerd tot één betrouwbaarheidseis en vervolgens gekoppeld aan een set met maatregelen:

- **keuze voor de set met zware maatregelen:** indien bij twee van de drie categorieën (vertrouwelijkheid, integriteit, beschikbaarheid) de gevolgen bij schending hiervan als groot zijn geclassificeerd.
- **keuze voor de set met middelmatige maatregelen:** indien er niet voldaan is aan de criteria voor de set met zware maatregelen **en** indien bij twee van de drie categorieën de gevolgen bij schending hiervan tenminste als gemiddeld zijn geclassificeerd.

- **keuze voor de set met lichte maatregelen:** indien er niet voldaan is aan de criteria voor de sets met middelmatige en zware maatregelen.

De uitwerking van bovenstaand algoritme is uitgewerkt in tabel 6. Deze tabel bevat namelijk alle mogelijke combinaties die gemaakt kunnen worden met de gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid.

	Gevolgen bij schending van			Set met maatregelen		
Rij	Vertrouwelijkheid	Integriteit	Beschikbaarheid	Zwaar	Middelmatig	Licht
1	Groot	Groot	Groot	+		
2	Groot	Groot	Gemiddeld	+		
3	Groot	Groot	Klein	+		
4	Groot	Gemiddeld	Groot	+		
5	Groot	Gemiddeld	Gemiddeld		+	
6	Groot	Gemiddeld	Klein		+	
7	Groot	Klein	Groot	+		
8	Groot	Klein	Gemiddeld		+	
9	Groot	Klein	Klein			+
10	Gemiddeld	Groot	Groot	+		
11	Gemiddeld	Groot	Gemiddeld		+	
12	Gemiddeld	Groot	Klein		+	
13	Gemiddeld	Gemiddeld	Groot		+	
14	Gemiddeld	Gemiddeld	Gemiddeld		+	
15	Gemiddeld	Gemiddeld	Klein		+	
16	Gemiddeld	Klein	Groot		+	
17	Gemiddeld	Klein	Gemiddeld		+	
18	Gemiddeld	Klein	Klein			+
19	Klein	Groot	Groot	+		
20	Klein	Groot	Gemiddeld		+	
21	Klein	Groot	Klein			+
22	Klein	Gemiddeld	Groot		+	
23	Klein	Gemiddeld	Gemiddeld		+	
24	Klein	Gemiddeld	Klein			+
25	Klein	Klein	Groot			+
26	Klein	Klein	Gemiddeld			+
27	Klein	Klein	Klein			+

Tabel 6: Keuze voor een set van lichte, middelmatige of zware maatregelen op basis van de criteria uit de eerste en tweede stap.

5.5.2 Stap 3

In de éérste twee stappen is een koppeling gelegd tussen 27 mogelijke combinaties van “gevolgen bij schending van de betrouwbaarheid” en de drie sets met maatregelen. In de derde stap wordt op basis van de 13 organisatiekenmerken 3 risicoprofielen aangemaakt waardoor de bijdrage van de organisatiekenmerken van 2^{13} naar 3 mogelijkheden wordt gereduceerd. Vervolgens kan hiermee in de vierde stap de keuze voor een set met maatregelen worden aangescherpt.
Voor het maken van deze tussenstap is een algoritme nodig op basis waarvan bepaald wordt hoe de 2^{13} combinaties tot drie combinaties worden gereduceerd. In dit model is gekozen om te kijken naar de meerderheid van stemmen en minderheid van stemmen binnen een groep van organisatiekenmerken en om aan bepaalde groepen met organisatiekenmerken meer gewicht te hangen. Hierbij wordt begonnen om allereerst te bepalen welke combinaties als hoog worden geclassificeerd, op basis van de meerderheid van stemmen, om vervolgens te bepalen welke combinaties als laag worden geclassificeerd, op basis van minderheid van stemmen. De overgebleven combinaties worden dan vervolgens als middelmatig geclassificeerd. Deze volgorde van classificeren zorgt ervoor dat indien er heel veel kenmerken op een organisatie van toepassing zijn of indien een groep met kenmerken heel sterk is vertegenwoordig deze organisatie in een hoog risicoprofiel terecht komt en indien heel weinig kenmerken op een organisatie van toepassing zijn

deze in een laag risicoprofiel terecht komt. Indien een organisatie er een beetje tussen in zit dan komt deze in het middelmatige risicoprofiel. Daarnaast wordt extra gewicht gegeven aan de groepen 1, “toegang tot de informatie van buiten de organisatie”, en 2,” toegang tot de informatie van binnen de organisatie”, om te voorkomen dat een organisatie te makkelijk in het lage risicoprofiel wordt ingedeeld terwijl de informatievoorziening van de organisatie naar de buitenwereld erg open is. Verder zijn voor de bepaling van de indeling in het hoge risicoprofiel de groepen 2 en 3 samengenomen omdat groep 2 te klein is en dus te makkelijk een meerderheid aan stemmen heeft.

Samengevat worden de combinaties van organisatiekenmerken als volgt geaggregeerd tot 3 risicoprofielen:

- **profiel met een hoog risico**
  Een organisatie wordt ingedeeld in het profiel met een hoog risico indien:
  - Uit groep 1 het merendeel van de kenmerken van toepassing zijn op de organisatie (dus tenminste drie van de vier)
    of
  - Uit groep 2 en 3 samen het merendeel van de kenmerken van toepassing zijn op de organisatie (dus tenminste vier van de zes)
    of
  - Uit groep 4 het merendeel van de kenmerken van toepassing zijn op de organisatie (dus tenminste twee van de drie)

- **profiel met laag risico**
  Een organisatie wordt ingedeeld in het profiel met een laag risico indien:
  - Uit groep 1 geen kenmerken van toepassing zijn op de organisatie
    en
  - Uit groep 2 geen kenmerken van toepassing zijn op de organisatie
    en
  - Uit groep 3 maximaal één kenmerk van toepassing is op de organisatie
    en
  - Uit groep 4 maximaal één kenmerk van toepassing is op de organisatie

- **profiel met een normaal risico**
  Een organisatie wordt ingedeeld in het profiel met een normaal risico indien:
  - De organisatie niet voldoet aan het profiel met een laag risico
    en
  - De organisatie niet voldoet aan het profiel met een hoog risico

5.5.3 Stap 4

In de vierde stap wordt de keuze van een set met maatregelen uit de tweede stap aangescherpt op basis van het risicoprofiel uit stap drie. In dit model gebeurt dit op basis van afwijking van het normale risicoprofiel. Tijdens de tweede stap zijn we er namelijk impliciet vanuit gegaan dat de organisatie voldoet aan een normaal risicoprofiel door de risico’s tijdens die stap niet mee te nemen. Elke organisatie heeft namelijk te maken met bepaalde risico’s met betrekking tot het beschermen

van de betrouwbaarheid van de informatievoorziening. Dit gegeven is impliciet meegenomen bij het koppelen van gevolgen bij schending van de betrouwbaarheid aan een set met maatregelen. Indien het risico dat een organisatie loopt echter hoger is dan normaal, komt de organisatie in een hoger risicoprofiel terecht en dient dus de keuze voor een set met maatregelen naar boven te worden bijgesteld. Indien het risico dat een organisatie loopt lager is dan normaal, dient de keuze voor een set met maatregelen naar beneden te worden bijgesteld. Hieronder is per risicoprofiel uitgelegd welke gevolgen dit heeft voor de uiteindelijke set met maatregelen.

De organisatie bevindt zich in het lage risicoprofiel

Indien het lage risicoprofiel van toepassing is op de organisatie, dient de keuze voor een set met maatregelen naar beneden te worden bijgesteld. In tabel 7 zijn de mogelijke verschuivingen tussen de sets met maatregelen weergegeven.

Keuze na 1e stap	Keuze na 2e stap		
	Licht	Middelmatig	Zwaar
Licht	X		
Middelmatig	X ←		
Zwaar		X ←	

Tabel 7: Verandering van keuze van maatregelen na de vierde stap op basis van het lage risicoprofiel

De organisatie bevindt zich in het normale risicoprofiel

Indien het normale risicoprofiel van toepassing is op de organisatie, blijft de keuze uit de tweede stap gehandhaafd.

De organisatie bevindt zich in het hoge risicoprofiel

Indien het hoge risicoprofiel van toepassing is op de organisatie, dient de keuze voor een set met maatregelen naar boven te worden bijgesteld. In
tabel 8 zijn de mogelijke verschuivingen tussen de sets met maatregelen weergegeven.

Keuze na 1e stap	Keuze na 2e stap		
	Licht	Middelmatig	Zwaar
Licht	→	X	
Middelmatig		→	X
Zwaar			X

Tabel 8: Verandering van keuze van maatregelen na de vierde stap

5.5.4 Geautomatiseerd zoeken naar optimale algoritmes voor de stappen 1 t/m 3

In paragraaf §5.5.1 t/m §5.5.3 zijn op logische gronden bepaalde keuzes gemaakt om tijdens stap een,drie en vier van het model het aantal mogelijke koppelingen tussen de organisatie enerzijds en de sets met maatregelen anderzijds te reduceren. De keuzes die tijdens deze stappen gemaakt zijn kunnen er voor zorgen dat de uiteindelijke koppeling tussen organisaties en de sets met maatregelen niet optimaal is.

Met behulp van een computer kan men doorrekenen of er een beter criterium is op basis waarvan:

- de gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid worden samengevoegd tot één component: gevolgen bij schending van betrouwbaarheid.
- de 13 organisatiekenmerken worden samengevoegd tot 3 risicoprofielen.

- een set met maatregelen wordt geselecteerd voor een organisatie op basis van “gevolgen bij schending van betrouwbaarheid” en het risicoprofiel.

Hiervoor moet men aan de hand van test gegevens en aan de hand van een optimalisatie algoritme uitrekenen wat de meest optimale criteria zijn. De testgegevens moeten dan bestaan uit een lijst met organisaties waarbij bekend is:

- welke gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid van toepassing zijn op een organisatie.
- welke kenmerken van toepassing zijn op een organisatie.
- welke maatregelen voor die organisatie moeten worden gehanteerd op basis van expertkennis.

