IT beveiligingsbeleid aangepast aan nieuwe evoluties van IT

Beveiliging van mobile computing in de onderneming

Tom Princen

promotor :
Prof. Jeanne SCHREURS

Masterproef voorgedragen tot het bekomen van de graad van master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica, afstudeerrichting informatie- en communicatietechnologie

universiteit hasselt

Woord vooraf

Deze eindverhandeling vormt het sluitstuk in mijn opleiding Master in Handelsingenieur in de Beleidsinformatica aan de Universiteit Hasselt.

Graag wil ik verschillende personen danken die bijgedragen hebben tot de realisatie van deze eindverhandeling. Een speciaal dankwoord gaat naar mijn promotor Professor Jeanne Schreurs voor haar deskundige begeleiding en advies.

Tot slot een bijzonder woord van dank aan mijn familie, vrienden voor hun steun doorheen mijn studies.

Samenvatting

Toen IBM zijn eerste computer introduceerde in 1981 betekende 'computer security' niets meer dan het afsluiten van het bureau waar de computer zich bevond zodat niemand hem kon meenemen. (Rubenking, Computing Moves Into the Cloud, 2008) Maar in 1984 werd door onderzoeker Fred Cohen een volledig nieuwe term geïntroduceerd: 'computer virus'. (Cohen, 1984) Hij ontwikkelde een software die ervoor zorgde dat deze stukjes schadelijke software konden worden opgespoord en verwijderd. Sindsdien is er veel veranderd.

Er zijn een groot aantal nieuwe bedreigingen, uitdagingen en risico's wat betreft de security in de onderneming. Bedreigingen kunnen gerangschikt worden onder twee grote noemers: interne bedreigingen en externe bedreigingen. Daarbinnen kan men ook het onderscheid maken tussen menselijke en niet-menselijke bedreigingen.

Momenteel vinden er in het IT-landschap een aantal evoluties plaats. Deze evoluties hebben een impact op de manier hoe er zaken wordt gedaan. Deze evoluties hebben dus een belangrijke impact op het hele ICT gebeuren. De belangrijkste evoluties de laatste jaren zijn:

- Instant Messaging
- SAAS
- SOA
- Mobile computing
- Virtual computing
- Cloud computing

Deze ingrijpende trends zullen het ICT-landschap voor altijd wijzigen. (Arend, et al., 2009) Ondernemingen zullen hierbij rekening gaan moeten houden, willen of niet. Indien ze daarbij geen rekening houden zullen ze hopeloos achterop raken en dit kan negatieve implicaties hebben.

Beveiliging is een vandaag de dag een cruciaal gegeven binnen de bedrijfsvoering. Om problemen te voorkomen moet de onderneming voldoende aandacht besteden aan beveiliging van haar informatiesystemen. De security policy is een cruciaal onderdeel in de beveiliging van de

onderneming. Volgens Wood (1995) hebben policies de volgende functie : "*Policies act as clear statements of management intent and demonstrate that employees should pay attention to information security"* De trends zullen ertoe leiden dat de security policy moet aangepast worden opdat men rekening houdt met deze trends. Er zijn vele typen policies. Whitman en Mattord (2009) onderscheiden de volgende typen:

- Enterprise information security policy
- Issue specific security policy
- System specific security policy

In het laatste hoofdstuk wordt ere en issue specific policy ontwikkeld voor de Blackberry smartphones opdat deze van buiten het bedrijfsnetwerk connectie kunnen maken met de bedrijfsnetwerken.

Er zijn ook een aantal internationale standaarden ontwikkeld die bedrijven een houvast bieden met het ontwikkelen van een security policy. Een drietal standaarden werden van dichterbij bestudeerd:

- Control Objectives for Information and related Technology
- Generally Accepted System Security Principles
- ISO 27002

Deze drie standaarden hebben elk een andere benadering. Daar waar COBIT eerder praktisch is van aard zullen de andere twee standaarden eerder theoretisch zijn. Ze geven tevens ook niet meteen een manier hoe trends, zoals eerder vernoemd, moeten worden opgevangen. Maar ze bieden wel een houvast.

In dit werk werd dan beslist om te gaan onderzoeken hoe één van deze evoluties, mobile computing, een invloed kan hebben op de security policy die wordt gehanteerd in de onderneming. Om dit probleem te kunnen aanpakken moet men eerst naar beveiligingproblemen binnen mobile computing gaan kijken. Door het NIST (2008) werd een groot aantal problemen vastgesteld voor mobiele toestellen:

- Verlies, diefstal of het afschrijven

- Ongeautoriseerde toegang
- Malware
- Spam
- Elektronisch afluisteren
- Cloning
- Server resident data
- Wireless security

Volgens Hoffman (2007) zijn smartphones onderhevig aan de volgende bedreigingen:

- Malware
- Direct Attack
- Data-Communication Interception
- Authentication Spoofing and Sniffing
- Physical Compromise

Het beveiligen van de toestellen is natuurlijk niet voldoende. Sommige applicaties, zoals mobiel leren, worden door reizende werknemers gebruikt. Mobiel leren is tevens een vanuit beveiligingsstandpunt interessante applicatie om te beveiligen. Zulk een applicatie bevat de meeste beveiligingsuitdagingen die ook bij andere applicaties voorkomen. De applicatie zorgt voor tijdelijke data op het toestel en de transmissiedata moet worden beveiligd. Men mag ook niet de toegang tot de applicatie uit het oog verliezen. Daarnaast moet toegang tot het toestel worden beveiligd.

Het probleem om een mobiel toestel, in ons geval een Blackberry smartphone, te beveiligen moet dus worden aangepakt op basis van drie onderdelen: device-level authentication, transmissiebeveiliging en de beveiliging van het bedrijfsnetwerk.

Door een interview met een expert van KBC werd een praktijkvoorbeeld uitgediept. KBC houdt een aantal practices erop na die zij als bank toepast om zo veilig mogelijk te werken. Zo zullen ze gebruik maken van het perimeterconcept binnen de onderneming en ze maken gebruik van een whitelist. Tevens schakelen zij de gebruiker in als firewall omdat de hoeveelheden informatie enorm zijn.

Om aan al deze problemen een oplossing te bieden werd er gestructureerd tewerk gegaan. Het probleem werd opgesplitst in drie deelproblemen die werden behandeld.

- lokale data en applicatiedata(statische, vluchtige data behoort tot het deelprobleem), toegang tot het toestel en het digitaal leerplatform,
- malware en hackers,
- datatransmissie

Elk van deze deelproblemen wordt uitgebreid behandeld binnen dit werk. Tenslotte wordt er als voorbeeld een implementatie uitgevoerd van een Blackberry Enterprise Server Express in combinatie met Windows 2003 server Enterprise en Exchange Server 2006 om tot een veilige omgeving te komen. Hierbinnen worden de concepten toegepast in een reële situatie om Blackberry smartphones op een veilige manier connectie te laten maken met bedrijfsapplicaties en bedrijfsgegevens.

Inhoud

Figuren

Tabellen

Bijlagen

1.1 Probleemstelling

1.1.1 Hoofdonderzoeksvraag

In de huidige bedrijfsomgeving is het in sommige gevallen cruciaal dat de werknemers kunnen beschikken over bedrijfsinformatie wanneer onder weg zijn. Zo wordt mobiel surfen niet langer als een luxe beschouwd maar maakt het onderdeel uit van de genetwerkte strategie van de onderneming. (Lopez, 2009) Er zijn tal van initiatieven en evoluties waardoor de werknemer steeds meer gebruik gaat maken van mobiele apparaten. Zo kan men met behulp van mobiele telefoons e-mail berichten controleren ver buiten de bedrijfsmuren. In deze context wordt vaak gebruik gemaakt van mobiele apparaten zoals smartphones. Dit zijn kleinere toestellen dan bijvoorbeeld laptops en ze zijn dus draagbaarder.

Door onder andere de globalisering zijn werknemers ook verplicht ver te reizen om contacten te onderhouden met leveranciers en klanten. (Norberg, 2002) Tijdens het reizen brengt men veel tijd door in transit. Deze tijd kan nuttig worden besteed. Hier kan mobiel leren een uitkomst bieden opdat deze tijd vanaf nu nuttig wordt besteed.

Het probleem dat onstaat door deze nieuwe werksituatie, de evolutie van mobile computing en mobiel leren, is dat de IT-afdeling aanpassingen zal moeten doorvoeren indien ze het lekken van data en andere beveiligingsincidenten wil voorkomen. Maar in welke mate, met andere woorden: waar moet de onderneming op letten? Dit werk probeert een licht te werpen op deze vraag en een advies te geven. Daarom luidt de centrale onderzoeksvraag als volgt:

> **"Hoe moet de organisatie haar beveiligingsbeleid aanpassen om tegemoet te komen aan de nieuwe bedreigingen als gevolg van de technische evoluties? Meer bepaald, hoe moeten de policies binnen de onderneming worden aangepast. "**

Er wordt gewerkt met behulp van een aantal subvragen:

1. **"Wat zijn de bedreigingen voor een informatiesysteem?"**

Alvorens men een aanpak voor de bedreigingen kan formuleren moet worden vastgesteld welke de bedreigingen zijn. Dit op een zo algemeen mogelijk manier opdat er geen bedreigingen uit het oog worden verloren. Een gedetailleerde bespreking wordt niet gegeven. Het doel is een overzicht te creëren.

2. **"Geef een omschrijving van nieuwe ICT hulpmiddelen. Welke nieuwe bedreigingen, uitdagingen en risico's zijn het gevolg van de nieuwe IT omgeving?"**

Het is van belang om nieuwe evoluties te gaan van naderbij bekijken om te bepalen waar de onderneming moet op inspelen, welke zijn de bedreigingen met betrekking tot de evoluties.

3. **"De IT security policy. Wat is het? Geef een omschrijving."**

Nadat de verschillende evoluties zijn bepaald moet de onderneming aanpassingen doorvoeren op de IT security policy. Maar alvorens men dit kan doen moet een inzicht verkregen worden in best practices rond security policies. Welke standaarden zijn handig, welke niet? Hoe worden evoluties aangepakt door de internationale standaarden.

4. **"Wat zijn de bedreigingen voor mobile computing(smartphones)? Hoe worden de smartphones momenteel beveiligd?"**

Wanneer het belang is vastgesteld moet worden bepaald wat de specifieke bedreigingen als gevolg van de evolutie van mobile computing zijn, meer bepaald wat zijn de bedreigingen voor smartphones?

5. **"KBC heeft een policy opgebouwd om het hele ICT gebeuren onder controle te houden. Hoe hebben ze deze policy aangepast om tegemoet te komen aan de problematiek van nieuwe evoluties waaronder mobiele apparaten? "(case)**

Op een kleine schaal kan de onderneming makkelijker beveiligingsincidenten aanpakken. Maar wat gebeurt er wanneer de onderneming op grote schaal moet worden beveiligd? Hoe gaat ze om met grote hoeveelheden gegevens. Hoe gaat men in grote bedrijven om met de

complexiteit om informatiesystemen te beschermen. Dit deel zal gaan over security management en deels over de ICT security policy bij KBC.

6. **"Wat is mobile learning en hoe kan mobile learning afdoende worden beveiligd? "**

Een interessante applicatie die momenteel vaker wordt gebruikt is mobile learning. Deze deelvraag probeert een antwoord te vinden op wat mobile learning is en welke specifieke eisen zulk een applicatie vereist. Dit is van belang wanneer men later een advies wil opbouwen hoe de onderneming mobiele applicaties wenst te beveiligen.