Daarnaast moet de lijst met testgegevens genoeg organisaties bevatten waarover bovenstaande bekend is om zo te beschikken over een set met trainingsgegevens en een set met gegevens om de gevonden optimale criteria te valideren.
Het optimalisatie algoritme moet zo gekozen worden:

- dat er een oplossing gevonden wordt die optimaal is met betrekking tot het aantal foutief geclassificeerde organisaties. Een oplossing met geen fouten vindt je zelden.
- dat de oorzaak, waardoor een aantal organisaties foutief geclassificeerd zijn, de minste gevolgen heeft voor de foutief geclassificeerde organisatie. Zo kan het bijvoorbeeld erger zijn dat een organisatie foutief wordt geclassificeerd omdat de keuze van de maatregelen te licht is dan weer de organisatie foutief wordt geclassificeerd omdat de keuze van de maatregelen te zwaar is. Men kan een voorkeur hebben voor te veel beveiligen ten opzichten van te weinig beveiligen.

De kans dat een oplossing wordt gevonden waarbij alle organisaties worden geclassificeerd is niet echt groot. Daarom moet zoals hierboven vermeld een optimalisatie algoritme een voorkeur hebben voor ten eerste natuurlijk correct geclassificeerde organisaties en ten tweede voor foutieve classificatie oorzaken die niet al te grote gevolgen voor de geclassificeerde organisatie heeft. Deze voorkeur voor foutieve classificatie oorzaken kunnen zijn:

- voorkeur voor een minimale afstand tussen classificatie uit model en gewenste classificatie. Bijvoorbeeld laag worden geclassificeerd terwijl in werkelijkheid men hoog classificeert dient te worden is erger dan wanneer men middelmatig wordt geclassificeerd in men in werkelijkheid hoog geclassificeerd dient te worden.
- voorkeur voor overschatting van de classificatie. Indien men liever een oplossing heeft waarbij organisaties te hoog worden geclassificeerd dan te laag worden geclassificeerd zodat organisaties nooit te weinig beveiligd zijn. Liever iets te veel kosten maken dan te weinig beveiligen.
- voorkeur voor onderschatting van de classificatie. Indien men liever een oplossing heeft waarbij organisaties te laag worden geclassificeerd dan te hoog worden geclassificeerd zodat de kosten binnen de perken blijven. Liever iets te weinig beveiligen dan te veel kosten maken.

Het doorrekenen met behulp van een computer van alle mogelijke criteria is echter omslachtig. Er moeten namelijk optimale grenzen bepaald worden waarlangs:

- alle combinaties van gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid worden toegekend aan een lage, middelmatige of hoge classificatie. Dit kost 3^6 berekening. 3^3 berekening voor het bepalen van de grens tussen hoge en middelmatige classificatie en 3^3 berekeningen voor het bepalen van de grens tussen middelmatige en lage classificatie.
- elke combinatie van organisatiekenmerken wordt toegekend aan slechts één van de drie risicoprofielen. Dit kost 2^{26} berekeningen, 2^{13} berekeningen voor het bepalen van de grens tussen classificatie in het hoge of middelmatige risicoprofiel en 2^{13} berekeningen voor het bepalen van de grens tussen classificatie in het middelmatige of lage risicoprofiel.
- elke combinatie van "gevolgen bij schending van betrouwbaarheid" met een risicoprofiel wordt toegekend aan exact één set met maatregelen. Dit kost 3^2 berekeningen, drie berekeningen om de grens te bepalen tussen hoge en middelmatige classificatie en drie berekeningen om de grens te bepalen tussen middelmatige en lage classificatie.

Het aantal berekeningen dat moet worden uitgevoerd indien de computer als een blind paard alle mogelijkheden grenzen narekent komt dan op $3^6 \times 2^{26} \times 3^2$ berekeningen. Afgerond komt dit neer op $4{,}4 \times 10^{11}$ berekeningen. Indien men de combinaties van grenzen weglaat die niet mogelijk zijn dan zal het aantal berekeningen lager uitkomen, maar de orde van grootte zal niet echt veranderen. Zelfs voor een moderne PC is deze orde van grootte een opgave waar de PC enkele dagen tot enkele weken of misschien wel maanden aan moet rekenen. Uiteraard afhankelijk van de omvang van de test gegevens. De meer test gegevens aanwezig zijn des te meer informatie aanwezig is om de optimale oplossing te vinden, maar dit is niet bevordelijk voor het vinden van een oplossing. Domweg alle mogelijkheden narekenen is dus niet de beste optie. Om via een geautomatiseerde weg de optimale grenzen te vinden zou men gebruik moeten maken van een "slim" optimalisatie algoritme. Bij de meeste "slimme" optimalisatie algoritmes is het echter niet gegarandeerd dat de beste oplossing gevonden wordt.

6 Toets

Het model uit hoofdstuk 5 is een theoretisch model waarin gebruik gemaakt wordt van expertkennis en waarin op logische gronden een aantal keuzes gemaakt zijn. Het blijft natuurlijk de vraag of de gemaakte keuzes in stap 1 t/m 4 van het model de juiste keuzes zijn en of de op basis van expertkennis samengestelde sets met maatregelen de juiste zijn. Om dit te kunnen toetsen is een enquête gehouden onder een aantal organisaties. Onder de organisaties die aan deze enquête hebben meegewerkt bevinden zich diverse bancaire instellingen, overheidsorganen en diverse aan de AEX genoteerde organisaties. Totaal hebben 23 organisaties een enquête ingevuld.

In bijlage C zijn de vragen uit de enquête na te lezen.
De deelnemers aan de enquête is gevraagd aan te geven:

- welke kenmerken op hun organisatie van toepassing zijn, zie deel I van de enquête. Deze vragen corresponderen met de gegevens die nodig zijn in stap 3 van het model, zie hiervoor §5.5.3.
- wat de gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid zijn voor hun organisatie, zie deel II van de enquête. Deze vragen corresponderen met de gegevens die nodig zijn in stap 1 van het model, zie hiervoor §5.5.1.
- welke toegangsbeveiligingsmaatregelen voor hun organisatie genomen moeten worden zodat de te maken kosten van beveiliging in evenwicht zijn met de verwachte financiele consequenties bij niet halen van de gewenste betrouwbaarheid, zie deel III van de enquête. Deze vragen zouden in een ideale situatie moeten corresponderen met de uitkomst van het toegangsbeveiligingsmodel.

Ten tijde van de afname van de enquête was het toegangsbeveiligingsmodel nog niet volledig afgerond. Dit heeft een aantal gevolgen:

- bepaalde vragen uit de enquête corresponderen niet voor de volledige 100% met de onderdelen van het model waarvoor ze nodig zijn. Voor bepaalde vragen is daarom een vertaalslag gemaakt voordat de gegevens van die desbetreffende één op één correspondeerde met de gegevens die nodig zijn om het model te kunnen testen. In bijlage D wordt hier verder op ingegaan.
- niet alle vragen worden gebruikt om het uiteindelijke model te toetsen omdat bepaalde gegevens in het uiteindelijke model niet meer nodig zijn. Daarnaast zijn een aantal vragen gesteld die nooit tot doel hadden om het model te toetsen, zoals de vragen uit deel IV van de enquête.

Met behulp van de gegevens uit deel I en deel II van de enquête is per organisatie een risicoprofiel en een classificatie voor “gevolgen bij schending van betrouwbaarheid” bepaald. Deze gegevens zijn voor de 23 organisatie in tabel 9 weergegeven. Op basis van deze gegevens is met behulp van het model een classificatie bepaald voor een set met maatregelen. De uitkomst hiervan kan zijn een set met lichte, middelmatige of zware maatregelen. Deze classificatie zou moeten corresponderen met de classificatie die volgt uit deel III van de enquête. Idealiter zou de kolom ‘model’ in tabel 9 moeten corresponderen met de kolom ‘enquête’.

	Input		Toegangsbeveiliging	
Bedrijf	Betrouwbaarheidseis	Risicoprofiel	Model	Enquete
1	Hoog	Hoog	Hoog	Hoog
2	Middelmatig	Hoog	Hoog	Middelmatig
3	Hoog	Hoog	Hoog	Middelmatig
4	Middelmatig	Hoog	Hoog	Middelmatig
5	Middelmatig	Hoog	Hoog	Hoog
6	Middelmatig	Hoog	Hoog	Hoog
7	Middelmatig	Hoog	Hoog	Hoog
8	Hoog	Hoog	Hoog	Hoog
9	Middelmatig	Hoog	Hoog	Hoog
10	Middelmatig	Hoog	Hoog	Hoog
11	Hoog	Hoog	Hoog	Hoog
12	Laag	Hoog	Middelmatig	Middelmatig
13	Middelmatig	Hoog	Hoog	Hoog
14	Middelmatig	Hoog	Hoog	Middelmatig
15	Middelmatig	Hoog	Hoog	Hoog
16	Middelmatig	Hoog	Hoog	Hoog
17	Hoog	Hoog	Hoog	Hoog
18	Hoog	Hoog	Hoog	Middelmatig
19	Middelmatig	Hoog	Hoog	Middelmatig
20	Laag	Hoog	Middelmatig	Middelmatig
21	Middelmatig	Hoog	Hoog	Hoog
22	Middelmatig	Hoog	Hoog	Middelmatig
23	Middelmatig	Middelmatig	Middelmatig	Middelmatig

Tabel 9: Toetsing toegangsbeveiligingsmodel met behulp van de enquête.

De classificatie volgens het model is echter niet voor alle organisaties gelijk aan de classificatie volgens de enquête. In zeven van de 23 gevallen zit het model er naast.

6.1 Geautomatiseerd zoeken naar de optimale oplossing

Het is goed mogelijk dat de keuzes die gemaakt zijn in §5.5.1 t/m §5.5.3 niet de optimale keuzes zijn en als gevolg daarvan het model in 7 van de 23 gevallen organisaties verkeerd classificeert. Zoals besproken in §5.5.4 kan met behulp van testgegevens gezocht worden naar de optimale grenzen waarlangs organisaties:

- laag, middelmatig of hoog worden geclassificeerd met betrekking to "gevolgen bij schending van betrouwbaarheid", zie stap 1 van het model in §5.5.1.
- aan een laag,middelmatig of hoog risicoprofiel worden toegewezen, zie stap 3 van het model in §5.5.2.
- aan een lage,middelmatige of hoge set met maatregelen worden toegewezen, zie stap 4 van het model in §5.5.2.

Zoals §5.5.4 besproken is het narekenen van alle combinaties een te tijdrovende operatie. Om toch een idee te krijgen of er een betere oplossing te vinden is, is met behulp van een computer alle mogelijke combinaties van stap 1 en 2 afzonderlijk en van stap 1 en 2 gezamenlijk doorgerekend. De resultaten zijn hieronder weergegeven.

Het doorrekenen van alle mogelijke combinaties van stap 1

Voor het vinden van een optimale oplossing doormiddel van het doorrekenen van alle mogelijk combinaties bij stap 1 moeten totaal 3^6 mogelijke combinaties worden bekeken. Van de 3^6 mogelijke combinaties zijn maar 513 combinaties bruikbaar voor het model aangezien uitgesloten is dat de

grens tussen middelmatig en hoog lager kan liggen dan de grens tussen middelmatig en laag en aangezien uitgesloten is dat beide grenzen aan elkaar gelijk mogen zijn. Daarnaast zijn alle mogelijke combinaties bij stap 1 doorgerekend met verschillende voorkeuren van het optimalisatie algoritme, zie §5.5.4 voor een toelichting hierop. De resultaten zijn weergegeven in tabel 10.

Aantal gevonden oplossingen	Aantal foutief geclassificeerde	Optimalisatie voorkeur
23	8	Geen voorkeur. Elke foutieve classificatie teld even zwaar.
23	8	Voorkeur voor een minimale afwijking bij foutieve classificatie.
1	8	Voorkeur voor te hoge classificatie bij foutieve classificatie.
23	8	Voorkeur voor te lage classificatie bij foutieve classificatie.

Tabel 10: Optimaliseren model op basis van stap 1 van het algoritme.

Het doorrekenen van alle mogelijke combinaties van stap 3

Voor het vinden van een optimale oplossing doormiddel van het doorrekenen van alle mogelijk combinaties bij stap 3 moeten totaal 2^{26} mogelijke combinaties worden bekeken. Van de 2^{26} mogelijke combinaties zijn maar 65514541 combinaties bruikbaar voor het model aangezien uitgesloten is dat de grens tussen middelmatig en hoog lager kan liggen dan de grens tussen middelmatig en laag en aangezien uitgesloten is dat beide grenzen aan elkaar gelijk mogen zijn. Daarnaast zijn alle mogelijke combinaties bij stap 3 doorgerekend met verschillende voorkeuren van het optimalisatie algoritme, zie §5.5.4 voor een toelichting hierop. De resultaten zijn weergegeven in tabel 11.

Tabel 11: Optimaliseren model op basis van stap 3 van het algoritme.

Aantal gevonden oplossingen	Aantal foutief geclassificeerde	Optimalisatie voorkeur
480	8	Geen voorkeur. Elke foutieve classificatie teld even zwaar.
8160	10	Voorkeur voor een minimale afwijking bij foutieve classificatie.
8160	10	Voorkeur voor te hoge classificatie bij foutieve classificatie.
8160	10	Voorkeur voor te lage classificatie bij foutieve classificatie.

Het doorrekenen van alle mogelijke combinaties van stap 1 en 3

Voor het vinden van een optimale oplossing doormiddel van het doorrekenen van alle mogelijk combinaties bij stap 1 en 3 moeten totaal $3^6 \times 2^{26}$ mogelijke combinaties worden bekeken. Dit een berekening van een dusdanige omvang dat de tijd een beperkende factor begint te worden. Deze berekening is daarom maar slechts één keer uitgevoerd en heeft een uitkomst gegeven aan de hand waarvan slechts 5 van de 23 organisaties foutief worden geclassificeerd. De grenzen behorende bij deze uitkomst zijn in tabel 12 weergegeven.

Grens tussen	Gevolgen bij schending van betrouwbaarheid (vertrouwelijkheid | integriteit | beschikbaarheid)	Organisatiekenmerken (kenmerk 1 t/m 13)
hoog en middelmatig	LAAG | GEMIDDELD | LAAG	0000000101000
middelmatig en laag	LAAG | LAAG | LAAG	0100000000100

Tabel 12: Gevonden grenzen bij geoptimaliseerd model op basis van stap 1 en 3.

De grenzen van “gevolgen bij schending van betrouwbaarheid” moeten als volgt worden geïnterpreteerd om de juist classificatie van te krijgen:

- indien de gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid van een organisatie allemaal groter zijn of gelijk zijn aan de grenswaarde tussen hoog en middelmatig dan wordt de gevolgen bij schending van betrouwbaarheid als hoog geclassificeerd.
- indien de gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid van een organisatie niet allemaal groter zijn of gelijk zijn aan de grenswaarde tussen hoog en middelmatig, maar de gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid van een organisatie zijn wel allemaal groter of gelijk aan de grenswaarde tussen middelmatig en laag dan wordt de gevolgen bij schending van betrouwbaarheid als middelmatig geclassificeerd.
- indien de organisatie niet als hoog of middelmatig kan worden geclassificeerd, wordt de organisatie als laag geclassificeerd.

De grenzen van organisatiekenmerken bestaan uit 13 cijfers corresponderend met de 13 organisatiekenmerken in dezelfde volgorde zoals deze in §5.3 zijn besproken. Het cijfer één geeft aan dat het van belang is dat het kenmerk op de organisatie van toepassing is. Het cijfer nul geeft aan dat het niet uitmaakt of het kenmerk op de organisatie van toepassing is of niet. Vervolgens moeten de grenzen als volgt worden geïnterpreteerd om de organisatie in te kunnen delen in het juiste risicoprofiel:

- indien tenminste de kenmerken die van belang zijn voor de grens tussen hoog en middelmatig van toepassing zijn op de organisatie wordt de organisatie ingedeeld in het hoge risicoprofiel.
- indien niet alle kenmerken die van belang zijn voor de grens tussen hoog en middelmatig van toepassing zijn op een organisatie maar, indien de kenmerken die van belang zijn voor de grens tussen middelmatig en laag wel van toepassing zijn op de organisatie wordt de organisatie ingedeeld in het middelmatige risicoprofiel.
- indien de organisatie niet kan worden ingedeeld in het hoge of middelmatige risicoprofiel wordt de organisatie ingedeeld in het lage risicoprofiel.

7 Conclusie

In deze scriptie is een model opgesteld om een globaal antwoord te geven op de vraag:

Wat is adequate toegangsbeveiliging voor een informatievoorziening die toegankelijk is via publieke netwerken?

Het opgestelde model heeft als doel een antwoord te geven in de goede richting gebaseerd op de organisatie in kwestie, maar is niet bedoeld voor een maat oplossing. Inherent aan modelleren is generaliseren en ook in dit model is gegeneraliseerd zodat het model overzichtelijk blijft maar nog wel bruikbaar is. Indien een organisatie een oplossing op maat wil hebben, moet de organisatie een risicoanalyse laten uitvoeren door experts die hierin getraind zijn.

In deze scriptie is een model opgesteld die aan de volgende randvoorwaarden moest voldoen:

- risico's voor een organisatie dienen globaal te worden geïnventariseerd.
- betrouwbaarheidseisen voor een organisatie dienen globaal te worden geïnventariseerd.
- een gestandaardiseerde set met maatregelen dient te volgen uit de geïnventariseerde set met risico's en betrouwbaarheidseisen.
- het model dient makkelijk toepasbaar te zijn door het management zonder enige vorm van expertkennis op het gebied van informatiebeveiliging.

Op basis van bovenstaande randvoorwaarden is een model opgesteld dat grafisch is weergegeven in figuur 12. Vervolgens is dit model aan de hand van een enquête getoetst waarbij in 70% van de gevallen het model de juiste set met toegangsbeveiligingsmaatregelen voorschrijft. Bij de uitkomsten, die zijn weergegeven in tabel 9, dienen wel een aantal punten te worden opgemerkt:

- in alle gevallen waarin het model een organisatie onjuist classificeert, betreft het een te hoge classificatie in plaats van een te lagen classificatie. Het lijkt er op dat het model de neiging heeft om eerder zwaarder te beveiligen dan nodig is. Dit is vanuit informatiebeveiligings oogpunt positief, "better safe then sorry", maar vanuit bedrijfskundig oogpunt negatief, want er worden meer kosten gemaakt dan nodig is.
- bijna elke organisatie is ingedeeld in het hoge risicoprofiel en beschikt over middelmatige tot hoge classificatie van gevolgen bij schending van betrouwbaarheid. Dit lijkt op het eerste gezicht misschien vreemd, maar er dient wel te worden opgemerkt dat de geënquêteerde organisaties allemaal relaties zijn van VKA. In de regel zullen organisatie met een laag risicoprofiel en een laag afbreukrisico, in de vorm van gevolgen bij schending van betrouwbaarheid, niet zo snel hun toevlucht zoeken tot een adviesbureau voor hun vragen over informatiebeveiliging. De kans dat de geënquêteerde organisaties allemaal beschikken over een hoog afbreukrisico en zijn in te delen in een hoog risicoprofiel lijkt mij best groot.
- het aantal geënquêteerde organisaties is vrij klein. Voor een betere toetsing zou het wenselijk zijn om meer organisaties te hebben met een grotere diversiteit aan risicoprofielen en "gevolgen bij schending van betrouwbaarheid".