1.1.2 Methodologie

Deze eindverhandeling is van start gegaan met behulp van een literatuurstudie. Zo kon er een dieper inzicht verkregen worden in de materie. Er kon zich een algemeen beeld worden gevormd van de huidige stand van zaken en een inzicht in de evoluties die zich voordoen. De verkenning van de evoluties was belangrijk voor het bepalen van nieuwe bedreigingen. In het begin van het onderzoek werd er geen specifieke beperking ingesteld op de soort van bedreigingen. Wanneer de waaier breed wordt gehouden in het begin kunnen er minder bedreigingen uit het oog verloren worden. Later werd er toegespitst op bedreigingen enkel voor mobile computing, meer bepaald smartphones. Deze beperking was vereist vermits het aantal evoluties en bedreigingen te groot bleek te zijn.

Naderhand werd er overgegaan tot een discussie met experten dewelke hun inbreng hadden die later zou worden opgenomen. Ze gaven een dieper inzicht in hoe werd omgegaan met grotere hoeveelheden data en hoe deze effeciënt konden worden beveiligd. Tevens werd er een inzicht verkregen in het gebruik van Blackberry toestellen in bedrijfsomgevingen en best practices in beveiliging hieromtrent. Daarom werd besloten toe te spitsen op smartphones van het type Blackberry, dit in combinatie met mobile learning. De reden voor deze keuze was dat Blackberry smartphones vaak worden gebruikt in een bedrijfsomgeving en de nieuwe evolutie van mobiel leren kon in het kader van beveiliging een interessante impact hebben. Tevens bleek een mobile learning applicatie onderhevig te zijn aan een grote hoeveelheid bedreigingen. Wanneer het mobile

learning platform veilig was vanuit technisch standpunt, dan zouden applicaties die minder beveiliging vereisten ook veilig zijn.

Uit de verkregen informatie van interviews en literatuurstudie kon er een advies worden gedestileerd hoe bedrijven best de beveiliging van de smartphones aanpakten en hoe dit aanpassingen vereiste in de IT security policy. Om het theoretische deel te kunnen verduidelijken werd er in een later stadium een praktijkgedeelte uitgewerkt. Het praktische deel van deze eindverhandeling bestaat uit het uitwerken van een voorbeeld implementatie waar de adviezen die eerder werden opgesteld in konden worden verwerkt. Zo heeft de lezer een goed inzicht in zowel praktijk als theorie.

1.1.3 Overzicht thesis

Hoofdstuk 1 bestaat uit een inleiding tot deze eindverhandeling. Er wordt een uiteenzetting gegeven van het probleem. Hierbij wordt de hoofdonderzoeksvraag samen met de subvragen en de methodologie geschetst. Daarna wordt er een overzicht gegeven van de hoofdstukken van de thesis samen met de inhoud.

In hoofdstuk 2 worden de nieuwe bedreigingen, uitdagingen en risico's beschreven. Deze worden omwille van duidelijkheid in twee categoriën gesplitst: interne bedreigingen, externe bedreigingen. Daarnaast wordt de categorie attacks apart besproken omdat dit een zeer belangrijk type van bedreiging is.

Hoofdstuk 3 geeft een beschrijving van de nieuwe evoluties die het IT landschap ingrijpend wijzigen. Deze evoluties zijn later in de thesis van belang om de mogelijke nieuwe bedreigingen te kunnen inschatten.

Het vierde hoofdstuk toont het belang aan van de IT security policy in de onderneming. Daarna wordt een overzicht gegeven hoe de belangrijkste internationale standaarden evoluties opvangen en hoe deze standaarden verschillen van elkaar.

In het vijfde hoofdstuk wordt dieper ingegaan op de specifieke bedreigingen voor mobile computing. De bedreigingen worden uitgebreid besproken. Deze bespreking komt van pas later in hoofdstuk 7 om een advies ter beveiliging te geven.

Het zesde hoofdstuk bekijkt de beveiligingspolitiek binnen KBC van naderbij. In dit heefdstuk wordt er tevens een uiteenzetting gegeven van de security policy van KBC en de manier hoe KBC omgaat met het inschatten van risico's.

In het zevende en laatste hoofdstuk wordt er met behulp van de vergaarde kennis uit de andere hoofdstukken een advies ter beveiliging van Blackberry smartphones gegeven. Er wordt ook een voorbeeld implementatie gedaan waarbij er wordt uitgegaan van een omgeving met een Blackberry Enterprise Server in combinatie met Microsoft Exchange server. Deze twee applicaties worden geïnstalleerd binnen een Windows 2003 server omgeving. Er wordt er ook van uitgegaan dat de werknemer wenst toegang te krijgen tot een mobile learning applicatie via een Blackberry smartphone binnen deze omgeving.

1.1.4 Inleiding

Toen IBM zijn eerste computer introduceerde in 1981 betekende 'computer security' niets meer dan het afsluiten van het bureau waar de computer zich bevond zodat niemand hem kon meenemen. (Rubenking, Computing Moves Into the Cloud, 2008) Maar in 1984 werd door onderzoeker Fred Cohen een volledig nieuwe term geïntroduceerd: 'computer virus'. (Cohen, 1984) Hij ontwikkelde een software die ervoor zorgde dat deze stukjes schadelijke software konden worden opgespoord en verwijderd. Sindsdien is er veel veranderd.

Vandaag de dag vormen de informatiesystemen een van de cruciaalste assets in de huidige bedrijfsvoering. (Doherty & Fulford, 2006) Alle gegevens die nodig zijn in de bedrijfsvoering zijn toegankelijk via de informatiesystemen en worden via deze weg opgeslagen. Zonder deze informatiesystemen kan de onderneming niet op een normale manier functioneren. Een mooi voorbeeld hiervan vindt u in de zogenaamde Technologie-, Media- en Telecommunicatie industrie. Deze is voor haar functioneren volledig afhankelijk van haar informatiesystemen. (Deloitte, 2006)

Het doel is dat de onderneming ervoor zorgt dat ze te allen tijde instaat voor de accuraatheid, integriteit en veiligheid van de informatiesystemen zodat haar werknemers zich kunnen fixeren op uitvoeren van hun job. (O'Brien & Marakas, 2005)

Bedrijven die in grote mate afhankelijk zijn van die gegevens en systemen kunnen ernstige schade oplopen indien ze buiten bedrijf zijn. Denk maar aan imago problemen en verloren opbrengsten door klanten die naar de concurrentie stappen. Graux (2008) bespreekt enkele cruciale vragen in verband met privacy. Hoe langer informatiesystemen buiten bedrijf zijn, des te groter de schade. Om de continuïteit van de bedrijfsvoering te verzekeren is het noodzakelijk dat bedrijven er aandacht aan besteden dat hun servers en dus ook de informatiesystemen te allen tijde beschikbaar zijn zodat klanten op hun wenken kunnen worden bediend en dat werknemers niet met hun handen in het haar zitten. Het is daarom niet ondenkbaar een zogenaamd 'business continuïty plan' op te stellen dat ervoor zorgt dat werknemers op een efficiënte en effectieve manier kunnen ageren indien er zich een probleem voordoet. (Busquiel, 2009) Maar voorkomen is uiteraard beter dan genezen. Net daarom is computer security een belangrijk topic.

De onderneming haar informatiesystemen staan bloot aan vele gevaren, zoals telkens weer blijkt uit een jaarlijkse survey uitgevoerd door het Computer Security Institute. Deze worden jaar na jaar logischerwijs diverser omdat technologieën evolueren en omdat tevens ook dagelijks nieuwe technologieën opduiken. Deze technologieën vormen een opportuniteit maar tegelijk ook een bedreiging. (Boni, 2000) Hieruit kan er worden afgeleid dat beveiliging iets is dat constant evolueert. Het is bedrijfsmatig van belang dat er voldoende aandacht aan wordt besteed. De nieuwe trends die zich aandienen, waarvan ik er later in dit werk enkele ga bespreken, lijken in de toekomst de toon te gaan aangeven. Als onderneming moet men met deze trends rekening gaan houden.

Er bestaan tal van vormen van misbruik. Het stelen van privé gegevens, stelen van bedrijfsgeheimen, privacyschending (Graux, 2008), enz. Om misbruik te voorkomen is het van belang dat informatiesystemen worden beschermd. Klassiek worden de bedreigingen van buitenaf meestal eerst onder de loep genomen. Maar werknemers kunnen soms ook misbruik maken van

gegevens uit de informatiesystemen. (Van Leemputten, 2009) Zo kan ook de privacy van klanten of collega's worden geschonden. (Graux, 2008)

De onderneming haar informatiesystemen staan niet alleen bloot aan softwarematige gevaren maar het fysieke aspect, de servers waarop de gegevens zijn opgeslagen, moet ook gevrijwaard worden. Volgens Van Der Beek (2007) werd uit een onderzoek uitgevoerd door netwerkspecialist Axians ontdekt dat 48 procent van Nederlandse bedrijven slecht voorbereid zijn op een ramp. Zo kan een brand zorgen voor de totale vernietiging van het datacentrum. Aardbevingen moeten ook als een mogelijk gevaar worden beschouwd. (O'Brien & Marakas, 2005)

In de ondernemingen werd in het verleden vaak te weinig aandacht besteed aan de beveiliging van de informatiesystemen. Men probeert momenteel een inhaalbeweging te maken om dit probleem op te lossen maar er moet nog veel werk verricht worden, dit blijkt uit een survey van 150 organisaties in de technologie-, media- en telecommunicatieindustrie. (Deloitte, 2006) Zo heeft Deloitte (2006) kunnen vaststellen dat de ondernemingen wel willen aandacht besteden aan beveiliging maar dat ze daartoe niet de middelen hebben: "73 percent of the companies surveyed expect to spend more time and money on security in 2006 but the average budget increase is expected to be only 9 percent." Maar uit recente vaststellingen is gebleken dat u dit best met een korrel zout neemt. Door de huidige crisis moeten vele bedrijven noodgedwongen gaan besparen. De IT-afdeling is een van de eerste onderdelen waarin als eerste zal worden geminderd in de uitgaven. Men zal ofwel sterk besparen of zelfs overgaan tot afschaffen van de afdeling. (De Rooij, 2009) Door de nieuwe evoluties die eraan komen, dewelke het IT-landschap volledig wijzigen, is dit niet de juiste reactie. De ondernemingspolicy zal moeten aangepast worden, nieuwe maatregelen zowel technisch als organisatorisch dringen zich op. De trends zullen, zoals aangetoond zal worden, een grote impact hebben op de manier hoe men met IT omgaat. Tevens zullen de trends een grote impact hebben op de security in de onderneming.

2 Bedreigingen, uitdagingen en risico's voor de bedrijfsinformatiesystemen

In dit hoofdstuk geven we een overzicht van de bedreigingen voor elke organisatie, van zowel de interne als de externe bedreigingen. Er wordt in dit hoofdstuk een overzicht gegeven van de gevaren, risico's en de uitdagingen.

Een jaarlijks onderzoek verricht in de Verenigde Staten, het CSI rapport, stelde vast dat het meest kostelijke beveiligingsincident financiële fraude was. Per geval werd er een kost vastgesteld van $ 500,000 (Computer Security Institute, 2008) Het meest voorkomende incident in 2007 was een virus incident, dit werd in bijna 50% van de ondervraagde ondernemingen vastgesteld. (Computer Security Institute, 2008)

In bedrijven wordt vaak aandacht besteed aan de externe bedreigingen. Maar vaak verliest men de interne bedreigingen, zoals de eigen werknemers, uit het oog omdat men teveel bronnen moet aanwenden om bedreigingen van buitenaf te behandelen. Het is ook van belang hieraan aandacht te besteden. Ontevreden werknemers kunnen immers de informatiesystemen saboteren. (NIST, An Introduction to Computer Security: The NIST Handbook, 2006) De mogelijkheid tot fraude mag niet uit het oog verloren worden, welke kan resulteren in hoge kosten. (Computer Security Institute, 2008)

Hier volgt een bespreking over de meest voorkomende bedreigingen. Deze informatie werd geselecteerd uit enkele surveys.

2.1 Bedreigingen

Door de diversiteit van mogelijke bedreigingen van informatiesystemen is een overzicht geven van alle mogelijkheden onmogelijk. Toch wordt er getracht in tabel 2 een overzicht te creëren van bijna alle mogelijke bedreigingen, doch in zeer algemene vorm.