Vervolgens is in de zoektocht naar een nog beter presterend model gezocht naar optimale parameters aan de hand waarvan keuzes in het model worden gemaakt. Vanwege de omvang van

deze operatie is dit beperkt tot het optimaliseren van de parameters uit stap 1 en stap 3 van figuur 13. De gevonden optimale parameters zorgen ervoor dat in 78% van alle gevallen het model de juiste set met toegangsbeveiligingsmaatregelen voorschrijft. De geoptimaliseerde parameters zijn weergegeven in tabel 12, maar hier dienen een drietal opmerkingen bij te worden gemaakt:

1) bij de huidige parameters kan geen enkele organisatie worden geclassificeerd met een lage "gevolgen bij schending van betrouwbaarheid".
2) de gevonden oplossing heeft de neiging om op basis van vrij weinig organisatiekenmerken en vrij lage "gevolgen bij schending van vertrouwelijkheid, integriteit en beschikbaarheid" al te kiezen voor een hoge classificatie van gevolgen bij schending van betrouwbaarheid en voor indeling in een hoog risicoprofiel. De oorzaak hiervan is vermoedelijk tweeledig:
   - er zijn vrij weinig testgegevens om te komen tot een optimale oplossing.
   - het zoeken van een optimale oplossing blijft altijd een zoektocht naar een oplossing op basis van bekende gegevens. De zoektocht gaat zich helemaal richten op de bekende gegevens. Dit wordt ook wel "overfitting" genoemd. Het blijft natuurlijk altijd de vraag of de oplossing op nieuwe gegevens evengoed presteert. Hiervoor is het gebruikelijk dat men de beschikbare informatie in tweeën deelt. Het ene gedeelte wordt gebruikt om een optimale oplossing te vinden en het andere gedeelte wordt vervolgens gebruikt om te kijken of de gevonden oplossing ook goed presteert op gegevens die het nog niet eerder heeft gezien. De enquête die als basis dient voor het vinden van deze oplossing bevat al niet veel informatie. Indien deze informatie ook nog een keer in tweeën wordt gedeeld, blijft er waarschijnlijk niet genoeg informatie over om een goede oplossing te kunnen vinden.
3) het is maar de vraag of een door een computer gevonden optimale oplossing wenselijk is. Misschien kan men beter genoegen nemen met een iets minder presenterend model waarin de gekozen grenzen voor de gebruiker helderder zijn dan met een model waarin de grenzen berekend zijn door een computer, maar de gebruiker geen gevoel heeft bij deze gekozen grenzen. Dit punt wordt nog eens versterkt door het feit dat het voor elk model de vraag is hoe het model functioneert op toekomstige onbekende data. Voor het model met de oorspronkelijke parameters is dit getest, dit is 70%, maar voor het model met de geoptimaliseerde parameters kan dit niet getest worden omdat alle gegevens al gebruikt zijn om het model te trainen. Gegeven deze onzekerheid lijkt het mij prettig voor de gebruiker om ten minste de gekozen grenzen te begrijpen zodat deze in individuele situaties kunnen worden bijgesteld.

7.1 Aanbevelingen voor verder onderzoek

Tijdens het opstellen van het toegangsbeveiligingsmodel zijn een aantal wegen behandeld waarlangs een oplossing gezocht is voor het vraagstuk van deze scriptie. Er zijn bepaalde aannames gemaakt en bepaalde wegen bewust niet ingeslagen om zo te kunnen focussen op een afgebakend probleem. Hieronder worden een aantal aanbevelingen gedaan voor verder onderzoek:

- een nauwkeuriger onderzoek naar de organisatiekenmerken van een organisatie. Nu zijn de organisatiekenmerken afgeleid van dreigingen uit risicoanalyses. Een uitgebreider onderzoek naar kenmerken waarlangs organisaties zich op het gebied van toegangsbeveiliging onderscheiden vergroot de mogelijkheden waarmee een model een organisatie nauwkeuriger kan classificeren.
- het zoeken en gebruiken van een "slim" zoek algoritme waarmee de optimale parameters van het model gevonden kunnen worden. Vanwege de omvang van het aantal parameters is het doorrekenen van alle mogelijke combinaties niet mogelijk. Zoekalgoritmes waar men aan kan

denken zijn bijvoorbeeld: neurale netwerken, genetische algoritmes, self-organizing maps, etc. Er zijn genoeg algoritmes in omloop die op een slimme manier een optimale, of bijna optimale, oplossing vinden. Voorwaarde hierbij is wel dat er genoeg gegevens zijn om mee te testen.

- het vervangen van het model door een classificatie algoritme zoals fuzzy systems waarbij de kennis van experts wordt vertaald in een classificatie systeem.

Een algemene opmerking voor verder onderzoek bedraagt de beschikbaarheid van meer testgegevens en nauwkeurigere testgegevens. Indien de vragen uit de enquête nauwkeuriger corresponderen met de gegevens die nodig zijn om te testen kan er in ieder geval geen ruis meer gaan zitten in een vertaalslag. Daarnaast is het wenselijk dat de testgegevens bestaan uit meer organisaties en dat de aanwezige organisaties een betere afspiegeling vormen van de verschillende organisaties die men kan onderscheiden.

A Literatuurlijst

1. Alan R. Simon, “Network Re-Engineering”, 1994
2. René van den Assem, VKA
3. CSI,FBI, “Computer crime and security survey 2003”
4. Richard Koorn, KPMG Information Risk Management
5. Greg Young, Gartner, Why is security so difficult?, 2004.
6. Giarte Media Group (referentie?)
7. P. Overbeek, E. Lindgreen en M. Spruit, “Informatiebeveiliging onder controle”, 2000
8. Shon Harris, “CISSP Certification”
9. Roger Clarke, “Authentication: A Sufficiently Rich Model to Enable e-Business”
10. Mark C. Paulk e.a., “Capability Maturity Model for Software, Version 1.1”, 1993
11. Henry Mintzberg, “Mintzberg over Management, De wereld van onze organisaties”,2002
12. Handboek A&K-analyse
13. The European Security Forum, “SPRINT, Risk analyses for information systems”,1997
14. Bundesamt für Sicherheit in der Informationstechnik,”IT baseline protection manual“,Juli 2001

B Organisatiekenmerken afgeleid uit SPRINT Threats, Vulnerabilities and Controls Assessment

In deze bijlage wordt toegelicht hoe de organisatiekenmerken, die onderdeel uitmaken van het model uit hoofdstuk 5, zijn afgeleid. Namelijk niet alle kenmerken van een organisatie zijn bruikbaar voor het bepalen van toegangsbeveiligingsmaatregelen. Bruikbare organisatiekenmerken zijn die kenmerken die, al dan niet gezamenlijk met de betrouwbaarheidseisen, een keuze voor bepaalde maatregelen forceren.
In de literatuur zijn hiervoor geen standaard lijsten te vinden. Om tot een standaardlijst te komen wordt het volgende proces doorlopen:

- De lijsten met dreigingen uit de SPRINT-analyse [13] en de BSI [14] worden bekeken.
- Bij elke dreiging wordt, indien mogelijk, de organisatiekenmerken bedacht die deze dreiging veroorzaken.
- Het verband van elk organisatiekenmerk met de toegangsbveiligingsmaatregels wordt bepaald en indien er een verband is wordt het organisatiekenmerk aan de lijst met organisatiekenmerken voor het theoretisch model toegevoegd.

Uiteraard zijn er meerder risico-analyse methodieken en toegangsbeveiligingsstandaaarden die een lijst met dreigingen voorschrijven, echter er is gekozen om één gangbare risico-analyse methodiek te nemen, SPRINT, en één gangbare beveiligingsstandaard te raadplegen, BSI.

B.1 SPRINT

De lijst met dreigingen zijn in SPRINT onderverdeeld in de categorieën: vertrouwelijkheid,integriteit en beschikbaarheid. Hieronder staan de relevante dreigingen en de daarbij bedachte organisatiekenmerken per categorie genoemd.

Vertrouwelijkheid

TC.1 Outsiders gaining sight of print-outs and documents

- **Kennis gedreven organisatie**: In een door kennis gedreven organisaties heeft de informatie die verzameld wordt of de kennis die ontwikkeld wordt zeer grote waarden voor de organisatie. Met deze kennis kan de organisatie zijn voorsprong ten opzichte van andere organisatie behouden of vergroten. Er dient dus voorkomen te worden dat deze kennis in handen komt van derde.
  Opnemen in lijst: Nee. Dit kenmerk wordt namelijk indirect meegenomen via de betrouwbaarheidseisen.

- **Controlerende organisties**: Controlerende organisaties beschikken net zoals kennis gedreven organisaties over informatie die niet door derde bekeken mag worden.
  Opnemen in lijst: Nee. Dit kenmerk wordt namelijk indirect meegenomen via de

betrouwbaarheidseisen.

- **Ambulante medewerkers**: Ambulante medewerkers hebben steeds vaker de mogelijkheid om op locatie te beschikken over (gevoelige) informatie van de organisatie. Dit wordt veelal bereikt door het meebrengen van draagbare computermiddelen of door op locatie verbinding te maken met het netwerk van de organisatie. Hierdoor neemt de kans toe dat de betrouwbaarheid van de informatie wordt geschonden. De draagbare computermiddelen kunnen namelijk verloren raken of worden gestolen en de mogelijkheid om op locatie een verbinding te maken met het netwerk van de organisatie kan worden misbruikt door derden.
  Opnemen in lijst: Ja, als "Ambulante medewerkers"

- **Extern ingehuuurde partijen**: Extern ingehuurde partijen verrichten veelal hun werkzaamheden op de locatie van de organisatie. De werkzaamheden van deze partijen zouden kunnen bestaan uit service verlenende diensten, zoals catering en schoonmaakdiensten, maar ook uit diensten die meer ondersteunend zijn aan het primaire proces, zoals beheren en onderhouden van de ICT faciliteiten. Tijdens hun werkzaamheden kunnen die partijen stuiten op (gevoelige) informatie omdat er bijvoorbeeld geen “clean desk policies” in het geval van de schoonmakers of heeft men toegang tot de (gevoelige) informatie omdat men de ICT systemen moet beheren. Algemeen gezien is het belangrijk om bij elke partner, leverancier of serviceprovider na te gaan in welke mate zij toegang hebben tot gevoelige informatie. Partners, leverancier of service providers die toegang hebben tot gevoelige informatie kunnen de betrouwbaarheid van de informatie in gevaar brengen.
  Opnemen in lijst: Ja, als "Toegang van partners/service providers tot kritieke informatie systemen"

TC.2 Disclosure by employees of sensitive information to outsiders

- **Grote onpersoonlijke organisatie:** In grote onpersoonlijke organisaties is de persoonlijke betrokkenheid van werknemers vaak minder sterk aanwezig dan in kleinere persoonlijkere organisaties. Afnemende betrokkenheid bij een organisatie kan lijden tot minder secuur omgaan met de bezittingen, dus ook de informatie, van de organisatie. Daarnaast kan het in een grote onpersoonlijke organisatie mogelijk zijn dat werknemers redelijk anoniem kunnen rondlopen. Er is veelal een gebrek aan sociale controle. Het gebrek aan sociale controle zal moeten worden gecompenseerd met controle bij het uitgeven/gebruiken van authenticatie middelen of rechten aangezien het voor de uitgevende partij niet altijd duidelijk is aan wie nu precies middelen of rechten wordt verstrekt.
  Opnemen in lijst: Ja, als "Sociale controle"

- **Concurrentiegevoelige organisaties**: De marktwaarde van de informatie in concurrentie gevoelige organisaties is hoog.
  Opnemen in lijst: Nee. Dit kenmerk wordt namelijk indirect meegenomen via de betrouwbaarheidseisen.

- **Politiekgevoelige organisaties**: Het vrijgeven of vrijkomen van bepaalde informatie kan politieke consequenties hebben.

Opnemen in lijst: Nee. Dit kenmerk wordt namelijk indirect meegenomen via de betrouwbaarheidseisen.

TC.3 Unauthorised entry into premises

- **Organisaties waar veel klanten komen:** Doordat veel klanten bij een organisatie over de vloer komen is het moeilijk te zien wie wel en wie niet zich in een bepaald gedeelte van het gebouw mag bevinden. Dit kenmerk breder genomen, bepaalt de soort huisvesting waar een bedrijf in zit, de markt waarin de organisatie opereert en de doelgroep die de organisatie bedient wat voor soort publiek bij een bedrijf over de vloer kan komen. Organisaties waarbij klanten het bedrijf bezoeken dienen bij de toegang die verleend wordt tot de IT-faciliteiten rekening te houden met een "publiek" gedeelte en een "bedrijfsmatig"gedeelte.
  Opnemen in lijst: Nee. De bovengenoemde kenmerken zijn zeker relevant voor informatiebeveiliging, maar niet voor toegangsbeveiliging in het bijzonder.

TC.5 Unauthorised acces to data by external employees

- **Gebruik van Inbel-faciliteiten**: Dit bedrijfskenmerk zit al verwerkt in het bedrijfskenmerk ":ambulante medewerkers".
  Opnemen in lijst: Nee.

- **Gebruik van Internet door medewerkers**: Door gebruik van Internet vanuit het bedrijf worden computersystemen blootgesteld aan virussen en trojans. In situaties waarbij medewerkers toegang hebben het Internet dienen de rechten strak geregeld te zijn en goed gecontroleerd te worden.
  Opnemen in lijst, Ja, als " Gebruik van Internet door de medewerkers".

TC.7 Interception of communication links

- **Geografische spreiding van de organisatie**: Doordat een organisatie geografisch verspreid is, dient de digitale communicatie plaats te vinden over eventueel aanwezige netwerken tussen de diverse locaties. Dit kan zowel publieke als private netwerken betreffen. In het geval van publieke netwerken heeft deze invloed op de toegangsbeveiliging omdat ook derde een poging kunnen ondernemen om via deze publieke netwerken toegang te krijgen tot de informatie of informatievoorzieningen. Daarnaast speelt bij geografische spreiding de organisatie structuur een rol. Zijn de afzonderlijke locaties, divisies, vrij autonoom of wordt alles centraal aangestuurd. De organisatiestructuur heeft invloed op de beheersbaarheid van de identiteiten van medewerkers.
  Opnemen in lijst: Ja, als "Geografische spreiding", "Organisatie vorm (structuur)".

- **Integratie van systemen met die van partners**: Door de integratie van de systemen met die van partners vindt communicatie plaats via kanalen die misschien wel te onderscheppen zijn. Hierbij is dus het kritieke punt dat er communicatie plaats vindt over een onbeveiligd netwerk.
  Opnemen in lijst: Ja, als "Communicatie over onbeveiligde netwerken".

- **Remote management**: Voor remote management wordt er toegang verleent aan een partner om, veelal over onbeveiligde netwerken of via inbelverbindingen, de informatiesystemen te beheren.
  Opnemen in lijst: Ja, als "Communicatie over onbeveiligde netwerken" en "Toegang van partners/service providers tot kritieke informatie systemen".

Integriteit

TI.1 Input errors

- **Lage opleiding van de medewerkers**: De opleiding van medewerkers dient te zijn aangepast aan de complexiteit van de handelingen die deze medewerker moet verrichten. Indien de opleiding in verhouding te laag is kan dit tot gevolg hebben dat er fouten gemaakt worden die niet gemaakt mogen worden.
  Opnemen in lijst: Nee. Aangezien het niveau van het werk meestal wel is afgestemd op het niveau van de opleiding

- **Intensieve informatieverwerkend organisatie**: In een organisatie waar veel gegevens worden verwerkt worden meer fouten gemaakt.
  Opnemen in lijst: Nee. Dit probleem is niet met behulp van toegangsbeveiliging op te lossen.

Beschikbaarheid

TA.4 Day-to-day system outages

- **Veel Legacy systemen**: Legacy systemen worden vaak niet meer ondersteund door de leverancier. Hebben vaak een eigen beheersstructuur die moeilijk te integreren is met een overkoepelende beheersstructuur. Legacy systemen bemoeilijken het uitvoeren van identiteit management. Daarnaast worden op legacy systemen de toegangsrechten vaak te ruim gezet om zo communicatie met andere legacy systemen mogelijk te maken.
  Opnemen in lijst: Ja, als "Legacy systemen".

TA.5 Degraded system performance

- **Periodearbeid**: Periodearbeid kan voor piekbelasting zorgen bij het gebruik van de informatievoorziening. De performance van de informatievoorziening kan hierdoor afnemen of de informatievoorziening kan zelfs geheel ontoegankelijk worden. Periodearbeid kan dus de gestelde beschikbaarheidseisen in gevaar brengen. Door de toegang tot kritieke informatie en informatiesystemen te beperken tot een selecte groep gebruikers, blijft de informatie en de informatievoorziening beter beschikbaar.
  Opnemen in lijst: Nee. Dit probleem wordt al indirect meegenomen in de betrouwbaarheidseisen.

B.2 BSI (Bundesamt fur sicherheit in der Informationstechnik)

De lijst met dreigingen zijn in BSI onderverdeeld in de categorieën: forjce majeure, organisational shortcomings, human failure, technical failure en deliberate acts. Hieronder staan de relevante dreigingen en de daarbij bedachte organisatiekenmerken per categorie genoemd. Sommige organisatiekenmerken zijn al reeds onderkend in §B.1, bij het analyseren van de dreigingen in SPRINT. Voor een toelichting op deze organisatiekenmerken wordt dan ook verwezen naar §B.1.

Force Majeure

T 1.1 Loss of personnel

- **Arbeidsintensieve organisatie**: In een arbeidsintensieve organisatie wordt relatief veel personeel ingezet en is de kans op uitval van personeel groter.
  Opnemen in lijst: Nee. Nonsense argument.

- **Grote van organisatie (aantal medewerkers)**: In grote organisaties met veel medewerkers is de beheersoverhead voor het voeren van identiteit management en het verstrekken van autorisatie groter. Sterke identiteit management en gebruik van rollen kunnen deze overhead reduceren.
  Opnemen in lijst: Ja, als "aantal medewerkers"

- **Doorstroom van medewerkers**: Veel medewerkers verlaten na een korte periode het bedrijf en worden vervangen door nieuwe medewerkers of medewerkers stromen door intern binnen het bedrijf en blijven dus niet lang op dezelfde functie zitten. Door deze grote instroom, uitstroom of doorstroom nemen de beheerswerkzaamheden voor het beheren van identiteiten, het uitgeven van authenticatie middelen en het verstrekken van autorisatie toe. Deze toename in beheerswerkzaamheden kan met behulp van sterk identiteit management en gebruik van rollen worden teruggedrongen.
  Opnemen in lijst: Ja, als "Instroom/ Doorstroom van medewerkers"

T 1.2 Failure of the IT system

- **Afhankelijkheid van de IT**: Bedrijven met een zware afhankelijkheid van de IT zijn gevoeliger voor het falen van IT systemen. Dit kenmerk wordt meegenomen in de betrouwbaarheidseisen.
  Opnemen in lijst: Nee. Dit kenmerk wordt al indirect meegenomen via de betrouwbaarheidseisen.

- **Professional Programs vs. maatwerk software vs. in-house development:** Professional Programs worden aan meerdere bedrijven verkocht en dus door een grotere groep mensen gebruikt. De kans dat fouten aan het licht komen is groter (meer mensen kunnen tegen fouten aan lopen) en dat kan met adequaat handelen van de leverancier weer een veiliger product opleveren. Bij in-house development wordt het pakket vaak alleen binnen de eigen organisatie

gebruikt.
Opnemen in lijst: Nee. Dit probleem is niet op te lossen met toegangsbeveiliging

- **Onderlinge afhankelijkheden tussen de systemen**:
  Opnemen in lijst: Nee. Dit probleem is niet op te lossen met toegangsbeveiliging.