Alvorens verder in te gaan op de diverse typen bedreigingen moet worden bepaald wat een bedreiging is: in de context van information security is een bedreiging of threat een persoon of een

object dewelke een constante bedreiging vormt voor een asset. (Whitman & Mattord, 2009) In dit geval is het asset de informatie die nodig is in de bedrijfsvoering.

Tabel 2 bevat een opsomming van de mogelijke bedreigingen in hun simpelste vorm. Hierin worden praktisch alle mogelijke bedreigingen opgenomen, maar sommige vallen buiten het bestek van dit werk. Opdat we geen enkele cruciale bedreiging uit het oog verliezen zullen we eerst met een brede waaier aan bedreigingen beginnen. In dit werk wordt later pas specifiek ingegaan op de bedreigingen voor mobiele toestellen en mobiele applicaties, meer bepaald de bedreigingen voor smartphones: Blackberry toestellen.

De bedreigingen die van belang zijn in dit werkt werden vet gedrukt. Ze worden lager verder besproken. Naast elke bedreiging wordt vermeld waar ze kan onstaan: intern ofwel extern. In sommige gevallen is dit niet van toepassing, dit wordt erbij vermeld. Tevens kunnen bedreigingen al dan niet menselijk zijn, dit vormt ook een groot onderscheid.

Tabel 1: Bedreigingen, menselijk en niet-menselijk. Aangepast overgenomen van Bayne (2002)

Menselijk	Niet-menselijk
Hacker (intern, extern)	Overstromingen (extern)
Diefstal (intern, extern)	Blikseminslagen (extern)
Niet-technisch personeel: bijvoorbeeld het financieel personeel (intern)	**Schadelijke code** (intern, extern)
Ongelukken (intern, extern)	Brand (niet van toepassing)
Onvoldoende getraind IT personeel (intern)	Elektriciteit: stroompiek, stroomuitval (niet van toepassing)
Backup personeel (intern)	Lucht; stof (niet van toepassing)
Technieker en elektriciens (intern, extern)	Warmte: te warm, te koud (niet van toepassing)
	Hardware failure: oude hardware (intern, extern)

De conclusies die kunnen worden getrokken uit deze tabel is dat er een zeer groot aantal 'menselijke' bedreigingen zijn, hiervan zijn er een groot aantal die uitgaan van de eigen werknemers. Dit benadrukt dat men als onderneming een sterk beveiligd systeem kan ontwikkelen en implementeren en eveneens grote budgetten investeren, maar uiteindelijk komt het erop neer dat men vertrouwen moet kunnen stellen in de werknemer. Hij krijgt namelijk paswoorden en toegang tot vertrouwelijke gegevens in onderneming en indien hij wil kan hij deze doorspelen aan de concurrentie. De gebruiker moet in feite als een firewall worden ingezet. Als hij deze functie niet vervult zullen gegevens uit de onderneming lekken. Dit is een filosofie die ik ook heb kunnen vaststellen bij KBC. (lager) Tevens moet de onderneming ook best nadenken over functiescheidingen om voorvallen zoals fraude te voorkomen. (Mercken, 2009) Maar dit valt niet binnen het bestek van dit werk.

2.1.1 Interne bedreigingen

Interne bedreigingen zijn die bedreigingen die hun oorsprong binnen de onderneming plaatsvinden. U vindt hier nu een uiteenzetting van de meest voorkomende types.

2.1.1.1 Onopzettelijke fouten

Onopzettelijke fouten zijn die fouten die voortkomen uit een onoplettendheid of slordigheid. De werknemer maakt bijvoorbeeld een typfout. Dit vormt niet meteen een bedreiging voor de infrastructuur en assets maar het vormt wel een bedreiging voor de integriteit (NIST, An Introduction to Computer Security: The NIST Handbook, 2006) van de gegevens en data. Er kunnen ook foute waarden worden ingegeven, dewelke kunnen leiden tot een crash van de informatiesystemen. In dat geval heeft het natuurlijk wel een impact op de data, namelijk dataverlies kan voorkomen. Dus de impact van dit soort fouten is zeker niet te onderschatten.

Een ander type onopzettelijke fouten waar men in het dagelijks leven ook vaak mee te maken heeft zijn bugs. Bugs zijn fouten die zich in de programmacode bevinden. Als gevolg van bugs kunnen systemen crashen of erger. Het NIST (2006) stelde het volgende: "*Programming and*

development errors, often called "bugs," can range in severity from benign to Catastrophic." Men kan dit soort problemen voorkomen door werknemers enkel toegang te geven tot de juiste bestanden. (een effectieve manier van toegangscontrole) Ook hetgeen wat men quality control measures noemt moeten aanwezig zijn in de onderneming en deze zorgen ervoor dat dit soort problemen zoals die hierboven beschreven staan niet meer voorkomen. Aandacht besteden aan inputcontrole en aan een duidelijke software interface in combinatie met procedures die fouten voorkomen kunnen heel wat onheil voorkomen. (Mercken, 2009)

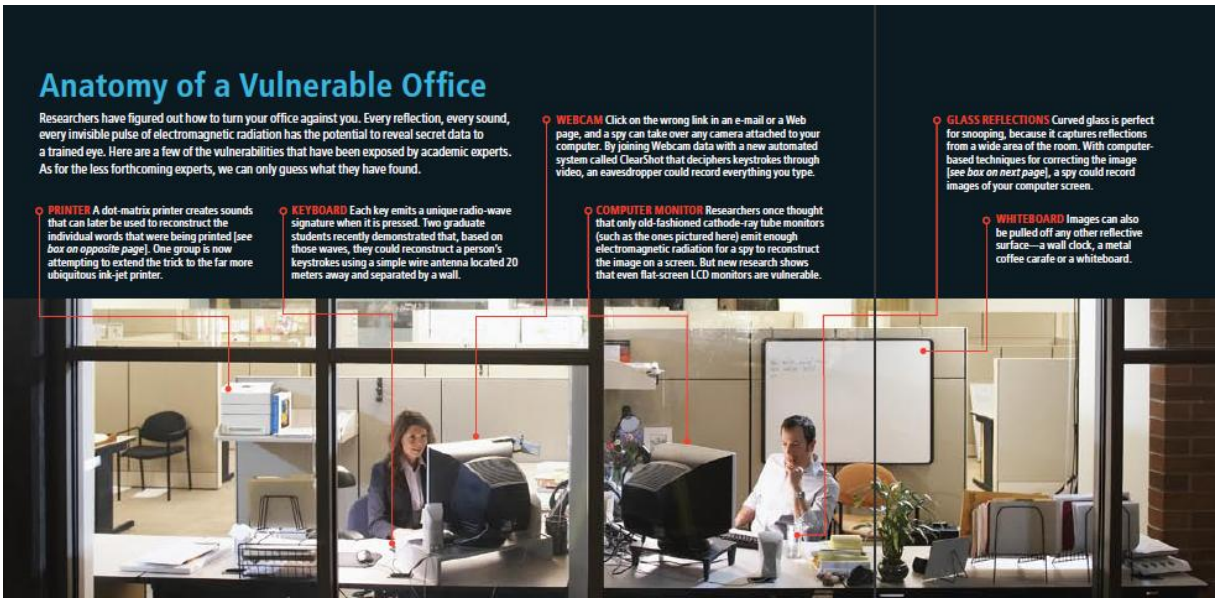
2.1.1.2 Werknemer sabotage

Werknemer sabotage is een bedreiging waarbij de werknemer doelbewust het informatiesysteem onklaar maken. Werknemers hebben immers een goed zicht waar de kwetsbaarheden zich bevinden en welke onderdelen cruciaal zijn voor een goed functioneren van de onderneming. (NIST, An Introduction to Computer Security: The NIST Handbook, 2006) Een werknemer kan bijvoorbeeld virussen introduceren in het netwerk waardoor de computers die met het netwerk verbonden zijn bedreigd worden. Zo kan een kwaadwillende werknemer , indien de toegang tot serverlokalen slecht beveiligd is, de servers uitschakelen. (Mercken, 2009) Als gevolg van zulke problemen lijdt de onderneming verlies. Vaak zijn dit werknemers die op een of andere manier ontevreden zijn met de situatie waarin zij verkeren. Het is dus aan te raden dat de onderneming erop toeziet dat de werknemers tevreden zijn om zulke voorvallen te voorkomen.

2.1.1.3 Industriele spionage of economische spionage

Industriële spionage of economische spionage, in het kader van dit werk, is een misdrijf waarbij er aan spionage wordt gedaan met behulp van elektronische hulpmiddelen: spionage via de computer of via netwerken. De 'hacker' zal zich binnenin de organisatie bevinden en deze zal allerlei bedrijfskritische informatie gaan stelen en doorspelen of doorverkopen aan de concurrentie tegen een vergoeding. (Campo, Epting, Heirdeis, Jeager, Koops, & Pohlmann, 2002) De concurrentie kan op die manier haar hand leggen op plannen van nieuwe productinformatie of andere geheime

informatie van het bedrijf. Een voorbeeld van de mogelijkheden van spionage vindt u in de volgende schets.



Figuur 1: How to spy in the office? (Gibbs, 2009)

De voorgaande figuur vindt u terug in bijlage 3 samen met een andere figuur waarin men uit de doeken doet hoe men kan spioneren op een printer door middel van het geluid dat een printer maakt. Natuurlijk is dit verregaand, maar dit zijn allen mogelijkheden waarop er data kan lekken uit de organisatie. De boodschap is dat gebruikers voorzichtig moeten omspringen met het gebruik van de apparatuur en software.

2.1.1.4 Fraude

Fraude is een soort van misdrijf dat vaak voorkomt in de financiële sector. Vandaag de dag automatiseert men traditionele methodes. Bij het automatiseren zal men proberen fraude te plegen door stukjes code in te brengen in de programmacode. (NIST, An Introduction to Computer Security: The NIST Handbook, 2006)

Zowel insiders als outsiders kunnen fraude plegen. Volgens Mercken (2009) kan fraude op tal van manieren gepleegd worden. De onderneming moet beschikken over een goed intern audit systeem welk dit zal voorkomen. Jaarlijks, of vaker, zal een externe firma de onderneming ook onderwerpen aan een audit. (Mercken, 2009)

2.1.1.5 Employee sabotage

Kwaadaardige code wordt in het volgende onderdeel verder besproken. Werknemers kunnen met opzet, uit wraak, kwaadaardige code gaan introduceren in de bedrijfsinformatiesystemen. Dit kan tot grote problemen leiden: uitval van de systemen, vertraging van het functioneren. (NIST, An Introduction to Computer Security: The NIST Handbook, 2006) Volgens het NIST (2006): "*The number of incidents of employee sabotage is believed to be much smaller than the instances of theft, but the cost of such incidents can be quite high*." Daarom is het van belang zeker rekening te houden met deze component.

2.1.2 Externe bedreigingen

Malicious code, malware, schadelijke code het zijn verzameltermen. Onder malicious code kan elke soort van code die de intentie heeft om informatie te stelen of kapot te maken worden verstaan. Hieronder vallen virussen, wormen en trojan horses. (Whitman & Mattord, 2009) De hoeveelheid malware is het voorbije jaar enorm toegenomen. (Panda Security, 2009) Daarom is het van belang dat we dit probleem verder gaan bekijken in dit onderdeel.

2.1.2.1 Virussen en wormen

Virussen zijn een algemene term voor allerlei soorten uitvoerbare codes die zich hechten aan andere programma's. Wanneer deze worden uitgevoerd zal het programma de computer proberen onklaar te maken of deze beschadigen en zich eventueel verder verspreiden. (Panko, 2005) Virusverspreiding vindt plaats via de bedrijfsnetwerken of via informatiedragers die mobiel zijn zoals een floppydisk, een cd of een memorystick.