T 1.10 Failure of a wide area network

- **Geografische spreiding**: zie §B.1

- **Connectiviteit met partners** / **leveranciers**: Al behandeld in §B.1 bij het kenmerk " Integratie van systemen met die van partners".

- **Connectiviteit met klanten**: Klanten krijgen soms toegang tot een beperkte set van de informatievoorziening en zij worden vaak in de gelegenheid gesteld om met het bedrijf te communiceren. Hiervoor worden bepaalde gedeeltes van de informatievoorziening opengezet, echter de kans is aanwezig dat te veel informatie beschikbaar komt. Dit probleem is een subset van het probleem "Connectiviteit met partners /everanciers".

- **Gebruik van internet applicaties door medewerkers**: zie §B.1.

T 1.12 Problems caused by big public events

- **Consument gericht bedrijf**: Bedrijven die als doelgroep consumenten hebben, zijn zichtbaarder voor het grote publiek en zullen als één van de eerste worden aangepakt voor sabotageachtige activiteiten. Daarnaast beschikken deze bedrijven over informatievoorzieningen die veelal voor een breed publiek beschikbaar moet zijn.
  Opnemen in lijst: Ja, als "Doelgroep".

- **Bedrijfstak onder vuur van actiegroeperingen**: Bedrijven waarbij de activiteiten liggen op een vlak die door bepaalde groepen in de maatschappij worden afgekeurd, zijn extra gevoelig voor sabotage van deze groepen. Toegangsbeveiliging van gevoelige informatie moet voor dit soort bedrijven dus op een hoog niveau zitten.
  Opnemen in lijst: Ja, als "Omstreden activiteiten"

Organisational Shortcomings

T 2.1 Lack of, or insufficient, rules

- **Decentrale georganiseerde organisatie**: In een decentraal georganiseerde organisatie worden regels niet van bovenaf opgelegd. Elk onderdeel is vrij om op een bepaalde manier met security om te gaan. Dit in tegenstelling tot het feit dat de onafhankelijke onderdelen wel met elkaar te maken hebben (zwakste schakel).

Opnemen in lijst: Ja, als "Organisatie vorm (structuur)"

- **Niet gebonden door wet en regelgeving**: Organisaties die niet gebonden zijn aan Wet & Regelgeving op het gebied van security hoeven hier dus ook minder aandacht aan te besteden of besteden hier ten onrechte minder aandacht aan.
  Opnemen in lijst: Ja, als "Wet & Regelgeving"

T 2.13 Inadequately protected distributors

- **Beveiligingsniveau van partners/leveranciers**: Partners en leveranciers kunnen toegang hebben tot de systemen. Slecht beveiliging aan de kant van partners en leveranciers is een gevaar voor de organisatie. Echter hier is met toegangsbeveiligingsmaatregelen vanuit de eigen organisatie weinig aan te doen.
  Opnemen in lijst: Nee. Hier is met toegangsbeveiliging binnen de eigen organisatie niks aan te doen.

T 2.16 Non-regulated change of users in the case of laptop PC's

- **Mobiltiteit medewerkers**: Zie §B.1: Ambulante medewerkers.

T 2.22 Lack of evaluation of auditing data

- **Externe controlling/accounting eisen**: Bedrijven met hogere controlle eisen voor bijvoorbeeld de jaarrekening hebben zwaardere eisen aan de beveiliging.
  Zie §B.2: Niet gebonden door wet en regelgeving

T 2.23 Security flaws involved in integrating DOS PC's into a server-based network

- **Diversiteit in verschillende systemen**: Indien veel verschillende systemen met elkaar moeten samenwerken, moeten vaak veel aanpassingen worden verricht zodat al die verschillende systemen met elkaar kunnen communiceren. Dit beinvloedt de beveiliging negatief. Echter dit is niet te beheersen met het toegangsbeveiligingsmodel.
  Opnemen in lijst: Nee.

Human Failure

T 3.1 Loss of data confidentiality/integrity as a result of IT user error

- **Opleiding van werknemers**: Zie §B.1: Lage opleiding van de medewerkers

T 3.6 Hazards posed bij cleaning staff or outside staff

- **Extern ingehuurde partijen**: zie §B.1

Technical Failure

T 4.1 Disruption of power supply

- **Afhankelijkheid van service providers**: Zodra veel services worden uitbesteed/afgenomen van externe partijen, wordt men daarvan ook afhankelijk.
  Opnemen in lijst: Nee. Dit probleem zit al indirect verwerkt in de betrouwbaarheidseisen.

Deliberate Acts

Zie §B.1, threat T 1.12

C Enquête

C.1 Algemeen

De enquête bestaat uit 4 gedeeltes. Deel I bevat vragen over de organisatie, de omgeving waarin de organisatie opereert en de ICT infrastructuur van de organisatie. Deel II bevat vragen over de betrouwbaarheidseisen die een organisatie stelt aan het primaire proces. Deel III bevat vragen over de logische toegangsbeveiliging van de organisatie. Deel IV bevat ten slotte vragen om de context van de enquête en eventuele toekomstige enquêtes beter te kunnen plaatsen.

Met behulp van de antwoorden uit deel I t/m IV wordt een model over logische toegangsbeveiliging gevalideerd. Het model leidt het gewenste niveau van logische toegangsbeveiliging af uit de betrouwbaarheidseisen die gesteld worden aan het primaire proces, uit de bedrijfskenmerken en uit algemene ICT-kenmerken van een organisatie(onderdeel).

Voor het invullen van de enquête neemt u een primair proces van uw organisatie of een primair proces van een organisatieonderdeel als uitgangspunt. Wij verzoeken u elke vraag te beantwoorden in de context van dit primaire proces en in de context van het desbetreffende organisatie(onderdeel). Indien u besluit om de enquête in te vullen voor een primair proces van een organisatieonderdeel dient u overal waar gesproken wordt over *organisatie* dit te vervangen door *organisatieonderdeel*.

Bij het beantwoorden van de vragen kan het voorkomen dat het ene antwoord volgens u geldt voor het ene gedeelte van de *organisatie* en een andere antwoord juist weer geldt voor een ander gedeelte van de *organisatie*. In dat geval vragen wij u voor het antwoord te kiezen dat als ondergrens geldt voor uw gehele *organisatie*.

Omcirkel bij elke vraag het juiste antwoord.

Vraag 1: aan wie rapporteert u?

a) Aandeelhouders
b) Raad van Bestuur
c) Hoger management
d) Midden management
e) Overige, nl:……

C.2 Deel I: bedrijfskenmerken en algemene ICT-kenmerken

Organisatie gerelateerde vragen

Vraag 2: hoeveel medewerkers zijn werkzaam in uw *organisatie*?

a) < 500
b) 500 – 5.000
c) > 5.000

Vraag 3: hoe groot is in uw *organisatie* het personeelsverloop (instroom + uitstroom) per jaar ten opzichte van het totaal aantal medewerkers?

a) < 10%
b) 10% – 20%
c) > 20%.

Vraag 4: hoe groot is in uw *organisatie* het functieverloop (het percentage medewerkers dat van functie verandert binnen de *organisatie*) per jaar?

a) < 10%
b) 10% – 20%
c) > 20%.

Vraag 5: wat voor voorzieningen zijn er in de standaard kantoorlocaties van uw *organisatie* getroffen om onbevoegde personen buiten de deur te houden?

a) Standaard voorzieningen voor beveiligen van een pand, zoals: alarminstallaties en sloten op de deuren.
b) Er wordt toegang verleend door middel van gepersonaliseerde authenticatiemiddelen zoals: keycards, biometrische scans, etc.
c) Er wordt toegang verleend door beveiligingspersoneel.

Vraag 6: welke van de onderstaande procedures benadert het beste de procedure die binnen uw *organisatie* geld voor het verlenen van toegang aan bezoekers tot het pand?

a) Bezoekers kunnen direct doorlopen naar de medewerker met wie zij een afspraak hebben.
b) Bezoekers dienen zich te melden bij de receptie, waar ze eventueel een badge krijgen en vervolgens door kunnen lopen naar degene met wie zijn een afspraak hebben.
c) Bezoekers dienen zich te melden bij de receptie, waarna de medewerker de bezoeker bij de receptie ophaalt en weer terugbrengt.

Vraag 7: is het in uw *organisatie* de gewoonte om mensen die u niet bekend voorkomen hierop aan te spreken?

a) Ja, iedereen die mij onbekend voorkomt.
b) Alleen mensen met een bezoekersbadge die onbegeleid rondlopen.
c) Nee, helemaal niet.

Vraag 8: beschikt uw *organisatie* over meerdere vestigingen?

a) Nee (ga verder met vraag 10).
b) Ja, een centraal hoofdkantoor met meerdere decentrale kantoren.
c) Ja, geen centraal hoofdkantoor, maar wel meerdere decentrale kantoren.

Vraag 9: in welke mate wordt er *organisatie*breed beleid centraal opgesteld en opgelegd aan de verschillende vestigingen?

a) Beleid wordt volledig centraal opgesteld en opgelegd aan de vestigingen. Er is geen ruimte voor eigen invulling door de vestigingen.
b) Beleid wordt in grote lijnen centraal opgesteld, maar de concrete invulling gebeurt door de vestigingen zelf.
c) Beleid wordt in grote mate opgesteld door de individuele vestigingen.

Sector gerelateerde vragen

Vraag 10: in welke sector bevinden zich de kernactiviteiten van uw *organisatie*?

a) Overheid.
b) Nuts.
c) Zorg.
d) Industrie.
e) Bouw.
f) Handel.
g) ICT.
h) Vervoer & Logistiek.
i) Financiële instelling.
j) Onderwijs.
k) Semi-overheid.
l) Overige, nl:……..

Vraag 11: voert uw *organisatie* activiteiten uit die maatschappelijk gevoelig liggen? Denk hierbij aan activiteiten die door bepaalde actiegroeperingen in de gaten worden gehouden. Voorbeelden hiervan zijn extra milieu gevoelige activiteiten en zichtbare dominantie van een markt.

a) In zeer sterke mate.
b) In geringe mate.
c) In z'n geheel niet.