Wormen zijn echter een andere vorm van kwaadaardige code. Dit zijn stukjes software die zichzelf propageren. Virussen doen dit niet, ze hebben immers een pogramma nodig waaraan ze zich kunnen hechten. Ze moeten, net zoals in de natuur een virus gebruik maakt van de cellen van zijn gastheer, gebruik kunnen maken van externe code. Deze externe code kan bijvoorbeeld een het besturingssysteem of ander reeds geïnstalleerd programma zijn. (Whitman & Mattord, 2009) Ze zijn ook afhankelijk van menselijke interventie, bijvoorbeeld het openen van een e-mail bijlage. (Panko, 2005) Wormen kunnen zelfstandig opereren. Zo heeft men e-mailwormen die via e-mail worden verspreid. Deze wormen zullen zichzelf e-mailen naar alle contactpersonen waarover de geïnfecteerde computer beschikt zonder menselijke interventie.

2.1.2.2 Trojan Horse

Trojan horses zijn een aparte klasse. Dit zijn stukjes schadelijke code die hun ware aard verbergen. Ze tonen hun ware aard alleen wanneer ze zijn geactiveerd. (Whitman & Mattord, 2009) Volgens Whitman en Mattord (2009) zullen ze er als volgt uitzien: ' *Trojan horses are frequently disguised as helpful, interesting pieces of software such as readme.exe files often included with shareware or freeware packages.'* Net daarom zullen ze worden geactiveerd: ze lijken op het eerste zicht onschuldig.

Panda Security (2009) heeft het voorbije jaar een toename vastgesteld in de hoeveelheid besmette machines, ze werden vooral besmet met software die als bedoeling heeft vertrouwelijke of persoonlijke data te stelen. Deze gevoelige informatie werd gestolen met behulp van trojan horses. Trojans werden vooral ontworpen voor het stelen van private data. Van alle malware die Panda Security ontvangt ter onderzoek, omvat 71% van de 37.000 samples Trojaanse paarden. (Panda Security, 2009) Dit is aanzienlijk. U kan de toename van malware om aan identity theft te doen vaststellen uit onderstaande grafiek. Op de horizontale as ziet u de tijd, op de verticale as is het aantal infecties door malware weergegeven.

Figuur 2: Malware infections ontworpen om persoonlijke data te stelen. Bron: (Panda Security, 2009)

2.1.2.3 Phishing en pharming

Met behulp van phishing en pharming zullen personen met kwade bedoelingen proberen te 'vissen' naar echte gegevens bij gebruikers. Wanneer pharming wordt toegepast zullen gebruikers een op het eerste zicht legitieme site komen. Nadien blijkt dat dit een vervalsing was die was nagemaakt om gebruikersgegevens te verkrijgen. Bij pharming wordt vaak gebruik gemaakt van malicious code om de gebruikers naar de vervalste site te leiden. (Whitman & Mattord, 2009) Onwetende, naieve gebruikers zullen zich laten vangen en gebruikersinformatie doorspelen aan een op het eerste zich legitieme website.

2.1.2.4 Diefstal

Een laatste bedreiging die zowel intern als extern haar oorsprong kan vinden is diefstal. Werknemers kunnen delen van de IT-infrastructuur stelen maar ook externen kunnen een mobiel toestel stelen. In het kader van dit werk is de diefstal van een smartphone zeker niet ondenkbaar. Zulke toestellen kunnen worden gestolen omdat ze klein en dus zeer mobiel zijn. Uit een survey van Harrington & Mayhew (2001) is gebleken dat het aantal diefstallen van mobiele telefoons door de jaren heen toeneemt. De resultaten van deze survey kunnen worden gevonden in de volgende figuur.

British Crime Survey estimates of mobile phone thefts (those aged 16 or more)

	1995	1997	1999	2000
Mobile phones stolen 1	160,000	270,000	400,000	470,000
% of all thefts	1.1%	2.6%	4.0%	5.5%

1 Based on risk figures grossed up to the population of England and Wales aged 16 or more. The risks relate to incidents in which a phone was stolen or an attempt was made.

Figuur 3: Aantal diefstallen van mobiele telefoons (Harrington & Mayhew, Mobile phone theft, 2001)

Dit is voor de onderneming een niet te onderschatten probleem. Men moet ook in het achterhoofd houden dat er soms gevoelige data op deze toestellen kan staan. Net daarom is het van belang.

2.1.3 Attacks

Attacks zijn een bedreiging die zowel intern als extern kan worden uitgevoerd. Omdat deze categorie uitgebreid is en zeer belangrijk wordt ze naast de externe en interne bedreigingen besproken. Aanvallen kunnen zowel intern als extern hun oorsprong vinden: zowel een werknemer als een derde kan een aanval uitvoeren op de bedrijfsnetwerken.

Er zijn veel soorten van aanvallen: malicious code, brute force attacks, dictionary attacks, spoofing, DOS-attacks, … (Whitman & Mattord, 2009) Zoals u kan zien is er een grote diversiteit

van aanvallen. Ik zal in het kader van dit werk er slechts enkele bespreken. Vermits er een grote diversiteit hierin is kan men hierin zeer ver gaan.

2.1.3.1 Hacking

Hacken op zich is een verzamelterm. Hacken, het inbreken in een systeem, kan op talloze manieren worden gedaan. Vroeger waren hackers eerder hobbyisten die hun kennis probeerden te bewijzen door middel van in te dringen in de systemen van de onderneming. Ze probeerden de gebruiker aan te tonen dat deze zijn computer slecht had beveiligd, maar ze deden verder niets met de gegevens. Tegenwoordig is dit niet meer het geval. (Campo, Epting, Heirdeis, Jeager, Koops, & Pohlmann, 2002) De hackers zullen vanaf nu overgaan tot het verkopen van de gegevens die ze vergaard hebben via het hacken van de computersystemen of deze op een andere manier misbruiken. Hackers treden tegenwoordig georganiseerd en professioneel op.

Er zijn verschillende typen van hacken. Deze zijn wat men hactivism noemt, hacking-for-ransom, hacking-for-theft en hacking-for-monetary purposes. (Elms, Laprade, & CPCU, 2008)

Hacking-for-ransom: Hacking-for-ransom is een relatief nieuw begrip. Het is een vorm van hacking waarbij de hacker gevoelige informatie probeert buit te maken over een bepaalde persoon. Hij zal deze persoon dan geld afpersen om de informatie zoals ze is te behouden, al dan niet in het geheim. In sommige gevallen zullen ze dreigen de gestolen informatie te wijzigen indien er een bepaalde som niet wordt betaald. (Elms, Laprade, & CPCU, 2008)

Hacking-for-theft en **Hacking-for-monetary :** Dit zijn vormen waartegen men zich als onderneming minder goed kan beschermen. Bij deze vorm zal de hacker informatie stelen en doorverkopen. Bijvoorbeeld zullen klantgegevens worden doorverkocht aan concurrenten. De reden waarom men zich hier moeilijker kan tegen beschermen is dat personeelsleden die slechte of oneerlijke bedoelingen hebben zich toegang tot gegevens kunnen verschaffen en deze doorverkopen. Men kan afgedankte personeelsleden wel buitensluiten maar voor de huidige kan men dit niet doen. (Elms, Laprade, & CPCU, 2008) Dit voorbeeld onderstreept nog maar eens hoe belangrijk het is ook te kunnen vertrouwen op personeel.

Het is van groot belang deze bedreiging correct in te schatten als onderneming. Een hacker kan in werkelijkheid de productie lam leggen. Deze bedreiging kan zowel intern als extern zijn oorsprong vinden.

2.1.3.2 Denial of service(DOS)

Een denial of service attack is een aanval waarbij een hacker controle neemt over een computer systeem met behulp van een progamma. Dan zal hij deze 'overgenomen' computer gebruiken om een aanval te lanceren waarbij hij de slachtoffer computer bombardeert met zogenaamde junk data opdat deze crasht. (Elms, Laprade, & CPCU, 2008) Men kan als hacker ook de aanval grotere proporties laten aannemen. Hierbij zal de hacker meerder computers overnemen en deze allemaal tegelijkertijd junk data laten sturen naar de geviseerde computer opdat deze zou crashen.

2.1.3.3 Wireless network breach

Een wireless network breach doet zich voor wanneer een kwaadwillende inbreekt op het draadloze bedrijfsnetwerk. Het draadloze netwerk kan moeilijker worden beveiligd omdat men de toegang niet opdezelfde manier kan afschermen. Deze bedreiging wordt verder beschreven in het onderdeel 5.2.6.

2.1.4 Conclusie

De onderneming moet een goed overzicht opbouwen van alle mogelijke bedreigingen die relevant zijn. Er zijn vele bedreigingen en ze zijn zeer divers zoals blijkt uit de opsomming. De categorie van attacks kan als zeer belangrijk worden bestempeld.

Men moet gevolg geven aan deze bedreigingen. Daarom moet de onderneming deze bedreigingen prioritiseren, net zoals KBC dit doet bij de risk assessment (later in dit werk hier meer over). Als alle risico's zijn vastgesteld die een negatieve impact kunnen hebben, gaat men best over naar het plannen van het omgaan met die risico's. Men moet een beveiligingsbeleid, of een security policy

uitzetten. De security policy kan veel problemen voorkomen. Door het uitvoerig plannen kan er op voorhand al geanticipeerd worden. Hierover kan u meer lezen in het hoofdstuk vier.

3 Nieuwe ICT hulpmiddelen en toepassingen, een omschrijving

Dit hoofdstuk zal dieper ingaan op de belangrijkste evoluties die zich voordoen in informatie technologie. Hier wordt er onderzocht hoe zulke evoluties kunnen zorgen voor beveiligingsproblemen. Elke trend wordt in dit hoofdstuk kort beschreven samen met een beschrijving van de mogelijke beveiligingsrisico's.

3.1 Instant messaging

3.1.1 Wat is instant messaging?

Instant messaging is een in ons leven vaak gebruikte trend. (Deloitte, 2006) Hoewel deze vaak wordt gebruikt, is het ook een tehchnologie die niet uitblinkt in veiligheid. (Symantec, Security Enterprise, 2006) Volgens de industrieanalisten Radicati en Gartner (2006, in Gililand, 2006) wordt instant messaging door meer dan 200 milioen mensen gebruikt in organisaties voor het werk of buiten het werk. Deze manier van communicatie is snel populair geworden omdat het een verbeterde manier van e-mail is (Hindocha, 2003) en omdat de manier van communicatie directer is. Omdat dit een zeer populaire technologie is, zal deze worden gebruikt als doelwit van een aanval. Toch tonen cijfers uit een recente survey van CSI aan dat het misbruik afneemt van 2007 naar 2008. (Gocsi, 2008)

3.1.2 Bedreigingen van Instant Messaging

Instant messaging is onderhevig aan tal van bedreigingen. Volgens Symantec (2006) : *"Most IM systems presently in use were designed with scalability rather than security in mind."* Gebruikers, werknemers, moeten hiervan op de hoogte zijn dat dit een technologie is dewelke niet veilig is. Met behulp van instant messaging kan men niet enkel tekstberichten verzenden en ontvangen maar ook files. Op deze manier kan er schadelijke software worden overgebracht van de ene computer naar de andere. Tevens kunnen bugs in de instant messaging clients voor beveiligingsproblemen

zorgen. Op elke desktop, waarbij de gebruiker gebruik maakt van instant messaging, moet er een instant messaging client worden geïnstalleerd. (Hindocha, 2003) Indien er zich een zwakheid in deze client bevindt, dan is elke desktop waarop de applicatie geïnstalleerd is kwetsbaar.

Volgens de meest recente data van het Imlogic Threat Center (2006, in Gililand, 2006) zullen hackers gebruik maken van het vertrouwen dat de gebruiker heeft in een 'buddy'. Men ontwerpt dan een worm of virus die dat uitbuit. Accepteren van onbekende contactpersonen is dan logischerwijs ook uit den boze.