Vraag 12: wie is de belangrijkste afnemer van de producten of diensten van uw *organisatie*?

a) Consument.
b) Overheid.
c) Bedrijfsleven.
d) Overige, nl:…….

Vraag 13: hoe groot is in uw branche de invloed van een eventuele branche specifieke toezichthouder op het vereiste niveau van informatiebeveiliging?

a) Groot.
b) Middel.
c) Klein.

ICT gerelateerde vragen

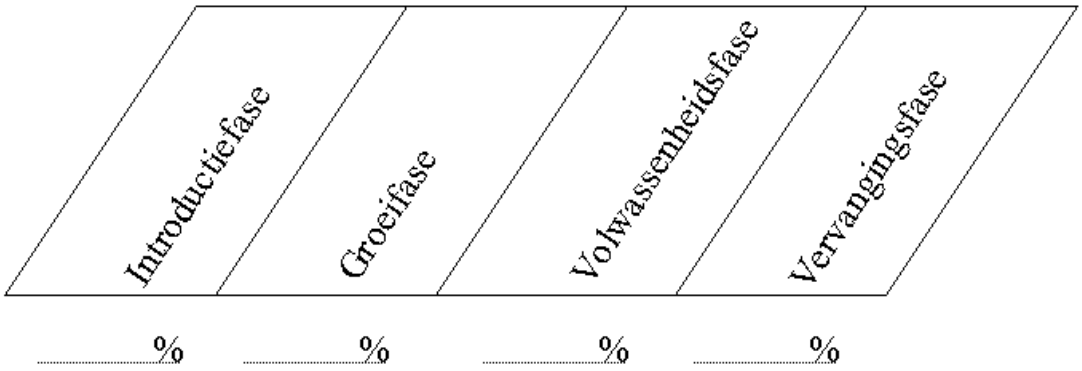
Vraag 14: kunt u in de onderstaande tabel aankruisen welke gebruikers toegang hebben tot bepaalde gegevens vanaf een bepaalde locatie?

	Gegevens / toepassingen					
Gebruikers	Toegang tot Intranet (portals)	Toegang tot e-mail/agenda	Toegang tot relatiebeheersystemen (CRM)	Toegang tot productiesystemen (ERP)	Toegang tot bestanden (fileservers)	Toegang tot interne specifieke bedrijfsapplicaties systemen
Medewerkers binnen het bedrijfspand						
Medewerkers buiten het bedrijfspand						
Partners / service providers binnen het bedrijfspand						
Partners / service providers buiten het bedrijfspand						
Klanten						

Vraag 15: Bedrijfsapplicaties die de informatievoorziening ondersteunen kunnen zich bevinden in diverse fases van een levenscyclus:

Introductiefase: In deze fase wordt de applicatie voor het eerst geïntroduceerd in de productieomgeving.
Groeifase: In deze fase wordt de applicatie al geruime tijd in een productieomgeving gebruikt, maar bevat de applicatie nog diverse kinderziektes die in deze fase verholpen worden.
Volwassenheidsfase: In deze fase bevinden er zich geen kinderziektes meer in de applicatie en worden alleen nog functionele wijzigingen van de applicatie doorgevoerd.
Vervangingsfase: In deze fase worden er geen functionele wijzigingen meer de applicatie doorgevoerd en is de ontwikkeling aan de applicatie gestaakt.

Kunt u in de onderstaande figuur aangeven welk percentage van uw bedrijfsapplicaties zich in de diverse levensfases bevindt? Hierbij telt een applicatie die meerdere keren binnen uw *organisatie* gebruikt wordt ook meerdere keren mee.



Vraag 16: hebben medewerkers op hun werkplek toegang tot internet?

a) Vrijwel alle medewerkers hebben volledige toegang.
b) Vrijwel alle medewerkers hebben alleen toegang tot specifieke voorzieningen.
c) Vrijwel alle medewerkers hebben geen toegang.

C.3 Deel II: betrouwbaarheidseisen

In dit gedeelte van de enquête wordt u gevraagd aan te geven welke eisen u stelt aan de betrouwbaarheid van de informatie en informatievoorziening voor uw primaire proces. Voor dit doel is betrouwbaarheid onderverdeeld in 3 gebieden, te weten: vertrouwelijkheid, integriteit en beschikbaarheid. Allereerst dient u aan te geven welk primaire proces als uitgangspunt dient voor de enquête.

Vraag 17: omschrijf het primaire proces dat als uitgangspunt dient voor het invullen van deze enquête?

……

……

……

……

Vraag 18: wat zijn de mogelijke gevolgen voor uw primaire proces indien de vertrouwelijkheid van de informatie, die onderdeel is van het primaire proces, en informatievoorziening worden gecompromitteerd?

a) Het voortbestaan van de *organisatie* wordt ernstig in gevaar gebracht.
b) Er wordt grote schade toegebracht aan het bereiken van de bedrijfsdoelstellingen. Financiële gevolgen en gevolgen voor het imago zijn groot.
c) Er wordt beperkte schade toegebracht aan het bereiken van de bedrijfsdoelstellingen. Financiële gevolgen of gevolgen voor het imago zijn beperkt.

Vraag 19: wat zijn de mogelijke gevolgen voor uw primaire proces indien de integriteit van de informatie, die onderdeel is van het primaire proces, wordt aangetast?

a) Het voortbestaan van de *organisatie* wordt ernstig in gevaar gebracht.
b) Er wordt grote schade toegebracht aan het bereiken van de bedrijfsdoelstellingen. Financiële gevolgen en gevolgen voor het imago zijn groot.
c) Er wordt beperkte schade toegebracht aan het bereiken van de bedrijfsdoelstellingen. Financiële gevolgen of gevolgen voor het imago zijn beperkt.

Vraag 20: hoe lang moet informatie, die onderdeel is van het primaire proces, en de informatievoorziening, ondersteunend aan het primaire proces, onbeschikbaar zijn voordat: er grote schade toegebracht wordt aan het bereiken van de bedrijfsdoelstellingen, er grote financiële schade optreedt of het imago grote schade oploopt?

a) Eén uur.
b) Eén dag.
c) Eén week.
d) Eén maand.

Vraag 21: Welke bijzondere omstandigheden zijn naar uw mening van invloed op de door u gemaakte keuzes bij vraag 18, 19, 20?

……

……

……

……

……

……

C.4 Deel III: gewenste beveiligingsniveau

In dit gedeelte van de enquête wordt u gevraagd aan te geven wat uw mening is met betrekking tot een aantal toegangsbeveilingsproblemen. Hierbij kunt u gebruik maken van de door u ingevulde antwoorden uit deel I en II van de enquête. Het is van belang dat u de onderstaande vragen invult in de context van het gekozen primaire proces en in de context van het gekozen organisatie(onderdeel).
De keuzemogelijkheden bij de onderstaande vragen zullen mogelijk niet altijd even goed overeenkomen met **uw** mening. In dat geval vragen wij u te kiezen voor het antwoord dat het dichtst bij **uw** norm in de buurt komt.

Vraag 22: welke informatie zou een nieuwe medewerker bij zijn indiensttreding ten minste moeten overleggen voor het vaststellen van zijn identiteit en welke controle zou hierop minimaal plaats moeten vinden?

a) Kopie van het paspoort voor HRM (wettelijk verplicht).

b) Paspoort met controle van het paspoort door de HRM-medewerker.
c) Paspoort met controle van paspoort, en screening via een externe instantie.

Vraag 23: welke informatie zou een zakelijke partner ten minste moeten aanleveren en welke controle zou er minimaal moeten plaats vinden op deze informatie alvorens de medewerkers van een partner toegang tot de informatievoorziening krijgen?

a) Zelf aangedragen informatie.
b) Uittreksel Kamer van Koophandel en controle van deze bij de KvK.
c) Uittreksel Kamer van Koophandel en persoonlijke identificatie van de desbetreffende medewerker.

Vraag 24: welke informatie zou een klant ten minste moeten aanleveren en welke controle zou er minimaal op deze informatie moeten plaatsvinden alvorens de klant toegang tot de informatievoorziening wordt verleend?

a) Zelf aangedragen informatie.
b) Financiële gegevens, zoals bijvoorbeeld creditcard- of bankrekeninggegevens, en controle van deze gegevens bij een financiële instelling.
c) Persoonlijke identificatie of afgeleide identificatie via, bijvoorbeeld PKI, en controle van deze informatie bij een Trusted Third Party (TTP).

Vraag 25: Waarvan zal voor het verstrekken van logische toegang tot de informatievoorziening ten minste gebruik moeten worden gemaakt?

a) Een functionele id waarbij handelingen niet worden gelogd of tot een persoon herleidbaar zijn.
b) Een uniek user-id waarbij bepaalde handelingen worden gelogd.
c) Een uniek user-id waarbij alle handelingen worden gelogd.

Vraag 26: Hoe zou het beheer van login-accounts plaats moeten vinden?

a) Decentraal per applicatie, dus voor elke applicatie apart op verschillende fysieke locaties.
b) Centraal per applicatie, dus voor elke applicatie apart vanaf dezelfde fysieke locatie.
c) Centraal voor de geïntegreerde informatievoorziening, dus tegelijk voor alle applicaties.

Vraag 27: hoe dient in uw *organisatie* een gebruiker te worden geregistreerd die zowel klant als medewerker van uw organisatie is?

a) Onder 2 aparte identiteiten: 1 voor de rol als klant en 1 voor de rol als medewerker.
b) Onder 2 aparte identiteiten: 1 voor de rol als klant en 1 voor de rol als medewerker waarbij er een koppeling is tussen deze 2 identiteiten.
c) Onder 1 identiteit, die zowel geld voor de rol als klant als voor de rol als medewerker.

Vraag 28: zou een medewerker binnen uw *organisatie* moeten beschikken over een loginnaam die toegang geeft tot alle systemen waarvoor hij is geautoriseerd (Single Sign On)?

a) Ja.
b) Nee.