Nu wordt er overgaan naar het gedetailleerder bespreken van enkele bedreigingen:

- **Ongeauthoriseerde openbaarmaking** van informatie is een vaak voorkomend misbruik. In de onderneming worden vaak logs bijgehouden waarin de gesprekken zijn opgeslagen die worden gevoerd op een werkstation. Wanneer een hacker er in slaagt om deze logs in te kijken, dan er gevoelige bedrijfsinformatie worden gestolen (Hindocha, 2003) en dan kan tevens ook de privacy van werknemers worden geschonden.

- Instant messaging is een technologie die ook voor zogenaamde **DOS** aanvallen kwetsbaar is. (Symantec, 2006) DOS aanval staat voor Denial Of Service aanval en dit is een aanval waarbij een kwaadwillende gebruik maakt van een computer of meerdere (DDOS, Distributed Denial Of Service) computers om een andere computer te overstelpen met berichten. De slachtoffercomputer zal de berichten niet meer kunnen verwerken en als gevolg daarvan zal deze crashen. (Campo, Epting, Heirdeis, Jeager, Koops, & Pohlmann, 2002)

- **Hacken** (account hijacking) en misleiden van gebruikers is ook een misbruik dat vaak wordt toegepast. (Symantec, Security Enterprise, 2006) De gesprekspartner zal zich dan als iemand anders gaan voordoen.(spoofing) Maar ook het hacken van de gebruiker komt

vaak voor. De hacker maakt dan gebruik van bijvoorbeeld een trojan horse (zie lager) en zal op die manier het paswoord van de gebruiker achterhalen om dat dan te misbruiken.

- **Het verschaffen van toegang tot een werkstation** en op die manier de data wijzigen die daar aanwezig is ook voorkomend gevaar, samen met het afluisteren van een gesprek. (Symantec, 2006) Het afluisteren is relatief makkelijk indien de verbinding niet beveiligd is. Het verschaffen van toegang wordt meestal gedaan via bugs in de software. De kwaadwillende zal daarvan gebruik maken om zich toegang te verschaffen vanop afstand. Een wijze raad om dit te voorkomen is steeds de nieuwste versie van de software installeren en updates downloaden, indien beschikbaar. (Symantec, 2006)

- **Backdoor Trojaanse paarden** kunnen binnensluipen via een p2p protocol. Een instant messenger maakt daar vaak gebruik van. (Hindocha, 2003) Het trojaans paard kan de instant messenger zo instellen dat het alle files deelt die op de desktop aanwezig zijn en kan op die manier toegang verkrijgen tot de computer. Zo kan informatie worden gestolen en de computer kan onklaar worden gemaakt. (Hindocha, 2003)

- **Wormen** vormen een aanzienlijke bedreiging voor de security professional. Ze kunnen in feite via mail goed worden opgevangen door een anti-virus scanner te installeren op de e-mail server. Maar via instant messaging kan een worm pas worden opgevangen vanaf het moment dat hij de desktop bereikt waar er gebruik wordt gemaakt van de instant messenger. Daarom is het nodig ook een beveiliging te voorzien op de desktop zelf. Met andere woorden: de vele lagen moeten door een overkoepelend systeem worden beveiligd. Volgens Hindocha (2003) is ook van belang de werknemers voldoende te informeren van de gevaren zodat ze er niet met 'beide voeten' in trappen.

3.1.3 Advies ter beveiliging Instant Messaging

Blokkeren van instant messaging is moeilijk. De meeste beveiligingsbedrijven bieden wel een oplossing om de applicaties op poort-niveau af te sluiten. Maar dit blijkt niet altijd de oplossing te zijn. (Gilliland, 2006) Tegenwoordig heeft men ook de HTTP-tegenhanger van instant messaging. Deze messenger maakt gebruik van een browser. Een browser is meestal wel bechikbaar op de meeste dekstops in de onderneming en men kan deze dus moeilijker beperken, tenzij men individuele websites gaat blokkeren. Maar er is gebleken dat afsluiten of bannen niet meteen een goede oplossing is. Vandaag de dag gebruiken ongeveer 70 miljoen werknemers instant messaging voor bedrijfsdoeleinden, in 2005 was er een groei van 300 percent in het aantal bedreigingen met betrekking tot instant messaging. (Gilliland, 2006) Het bannen van instant messaging in de onderneming zou enkele problemen met zich meebrengen: frustratie bij de gebruikers enerzijds en afname in de productiviteit van de werknemers anderzijds. (Gilliland, 2006) Volgens een recente studie van Microsoft zou een investering in instant messaging een redelijke opbrengst met zich meebrengen. Dit kan u afleiden uit de volgende tabel waar u een uitwerking van een case vindt. (Gilliland, 2006) Zo kunt u afleiden uit figuur 1 dat Intel $25,000,000 bespaart in tijd over een periode van drie jaar door het gebruik van instant messaging.

Value Measures	**Results**
Internal rate of return (IRR)	Fair Isaac: 246 ercent
Payback	Te as Tech: 8 months
Cycle time	Fair Isaac: ⇩ delays by 100 hours er year er individual
Reduced conference call e ense	Siemens: ⇩ $95 er conference call
Productivity im rovements	Intel: ⇧ $25,000,000 in saved time over three years

Figuur 4: Hoeveel wordt er bespaard, de productivity improvements geven een idee. (Gilliland, 2006)

Beveiligen van instant messaging systemen is niet te onderschatten.Traditioneel zijn de systemen beveiligd op een gelaagde manier. Dit wil zeggen dat er wel software aanwezig is om bepaalde beveiligingsrisico's op te vangen maar omdat IM een specifieke manier van beveilging vraagt volstaat die aanpak niet. (Gilliland, 2006) Beter zou een een specifiekere overkoepelende aanpak

zijn, maar in bedrijven is deze nog niet meteen doorgesijpeld. Er zijn immers teveel applicaties waarmee u aan instant messaging kan doen.

Instant messaging clients kunnen niet enkel worden geïnstalleerd op desktops, ze kunnen ook worden geïnstalleerd op mobiele toestellen zoals laptops, smartphones en PDA's (Symantec, 2006). Net als dekstops zullen deze andere toestellen moeten worden gevrijwaard van de beveiligingsproblemen die instant messaging met zich meebrengt.

3.1.4 Conclusie instant messaging

Er kan geconcludeerd worden dat men de systemen best goed beheert en dat men zich als bedrijf best beperkt tot één applicatie (een universele client waarop men standaardiseert) die door de hele onderneming wordt gebruikt. Volgens Hindocha (2003) is het ook nuttig om desktops en andere toestellen binnen de organisatie lokaal te beveiligen zodat men gewapend is tegen DOS aanvallen, worms,… Men moet met andere woorden op meerdere 'lagen' veiligheid inbouwen.

3.2 SaaS

3.2.1 Wat is het?

Software as a Service is een relatief nieuwe trend. (Gyssels, 2009)Het is een verzamelnaam voor een nieuwe manier van zaken doen wat het softwarepark van bedrijven betreft. Softwarebedrijven gaan niet langer hun software verkopen op CD's, dewelke programma's bevatten die lokaal moeten geïnstalleerd worden maar de bedrijven zullen overgaan tot het aanbieden van hun paketten via het internet. Bedrijven die wensen gebruik te maken van die software zullen deze dan via het internet kunnen benaderen. De onderneming zal voor het echte gebruik van de applicatie betalen (Hines, 2007) en niet voor de software zelf. Dit wordt ook bevestigd door de Software & Information Industry Association (2007). Men betaalt als onderneming louter voor het gebruik van de applicatie, niet voor de aankoop van de applicatie. Maar gaan de software aanbiedende bedrijven wel voor afdoende beveiliging zorgen? Dit is een cruciale vraag voor de ondernemer die op zoek gaat naar een goede leverancier.

3.2.2 Voordelen en nadelen SaaS

Software as a Service is, zoals hoger aangehaald, een relatief nieuw paradigma. Maar zoals het vaak het geval is bij een nieuw paradigma heeft SaaS zowel zijn voordelen als zijn nadelen. De voordelen zijn: een makkelijkere implementatie, makkelijker onderhoud (upgrades en patches), flexibeler omgaan met licenties en beter applicatie life-cycle management. (Le Blanc, 2008) Tevens wordt de integratie van gegevens ook vergemakkelijkt. (Hines, 2007)

Een groot nadeel is dat er bij de implementatie een wijziging moet plaatsvinden bij de implementatie van SaaS waarbij de operaties worden getransformeerd naar een service aanbiedende benadering, dit kan wel eens een ingrijpende en moeilijke verandering zijn. En opdat de onderneming Software as a Service kan aanbieden is het noodzakelijk dat ze beschikken over een veilig, altijd beschikbaar data-centrum voor de klant zodat deze nooit zonder de service valt. (Le Blanc, 2008)

3.2.1 Bedreigingen SaaS

Maar wat zijn de problemen met SaaS, eens de nogal moeilijke aanpassingsfase voorbij is? Het overzicht vormt een van de grootste pijnpunten: de mate waarin de onderneming nog een duidelijk overzicht op de IT-operaties. (Schwartz, 2006) Een voorbeeld dat Schwartz (2006) aanhaalt is een onderneming die bestaat uit 10 afdelingen met een 5000-tal werknemers. Elke afdeling maakt gebruik van ongeveer 10 applicaties die via het SaaS model worden aangeboden. Cruciaal is nu hoe een nieuwe gebruiker wordt toegevoegd indien er een nieuwe werknemer in de onderneming komt, of een gebruiker de toegang ontzeggen indien hij de onderneming verlaat. Hoe worden paswoorden gemanaged? Deze vragen tonen aan dat het zeer moeilijk is om al deze applicaties overzichtelijk te beheren. Kwaadwillenden kunnen van zulke situaties gebruik maken om gebruikersgegevens te bekomen om op die manier bijvoorbeeld geheime informatie te bekomen. Een oplossing, volgens Schwartz (2006), is het gebruik van een paswoord in combinatie met een token. Iets wat men in de hand heeft en een paswoord, dit wordt gereguleerd door de HR-afdeling.

3.2.2 Conclusie SaaS

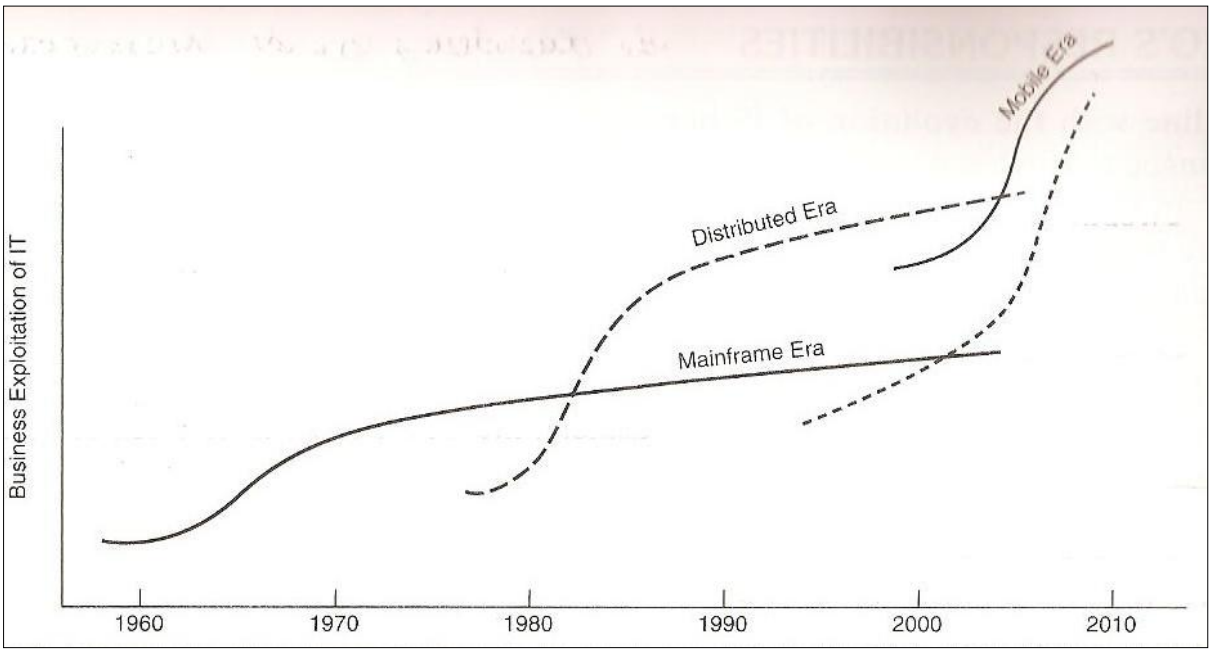
Ondernemingen kunnen zich richten op de kern van de zaak omdat ze vanaf nu gebruik kunnen maken van SaaS. Maar men moet als onderneming trachten een goede leverancier te vinden welke zijn diensten voldoende beveiligt. Zoniet kan men als onderneming voor verrassingen komen te staan zoals gebruikers die bestanden kunnen inkijken die vertrouwelijk zijn.

3.3 Gebruikers en applicaties worden mobiel

3.3.1 Wat is Mobile computing?

Mobiele technologie, met andere woorden mobile computing, wordt momenteel vaker gebruikt in de bedrijfswereld dan vroeger. (Arend, et al., 2009) Mobiel surfen wordt niet langer als een luxe beschouwd maar maakt onderdeel uit van de genetwerkte strategie van de onderneming. (Lopez, 2009) Er zijn tal van initiatieven en evoluties waardoor de werknemer steeds meer gebruik gaat maken van mobiele apparaten. Zo kan men met behulp van mobiele telefoons e-mail berichten lezen onder weg.

De meest bekende hardwareondernemingen zoals Dell (Wokke, 2009) zullen daarom een sprong wagen op de mobiele telefoonmarkt om toch maar een graantje mee te pikken. Mobiele operators, zoals Telenet (Telenet Mechelen, 2010) of Proximus (Proximus, 2010) hebben tevens ook formules die mobiel surfen aanmoedigen. De volgende figuur bevestigt de vaststelling dat het ‘mobile era’ steeds verder doordringt.



Figuur 5: Major IT eras (McNurlin, Sprague, & Bui, 2009)

Vermits er vanaf nu meer met een mobiele platforms wordt gewerkt zal ook dit ook extra beveiligingsrisico's met zich meebrengen.

3.3.1 Bedreigingen mobile computing

Mobiele apparaten vormen een makkelijk doelwit. Zo zullen PDA's, laptops, mobiele telefoons en andere mobiele apparaten vaak worden gebruikt om verbinding te maken met het bedrijfsnetwerk. Daarom worden deze toestellen vaak geviseerd en door hackers die via deze weg proberen gegevens te ontvreemden. (Deloitte, 2006) Uit onderzoek is gebleken dat de beveiliging die wordt toegepast op sommige mobiele toestellen slechts weinig bescherming biedt. In sommige gevallen is de graad van beveiliging slechts het niveau van het oude besturingssysteem Microsoft Windows 95. De beveiliging laat met andere woorden dus te wensen over. (De Rooij, 2009)

Mobiel werken op zich brengt gevaren met zich mee afhankelijk van het OS dat wordt gebruikt. De reizende werknemer maakt bijvoorbeeld soms gebruik van wat men in jargon 'off-line werken' noemt. Hij heeft dan geen directe internetverbinding maar hij kan toch deels met internetbestanden werken. Dit kan onverhoopte gevolgen met zich meebrengen. Zo heeft

'beveiligingsevangelist' Michael Sutton aangetoond dat een aanvaller betalingsgegevens kan bekomen omdat die off-line beschikbaar werden gesteld. (De Rooij, 2009)

Een andere moeilijkheid die zich niet aanbiedt op het gewone PC-platform is dat er mobiel met uiteenlopende platforms worden gewerkt. Dit is natuurlijk een extra moeilijkheid voor de onderneming om te managen. Een kleine greep uit het aanbod in mobiele besturingssystemen: Windows Mobile, RIM Blackberrys, Apple Iphone, Symbian toestellen,Palm, Google Android. (Lopez, Succesful Mobile Deployments Require Robust Security, 2009) Zoals u kan vaststellen zijn deze zeer uiteenlopend. Het vormt voor de IT-afdeling binnen de onderneming een hele uitdaging om die problematiek aan te pakken. Hierbij worden de problemen die mobiele applicaties met zich mee brengen buiten beschouwing gelaten. Dit wordt lager besproken.

3.3.2 Mobiele applicaties

Tegenwoordig worden applicaties ook mobiel gebruikt. Webmail is een van de vele toepassingen dewelke praktisch overal geopend kan worden indien men over een internetconnectie beschikt. Hierop zullen mobiele providers in België gewillig inspelen. Andere typen applicaties zoals mobile learning applicaties kunnen eveneens overal opgeroepen worden met behulp van mobiele toestellen. Deze applicaties verschillen in de behoefte wat beveiliging betreft. Dit zal lager aangetoond worden.

Mobile learning is samen met mobile computing een nieuwe trend. Hoe moet de onderneming mobile learning applicaties beveiligen? In de huidige samenleving wordt er steeds vaker gebruik gemaakt van laptops, netbooks (Gladstone, 2009) en dergelijke en wordt er vaker gebruik gemaakt van toegang op afstand. Mobiele technologie wordt immers steeds ambitieuzer. (Arend, et al., 2009) Daarom lijkt ook een combinatie van dit domein met de ‘cloud’ (Rubenking, 2008) niet onlogisch. De cloud is immers overal bereikbaar en dat is net wat men verlangt bij mobiel leren. Ook dit is iets dat vaker en vaker wordt gebruikt: web 2.0 is omnipresent. (Arend, et al., 2009) Denk maar aan Google Apps en Windows Live.

Doch wanneer men naar beveiliging kijkt zullen de applicaties fundamenteel verschillen. Elke applicatie kan een andere aanpak vereisen net omdat deze zo verschilt.

3.3.3 Conclusie gebruikers en applicaties worden mobiel

Mobiele apparaten zijn in opkomst. We bevinden ons immers in het 'mobile era' zoals uit figuur 5 blijkt. Deze apparaten zullen vaak worden gebruikt om cruciale bedrijfsinformatie op te roepen. Zo zullen PDA's, laptops, mobiele telefoons, netbooks in verbinding staan met het bedrijfsnetwerk en kunnen op die manier een doelwit vormen voor hackers die via deze weg proberen gegevens te ontvreemden. (Deloitte, 2006) Denk hierbij aan een verkoper die productinformatie, welke geheim is, oproept. Zulk een situatie impliceert dat zowel het toestel als de applicaties en de transmissiestroom van data een beveiliging vereisen.

3.4 Service Oriënted Architecture

3.4.1 Wat is Service Oriënted Architecture?

Service Oriented Architecture, afgekort SOA, is een nieuw concept. (Laudon & Laudon, 2006) Het wordt door de OASIS Group (2010) als volgt gedefineerd: *'A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.'* Volgens Laudon & Laudon (2006) is: ' *SOA is opgebouwd uit op zichzelf bestaande diensten die met elkaar communiceren om een werkende softwaretoepassing te vormen. Bedrijfsprocessen worden ondersteund door een reeks van deze diensten uit te voeren. Softwareontwikkelaars hergebruiken ook deze diensten in andere combinaties en zetten zo andere, nieuwe toepassingen in elkaar.'* SOA koppelt dus verschillende delen software die data uitwisselen grafisch samen en levert die als één geheel aan de gebruiker. In feite zijn het allemaal verschillende systemen die pas in een laat stadium aan elkaar worden gekoppeld en op die manier een relatieve fault tolerance en flexibilteit bieden. (Krishnan & Bhatia, 2008) . Deze integratie wordt verzorgd door een geheel van open standards

die informatie uitwisselen. (Krishnan & Bhatia, 2008) Een voorbeeld hiervan is een website waar u een vakantie kan boeken. Dit soort websites incorporeert onder andere elementen om een ticket te boeken met het vliegtuig, het hotel, de huurauto, enz. Dit zijn allemaal individuele delen die één groter geheel vormen.

3.4.2 Bedreigingen SOA en een oplossing?

De drie grootste problemen waarvoor men een oplossing moet vinden zijn credential management, authenticatie en authorisatie. (Krishnan & Bhatia, 2008) Wanneer men spreekt over credential management bedoelt men in de literatuur het management van de gebruikersnaam en het paswoord. Dit kan moeilijk zijn met allemaal verschillende applicaties die worden 'omgebouwd' tot een applicatie. Ook de authenticatie vormt op diezelfde manier een heikel punt. Hoe kan men op een betrouwbare manier zijn identeit bewijzen? Hetzelfde verhaal gaat op voor authorisatie, ook hier kan men voor een probleem staan. Het is immers niet makkelijk om bij applicaties die in wezen geen geheel vormen toch een overkoepelend geheel van credential management, authenticatie en authorisatie te bouwen. Het beheren van deze rechten is dus geen sinecure en vrij ingewikkeld voor beheerders.

De problemen die hier vanzelfsprekend optreden zijn fouten in de samenwerking van de applicaties die los van elkaar staan. Men moet als onderneming hieraan aandacht besteden zodat er geen fouten ontstaan. Zo kan een klant bijvoorbeeld een reis bestellen en als gevolg van slechte samenwerking van de geïntegreerde systemen zal een andere klant voor die reis betalen.

De oplossing kan men vinden in beter management en planning. (Oracle, 2010) Men moet vooraf goed nagedacht hebben over de applicaties alvorens iets te ondernemen.

3.4.3 Conclusie Service Oriënted Architecture

Service Oriented Architecture zorgt voor het samenbundelen van individuele applicaties, zoals hoger besproken. De problemen die hierbij ontstaan kunnen voor ernstige fouten zorgen binnen de bedrijfsvoering. De onderneming moet daarvan op de hoogte zijn en moet ze voorkomen.

3.5 Virtual computing

3.5.1 Virtual computing, wat is het?

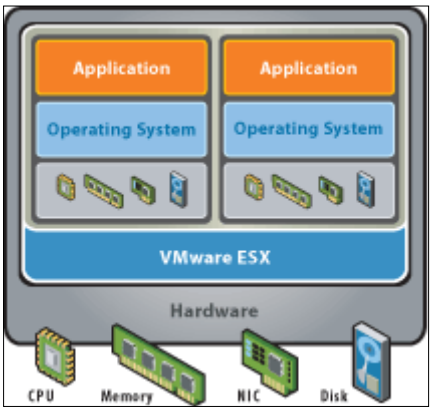
Virtual computing is een trend waarvan de ondernemingen het laatste jaar steeds vaker gebruik maken. Volgens Kim (2008): " The need for increased agility and the increasing cost and complexity of IT have driven the rapid adoption of virtualisation technologies." Volgens een survey uitgevoerd door de onderneming Tripwire maakte er in 2008 reeds 85% van de 219 ondervraagde ondernemingen reeds gebruik van virtualisatie en de overige 15% planden dit te doen. Dit toont aan dat virtual computing stilaan ingeburgerd raakt. Het zal natuurlijk ook een impact hebben op de beveiliging. Onderzoek uitgevoerd door Gartner (2008) ontdekte dat 60% van de virtuele servers minder veilig zullen zijn dan een fysieke server en dat 30% van de gevirtualiseerde servers binnen het jaar aan een beveiligingsincident zullen worden gelinkt. (Brodkin, 2008)

3.5.2 Bedreigingen virtual computing

Virtualisatie houdt nieuwe mogelijkheden in. Ondere andere de manier van hoe de onderneming haar datacenter organiseert wordt ingrijpend veranderd. Voordelen zijn dat er efficiënter gebruik kan worden gemaakt van bestaande hardware. Maar er komen ook extra problemen en beperkingen bij kijken. Welke werknemers mogen toegang hebben tot welke 'guest' en wie mag toegang tot welke 'host' hebben? Er zal nood zijn aan een goed uitgewerkte security policy die daarop een antwoord biedt.