Vraag 29: welke vorm van authenticatie zou binnen uw *organisatie* moeten worden gebruikt?

a) 1 factor, bijvoorbeeld: wachtwoord of PIN.
b) Sterke 1 factor, bijvoorbeeld: wachtwoord dat aan speciale eisen moet voldoen.
c) 2 factor, bijvoorbeeld: wachtwoord en token.

Vraag 30: welke vorm van controle tijdens de uitgifte van een authenticatiemiddel zou moeten worden toegepast?

a) Geen.
b) De ontvanger van het authenticatiemiddel zou moeten tekenen voor ontvangst.
c) De ontvanger van het authenticatiemiddel zou met een identiteitsbewijs moeten aantonen dat hij/zij de juiste persoon is.

Vraag 31: hoe zou moeten worden omgegaan met incidenten omtrent authenticatie middelen, zoals het verlies van tokens en pasjes, het vergeten van wachtwoorden?

a) Geen specifieke aandacht aan besteden.
b) Periodiek de incidenten afhandelen, bijvoorbeeld aan het einde van iedere week.
c) Afhandeling van incidenten integreren in een continu-proces.

Vraag 32: welke mate van fijnmazigheid van toegang tot de informatievoorziening is binnen uw *organisatie* nodig voor het onderverdelen van functies in rollen en het onderverdelen van toegang tot bepaalde informatie?

a) Indeling volgens alles of niets principe, iemand heeft dus toegang tot de volledige informatievoorziening of tot niets.
b) Indeling op applicatieniveau, per applicatie wordt al dan niet toegang verstrekt.
c) Indeling binnen applicaties, iemand krijgt al dan niet toegang tot specifieke delen van een applicatie.

Vraag 33: zou er bij het toekennen van rechten sprake moeten zijn van controle of functiescheiding?

a) 1 persoon kent de rechten toe en voert deze in, hierop vindt geen controle plaats.
b) 1 persoon kent de rechten toe en voert deze in, hierop vindt controle plaats.
c) Het toekennen van rechten en het invoeren hiervan wordt verdeeld over 2 personen.
d) Het toekennen van rechten en het invoeren hiervan wordt verdeeld over 2 personen en hierop vindt controle plaats.

Vraag 34: zou er controle moeten plaatsvinden op de rechten die gebruikers in het bezit hebben?

a) Nee.
b) Ja, periodiek.
c) Ja, continu-procesmatig.

Deel IV: context vragen

In dit gedeelte van de enquête stellen wij u een aantal vragen met als doel de context waarbinnen het onderzoek plaats vindt scherp te definiëren. Daarnaast willen wij als VKA bij het uitvoeren van onderzoek in de toekomst die onderwerpen oppakken waarmee wij u het beste van dienst kunnen zijn.

Vraag 35: beveiligingsontwikkelingen die in uw *organisatie* spelen

In de onderstaande vragenlijst wordt de volgende score gebruikt:

1. Niet van belang.
2. Enigszins van belang.
3. Van (groot) belang op langere termijn.
4. Thans van groot belang.

Vraag	1	2	3	4
Wat is het belang van de volgende ontwikkelingen voor uw *organisatie*?				
• Beveiligingsbewustzijn van medewerkers				
• Veilige toegang tot uw systemen door thuiswerkers				
• Veilige toegang tot uw systemen door leveranciers				
• Veilige toegang tot uw systeem door klanten				
• Veilige toegang tot uw systeem door partners				
• Beveiliging Internetsite en de diensten die daarop worden aangeboden				
• Privacybescherming van persoonsgegevens				
• Uitbesteden van informatiebeveiliging (Managed Security Services)				
• Gebruik van de elektronische handtekening				
• Identity Management				
• Business Continuity Management				
• Computer Security Incident Response				
• Applicatie beveiliging				
• Beveiliging van draadloze netwerken				
• Beveiliging van mobiele toepassingen				
• Overig, nl: …….. …….. …….. …….. ……..				

Vraag 36: hoe verhoudt het budget voor informatiebeveiliging van 2003 zich ten opzichte van 2002?

a) Het budget is in 2003 toegenomen ten opzichte van 2002.
b) Het budget is in 2003 gelijk gebleven ten opzichte van 2002.
c) Het budget is in 2003 afgenomen ten opzichte van 2002.
d) Onbekend.

Vraag 37: hoeveel beveiligingsincidenten, die schade hebben veroorzaakt, hebben er in uw *organisatie* het afgelopen jaar plaatsgevonden?

a) Geen
b) 1 – 5
c) 6 – 10
d) 11 – 30
e) 31 – 60
f) > 60
g) Onbekend.

Vraag 38: welk deel van de ondervonden incidenten heeft een interne oorzaak: fouten van interne medewerkers, uitval van systemen, etc?

a) < 25%
b) 25% – 49%
c) 50% – 75%
d) > 75%.

Vraag 39: kunt u een indicatie geven van de omvang van de totale financiële schade door de onder vraag 37 genoemde beveiligingsincidenten?

a) < € 10.000
b) € 10.001 – € 100.000
c) € 100.001 – € 500.000
d) € 500.001 – € 1.000.000
e) > € 1.000.000
f) Onbekend.

Vraag 40: welk percentage van de, onder vraag 37, ondervonden beveiligingsincidenten is het gevolg van onvoldoende logische toegangsbeveiliging?

a) < 25%
b) 25% – 49%
c) 50% – 75%
d) > 75%.

D Verband tussen model en enquête

D.1 Gevolgen bij schending van de betrouwbaarheid

Gevolgen bij schending van de vertrouwelijkheid
De gevolgen bij schending van de vertrouwelijkheid uit het model correspondeert met vraag 18 uit de enquête. Hierbij correspondeert de schaal laag/middel/hoog met antwoord c/b/a.

Gevolgen bij schending van de integriteit
De gevolgen bij schending van de beschikbaarheid uit het model correspondeert met vraag 19 uit de enquête. Hierbij correspondeert de schaal laag/middel/hoog met antwoord c/b/a.

Gevolgen bij schending van de beschikbaarheid
De gevolgen bij schending van de beschikbaarheid uit het model correspondeert met vraag 20 uit de enquête. Hierbij correspondeert de schaal laag/middel/hoog met antwoord d/c/b-a.

D.2 Organisatiekenmerken

Ambulante medewerkers
Dit kenmerk correspondeert met vraag 14 van de enquête. Indien bij vraag 14 is aangegeven dat er toepassingen beschikbaar zijn voor medewerkers buiten het bedrijfspand, is dit kenmerk van toepassing.

Communicatie over onbeveiligde netwerken
Dit kenmerk correspondeert met vraag 14 van de enquête. Indien bij vraag 14 medewerkers of partners / service-providers, die zich buiten het bedrijfspand bevinden toegang hebben tot toepassingen is dit kenmerk van toepassing.

Geografische spreiding
Dit kenmerk is van toepassing indien vraag 8 van de enquête met keuze b of c is beantwoord.

Toegang van partners/service providers tot kritieke informatie/informatiesystemen
Dit kenmerk correspondeert met vraag 14 van de enquête. Indien bij vraag 14 partners en service / providers toegang hebben tot bedrijfskritische applicaties (ERP,CRM, fileservers, interne specifieke applicaties) is dit kenmerk van toepassing.

Gebruik van Internet door de medewerkers
Dit kenmerk is van toepassing indien vraag 16 van de enquête met keuze a of b is beantwoord.

Legacy systemen
Dit kenmerk is van toepassing indien bij vraag 15 is aangegeven dat tenminste 25% van de informatiesystemen in de vervangingsfase zit.

Aantal medewerkers (grote van organisatie)

Dit kenmerk is van toepassing indien vraag 2 met b of c is beantwoord.

Instroom / Doorstroom van medewerkers

Dit kenmerk is van toepassing indien vraag 3 met b of c is beantwoord en/of wanneer vraag 4 met c is beantwoord.

Organisatievorm (structuur)

Dit kenmerk is van toepassing indien vraag 9 met b of c is beantwoord.

Sociale controle

Dit kenmerk is van toepassing indien vraag 7 met c is beantwoord.

Doelgroep

Dit kenmerk is van toepassing indien vraag 12 met a is beantwoord.

Omstreden activiteiten

Dit kenmerk is van toepassing indien vraag 11 met a is beantwoord.

Wet & Regelgeving

Dit kenmerk is van toepassing indien vraag 13 met a is beantwoord.

D.3 Toegangsbeveiligingsmaatregelen

De toegangsbeveiligingsmaatregelen met de corresponderende vragen uit de enquête zijn weergegeven in tabel 13.

Toegangsbeveiligingsmaatregel	Corresponderen vraag uit de enquête
Identiteit Management	
Informatie & Controle	22,23,24
Traceerbaarheid	25
Beheersbaarheid	26,27,28
Authenticate Management	
Sterke authenticatie	29
Controle uitgifte proces	30
Incident management	31
Autorisatie Management	
Granulariteit	32
Toekenningsproces	33
Controle gebruik	34

Tabel 13: Toegangsbeveiligingsmaatregelen met corresponderen vragen.

Bij alle maatregelen correspondeert een invulling van licht/middelmatig/zwaar met de antwoorden a/b/c uit de enquête. Bij de maatregelen 'Informatie & Controle' en 'Beheersbaarheid' horen drie corresponderende vragen uit de enquête. Hierdoor is niet direct een één op één koppeling te maken tussen de maatregelen en de antwoorden uit de enquête. Om toch de koppeling te kunnen maken is het volgende verband gelegd:

- De invulling van de maatregel is zwaar indien ten minste twee van de drie vragen uit de enquête met c zijn beantwoord.
- De invulling van de maatregel is middelmatig indien de invulling van de maatregel niet zwaar is en indien tenminste twee van de drie vragen uit de enquête met b of c zijn beantwoord.
- De invulling van de maatregel is licht indien de invulling niet middelmatig of zwaar is.