Virtualisatie heeft naast het efficiënter gebruik van hardware nog andere voordelen. Zo kan men sneller een server opzetten en in onderhoud is het makkelijk. Maar wanneer er niet goed over wordt nagedacht zullen er des te sneller fouten worden gemaakt die resulteren in slecht beveiligde servers. (Kim, 2008) Net omdat een server met behulp van virtualisatie snel is opgezet zal het beveiligingsprobleem zich snel verspreiden door de onderneming indien men er niets aan doet. Het is aan te raden dat men nadenkt over het implementeren van de beveiliging in de onderneming en dus ook bij de gevirtualiseerde servers. Op deze manier kan men nadien problemen voorkomen.

Het is dus nodig dat men beveiliging vanaf het begin mee implementeert. (Kim, 2008) Men heeft kunnen vaststellen dat er maar al te vaak laks wordt omgesprongen bij het opzetten van een virtuele server wat de beveiliging betreft. (Brooks, 2007) Zo worden er problemen gecreëerd die vanaf het begin hadden kunnen worden voorkomen. Een voorbeeld van een probleem dat zich vaak voordoet bij virtualisatie situeert zich in de anti-virus beveiliging. (Sloan, 2009) Traditionele anti-virus beveiliging zal nood hebben aan een operating systeem, zoals Windows. Maar wanneer men systemen zal gaan virtualiseren kan het dat dit niet voor handen is. Bijvoorbeeld Vmware ESX-server (VMware, 2009) is een virtualisatie software die op 'bare metal', rechtstreeks op de hardware, kan worden geïnstalleerd. U kan dit vaststellen in de volgende figuur.



Figuur 6: Vmware ESX server. (Vmware, 2010)

U ziet het blauwe deel, dit omvat de zogenaamde ESX server (het eigenlijke OS). Er wordt slechts gebruik gemaakt van een OS dat op 'bare metal' gefundeerd is. De hosts zitten hierboven. Wanneer de ESX geviseerd wordt en 'down' gaat, kan dit de applicaties en guests die hierboven zitten in de problemen brengen.

Wat gebeurt er nu indien niet de guests, maar de host wordt aangevallen door een virus. Voorheen was hier nog niet meteen aan gedacht en was er geen oplossing voor handen. (Sloan, 2009) Men is ondertussen wel aan het werk om hier een oplossing voor aan te bieden, in de vorm van vSphere. (VMware, 2009)

3.5.3 Conclusie Virtual computing

Vandaag de dag wordt men niet langer beperkt om op elke fysieke server of desktop slechts één OS te installeren. Virtualisatie biedt mogelijkheden om meer dan één OS te installeren. Maar het is oppassen geblazen. Net omdat het makkelijker is een nieuwe server te installeren, zullen makkelijker fouten worden gemaakt. (Kim, 2008) Een andere kwestie is: wat gebeurt er wanneer de host wordt aangevallen? Meestal beschermt men enkel de guests. Ook voor dit probleem moet men een oplossing vinden.

3.6 Cloud computing

3.6.1 Wat is cloud computing?

Cloud computing is een relatief nieuw paradigma. Wanneer er wordt gesproken van de cloud bedoelt men meestal het internet. (Joint, Baker, & Eccles, 2009) Dit is een stelling vanuit het standpunt van de consument.

Traditioneel worden programma's (Microsoft Word) en os (Microsoft Windows) lokaal geïnstalleerd op de werkstations en data (documenten) wordt lokaal opgeslagen. Indien er iets gedeeld moest worden, dan wordt dat gedaan via een centrale lokale server, die toegankelijk is voor alle gebruikers. (Joint, Baker, & Eccles, 2009) Door gebruik te maken van de cloud worden lokale servers geëlimineerd. Men maakt nu gebruik van de cloud om de samenwerking te bevorderen en het delen van gegevens te organiseren. Er wordt gebruik gemaakt van centrale servers gemanaged door derden in plaats van lokale privé servers. (Joint, Baker, & Eccles, 2009) Dell, Google, Microsoft,... zijn allemaal bedrijven die er proberen gebruik van te maken in hun business strategie.

Zoals u kan vaststellen is de cloud een overkoepelende evolutie van SaaS. De cloud biedt een aantal services aan: Infrastructure as a service, Database as a service, Software as a service, Platform as a service. (Motahari-Nezad, Stephenson, & Singhal, 2009) Hierover lager meer.

3.6.2 Toepassingen en voordelen van cloud computing?

Cloudcomputing heeft diverse toepassingen. Zo kan het bijvoorbeeld worden gebruikt in de biomedische wereld om informatie te delen. (Rosenthal, Mork, Li, Stanford, Koester, & Reynolds, 2008) Ze kunnen zogenaamde 'specialised grids' gaan vervangen en ook het bezit en beheer van eigen servers in de onderneming. (Rosenthal, Mork, Li, Stanford, Koester, & Reynolds, 2008) Men kan voor toepassingen die veel 'processing power' vragen eigen servers gebruiken, terwijl voor dat voor toepassingen die dat niet eisen er kan worden uitgeweken naar servers in de cloud. Zo hoeft er minder te worden geïnvesteerd in eigen datacentra. De eigen datacentra kosten vaak erg veel. Denk maar aan koeling, ruimte, stroom, low-level system administration en onderhandelingen over firewall en softwareconfiguraties. (Rosenthal, Mork, Li, Stanford, Koester, & Reynolds, 2008) Analyse van foto's, data mining, gene sequencing, enz. zijn toepassingen waarvoor er lokaal wordt geïnvesteerd. (hoge processing power) Men zal zogenaamde 'grids' aanleggen voor het verwerken van die data. Voor onderlinge samenwerking of minder resource intensieve toepassingen kan de cloud worden aangesproken. Dit resulteert in besparing van kosten. Men spreekt in dit geval van 'cloud-sourcing', men gaat in feite aan out-sourcing doen van bepaalde onderdelen van de IT infrastructuur of de hele infrastructuur. (Joint, Baker, & Eccles, 2009) Het grootste voordeel dat men uit de cloud haalt is kostenbesparing. (Mansfield-Devine S. , 2008)

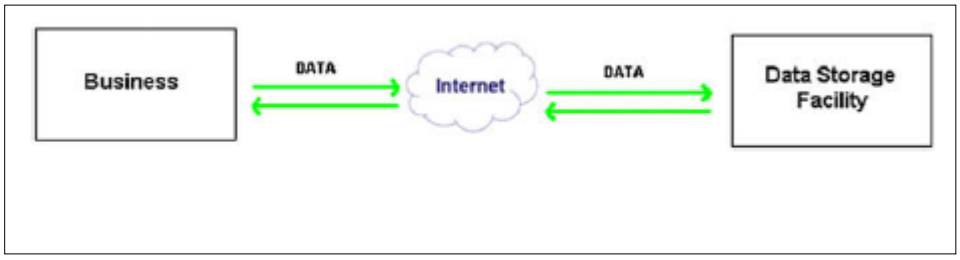
Cloud Computing is nieuwe trend die voor drastische wijzgingen zal zorgen. Net als praktisch alle trends brengt ook deze trend nieuwe beveiligingsproblemen met zich mee volgens Dan Kaminsky. (2009, in De Rooij, 2009) Zo zal de CIO, de Chief Information Officer, nooit weten op welke locatie de gegevens zijn opgeslagen. Dit gebeurt immers in de cloud, er is geen sprake van een bepaalde plaats. Indien er kwaad opzet wordt gepleegd kan men zich aanmelden als klant en dan in de cloud stukjes aanvallende software achterlaten die negatieve gevolgen heeft voor de cloud en dus ook de gegevens die erop opgeslagen zijn.

Men kan spreken van twee soorten clouds. De privé cloud en de publieke cloud. (Buyya et al, 2008) Met de privé cloud wordt een apart afgeschermd deel bedoeld enkel open voor de

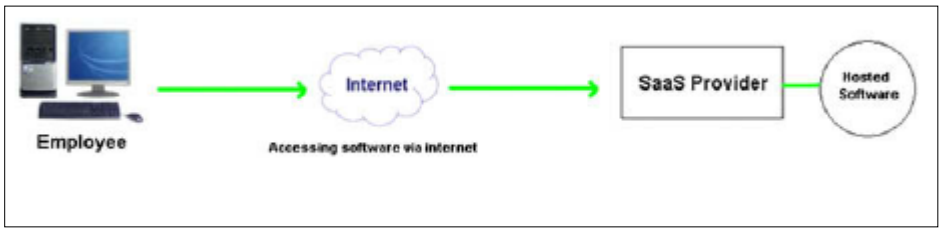
onderneming en eventueel leveranciers, terwijl met de publieke cloud het naar het internet opengestelde deel wordt bedoeld. (Joint, Baker, & Eccles, 2009) Vanzelfsprekend is een privé cloud voor een CIO overzichtelijker en veiliger. Maar ook deze vorm brengt extra voorzichtigheid met zich mee. Overzicht behouden op de assets wordt bemoeilijkt door de vluchtige aard van de cloud en wat gebeurd er indien er een probleem is? Bestaan er alternatieven? Indien er zich een probleem voordoet, zal het leven in de onderneming haar gewone gang kunnen gaan?

3.6.3 Typen cloud sourcing

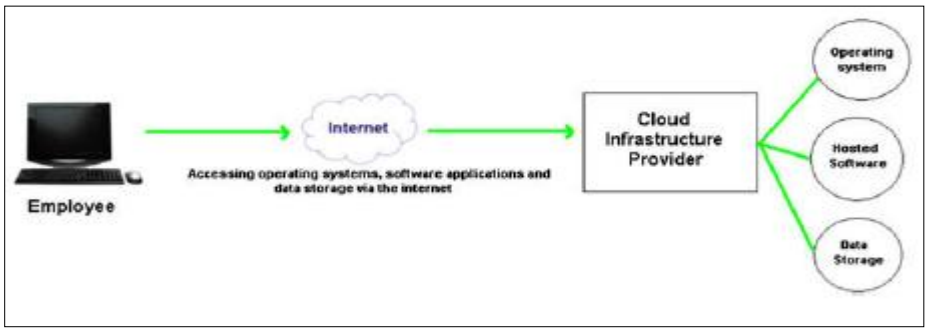
Voor bedrijven is er sprake van drie hoofdvormen van cloud sourcing. Deze zijn 'cloud-storage', 'cloud-service', 'cloud-infrastructur/platform', zoals eerder al even vermeld. Men zal dus respectievelijk als onderneming gebruik maken van opslag, een bepaalde service (SaaS) of van een geheel platform in de cloud. (Joint, Baker, & Eccles, 2009) U vindt de drie verschillende soorten weergegeven in de volgende figuren.



Figuur 7: Cloud-storage, opslagruimte. (Joint, Baker, & Eccles, 2009)



Figuur 8: Cloud-service, een applicatie (Joint, Baker, & Eccles, 2009)



Figuur 9: Cloud-infrastructure/platform, een gehele infrastructuur (Joint, Baker, & Eccles, 2009)

Voor de consumentenmarkt krijgt de betekenis 'cloud' een andere invulling. De cloud zal aan de modale consument niet meteen hardware en software aanbieden tegen een prijs voor het leveren van een bepaalde dienst, nog niet. Maar wel kan u denken aan webservices zoals Microsoft MSN, Gmail of Google search. (Rosenthal, Mork, Li, Stanford, Koester, & Reynolds, 2008) Dit is dus eerder beperkt van aard in vergelijking met de bedrijfswereld.

3.6.4 Gevaren in de cloud?

Nu worden de grootste gevaren besproken van de cloud, in de context van information security. De gevaren van de cloud zijn volgens Brodkin (2008) te situeren in de volgende 7 categorien die hieronder kort worden besproken.

3.6.4.1 Priviliged user access

Het opslaan van gegevens buiten de onderneming, in de cloud, brengt sowieso problemen met zich mee. Indien de data cruciaal is voor de onderneming en indien er grote schade kan worden geleden indien er iets mee gebeurt, dient de onderneming toch meer inzicht te hebben in wie de data beheert bij de service aanbieder. Inzage in wie er wordt aangenomen en hoe dit gebeurt zijn noodzakelijk. Hebben enkel de juiste personen toegang?

3.6.4.2 Regulatory compliance

Zijn de service aanbieders wel voldoende op de hoogte van algemene regelgevingen. Een van de maatregelen die kunnen worden getroffen zijn het organiseren van audits om te controleren indien men wel volgens 'regels' werkt. Met andere woorden: werkt de service aanbieder wel volgens de standaarden?

3.6.4.3 Data location

Omdat de data wordt opgeslagen in de cloud weet men als klant niet waar de data zich bevindt. Men moet als klant aan de service aanbieder vragen indien alle privacy wetten bijvoorbeeld wel worden gerespecteerd zodat men hiermee in orde is.

3.6.4.4 Data segregation

Wat wordt er met opgeslagen data gedaan? Hoe zal de serviceaanbieder zijn hardware ontdubbelen. Wordt dit wel gedaan? Hoe wordt de data opgeslagen, is deze voldoende beveiligd door de service aanbieder? Men moet, volgens Brodkin (2008), erop toezien dat de service aanbieder de juiste encryptie algoritmes gebruikt opdat de data voldoende wordt gescheiden van mekaar.

3.6.4.5 Recovery

Men moet opletten bij het selecteren van een service provider. Indien men een provider overweegt waarbij de data wordt opgeslagen op slechts één fysieke plaats, dan kan een ramp voor compleet verlies van gegevens zorgen. Dit zou een rampscenario zijn voor de onderneming. De aanbieder moet minstens op twee verschillende locaties de data opslaan zodat een aardbeving bijvoorbeeld niet voor systeemuitval kan zorgen.

3.6.4.6 Investigative support

Het loggen van wat er gebeurt met gegevens en applicaties in de datacentra kan een probleem zijn. Dat is een deel dat door de klant volledig uit handen wordt gegeven. Hoe moet u als klant daarop inspelen? Hoe kan men als klant onderzoeken of er is ingebroken op de systemen als men geen controle heeft over de systemen of als men niet de exacte locatie weet van waar de data is opgeslagen. (dit laatste is inherent aan de cloud)

3.6.4.7 Long-term viability

Hoe staat het met de service aanbieder? Blijft deze voor altijd voortbestaan? En indien dit niet het geval is, wat gebeurt er dan met de data? Men moet als klant hierop voorbereid zijn, volgens Brodkin.(2008)

3.6.5 The coming cloud crisis

Trend Micro doet de volgende vaststelling die men als onderneming in het achterhoofd moet houden, in verband met de cloud. Trend Micro spreekt van de 'coming cloud crisis'. Hoe is dit mogelijk? Nog niet zo lang geleden, en dit is nu nog het geval, had microsoft een monopolie op de ICT markt. Dit werd erkend door schrijvers van malicious code. Daarom is Microsoft Windows kwetsbaarder voor malicious code dan bijvoorbeeld Apple OS. Zelfs de veiligdheid van Mac OS X is relatief. (Mansfield-Devine S. , 2008) Trend Micro (2010) zegt het volgende:*' The monoculture represented by Microsoft Windows has always been attractive to malware writers and criminals alike. It is important to note that much of the current cloud innovation is also taking place in few large monoculture environments such as Google, Windows Azure and Amazon EC, and these monocultures too may well invite attack.'* Dit betekent dat hetzelfde kan gebeuren bij de cloud. Als de huidige evolutie zich voltrekt zullen kwaadwillenden de monopolies van Google, Amazon en Microsoft erkennen en zullen ze voor deze cloud malware gaan schrijven waardoor deze in wezen onveiliger worden. Men moet zich als onderneming de vraag stellen of deze evolutie op termijn dan nog wel een goed idee is?

3.6.6 Conclusie cloud computing

Hoewel het verplaatsen van weinig intensieve taken naar de cloud zijn voordelen heeft, zal het ook zijn nadelen hebben. Men moet als onderneming daarvan op de hoogte zijn. Is de applicatie die wordt verhuisd naar de de cloud cruciaal voor de onderneming? Zoja, dan moet men afspraken maken met de service aanbieder zodat eerder aangehaalde gevaren niet de kans krijgen om voor te komen.

3.7 Conclusie trends

Deze ingrijpende trends zullen het ICT-landschap voor altijd wijzigen. (Arend, et al., 2009). Dit zal een impact hebben op de manier waarop zaken worden gedaan in de onderneming. Ondernemingen zullen hierbij rekening gaan moeten houden, willen of niet. Indien ze daarbij geen rekening houden zullen ze hopeloos achterop raken en dit kan negatieve implicaties hebben het verdere bestaan van de onderneming.

Voor bedrijven zullen mobiele toestellen naar mijn inzicht voor één van de grootste problemen zorgen. Volgens een survey, uitgevoerd door Bluecoat in 2010, vormen mobiele toestellen steeds vaker een doelwit. Omwille van de gevaren die inherent zijn aan mobiele toestellen en omwille van dat er momenteel meer mobiele toestellen over de toonbank gaan dan desktop computers, zullen cyber criminelen hierop ook vaker inspelen. (Bluecoat, 2010) Ze zullen steeds vaker specifiekere aanvallen gaan uitdokteren om zwakheden van de mobiele toestelen uit te buiten. Net daarom is dit een interessant topic om uit te diepen.

4 IT Security Policy

De informatie en de technologie dewelke de informatie ondersteunt zijn voor vele ondernemingen het kostbaarste maar ook het minst begrepen asset in de onderneming. (IT Governance Institute, 2007) Zoals hoger reeds aangegeven zijn er een groot aantal nieuwe bedreigingen in de turbulente omgeving waarin de ondernemingen zich vandaag de dag bevinden. Tevens is het in het kader van het governance concept cruciaal dat de onderneming voldoende aandacht besteedt aan de beveiliging van haar informatiesystemen. (Mercken, 2009) De onderneming moet met deze doelen in het achtrhoofd een security policy uitwerken.

Nieuwe trends zoals mobiele toestellen, meer bepaald pda's of mobiele telefoons, zullen een impact hebben op de security policy. De security policy moet aangepast worden om de bedreigingen ten gevolge van de evoluties in de ICT wereld. Zoniet kan dit gevolgen hebben voor de onderneming, haar aandeelhouders en andere belanghebbenden. Toch wordt er in ondernemingen vaak nog te weinig aandacht besteed aan security policy. Uit een survey werd vastgesteld door Goodintelligence (2009) dat ondernemingen vaak geen security policy hadden voor de mobiele telefoons binnen de onderneming: *"Just under half of the respondents do not have a specific documented security policy for mobile phones."* Meer bepaald 46% van de ondervraagde ondernemingen had geen specifieke policy voor mobiele toestellen. (Goode Intelligence, 2009) Dit is een groot probleem. Dit probleem wordt van nader bekeken in dit hoofdstuk.

4.1 Wat is een IT security policy?

4.1.1 Definiëring en functie

Een information technology security policy wordt als volgt gedefineerd:*'Een geheel van regels in de organisatie die dienen om de informatie binnen de onderneming veilig te stellen.'* (Whitman & Mattord, 2009)De IT security policy kan helpen de integriteit, de beschikbaarheid en de vertrouwelijkheid van de data binnen een informatiesysteem te garanderen en dit geldt tevens ook voor de gegevens die worden verzonden tussen twee informatiesystemen (Straub, 1990) Volgens

Wood (1995) hebben policies de volgende functie : "*Policies act as clear statements of management intent and demonstrate that employees should pay attention to information security"* In dit geval gaat het over zogenaamde high level security policies.

Alvorens te gaan bepalen hoe een information technology security policy eruit ziet, dit wordt gedaan in het laatste hoofdstuk, is het van belang dat er eerst moet bestudeerd worden wat een een dergelijke high level policy precies is en waar deze zich bevindt binnen het hele security gebeuren. Een voorbeeld van een dergelijke security policy is de enterprise information security policy, maar hierover later meer.

Een high level policy, niet te verwarren met een IT security policy, is eigenlijk een algemene regel die in de onderneming wordt aangenomen, deze regel limiteert iets. (Simon, 1957) In het kader van informatiesystemen wordt een policy gebruikt om het gedrag van gebruikers van informatiesystemen te 'limiteren' tot acceptabel gedrag, gedrag dat de bedrijfsvoering of die van de aandeelheelhouders of andere belanghebbenden niet schaadt. Volgens SearchMobileComputing.com (2008) is een security policy het volgende: *'In general, a security policy defines what information is to be treated as sensitive (and therefore protected), who should have access to this information and under what conditions, and—very importantly—what to do when security is compromised (or even suspected of being compromised). From a physical security perspective, it should define who may have access to IT-specific areas of a given installation or building and how these areas are to be secured.'* Op basis van deze vaststellingen kan men regels opstellen, dewelke de security policy vormen. Volgens von Solms en von Solms (2004) bieden policies eigenlijk de 'blueprint', een blauwdruk net als bij de bouw van een huis, voor het security programma binnen de onderneming. Ze creëren een platform voor het implementeren van veilige practices binnen de onderneming. (von Solms & von Solms, 2004) Wanneer men specifieker gaat kijken, per systeem of per probleem, dan kan men pas spreken van een IT security policy.

4.1.2 Soorten policies

Er bestaan verschillende types policies, zoals al eerder aangehaald. Naargelang het type van policy verschilt het doel. De belangrijkste security policy is de **enterprise information security policy**

(EISP), dat is diegene die policy wordt genoemd in het inleidende onderdeel. Volgens Whitman en Mattord (2009): *"The EISP is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope and the tone for all security efforts."* Dit is de policy die op het hoogste level in de onderneming wordt opgesteld in samenwerking met het hogere management. In deze policy staan alle richtlijnen die nodig zijn om de 'blueprint' op te stellen. Enkel als er een wijziging is in de missie moet deze policy worden gewijzigd. Volgens Whitman en Mattord (2009) zorgt deze policy voor het ontwikkelen, implementeren en managen van het security programma binnen de onderneming.

Er bestaat ook een **issue specific security policy (ISSP)**. De hoger vernoemde policy moet worden vertaald in een lager level policy. Deze lager level policy is nuttig omdat hij bepaalde specifieke situaties adresseert. Bijvoorbeeld het gebruik van internet kan gedefinieerd worden in een issue specific security policy. Deze is het type policy die wordt ontwikkeld in het laatste hoofdstuk.

System specific policies zijn van een ander type dan een issue specific policy, deze is specifieker van aard. Een system specific policy verschilt van een issue specific policy zo dat hij definieert hoe een bepaald apparaat of toestel moet onderhouden worden of geconfigureerd. (Whitman & Mattord, 2009) Volgens Withman en Mattord (2009) kunnen system specific policies nog eens worden opgedeeld in twee categorieën: diegene die managerial guidance geven en die betrekking hebben op technische specificaties.

4.2 IT Security policy en internationale standaarden

De eerder aangehaalde regels moeten worden opgebouwd. Maar hoe begint de onderneming daar best aan? Er zijn een aantal methodes daartoe beschikbaar ter implementatie van een policy. Maar zullen deze tools volstaan om de evoluties op te vangen zoals mobiele toestellen of mobiele applicaties? Lekken in zulke toestellen of applicaties kunnen een probleem vormen voor de onderneming. Hoe zullen deze internationale standaarden deze problemen opvangen?

Ik zal nu overgaan tot een korte bespreking van de modellen die voor handen zijn. Achtereenvolgens zal COBIT, GASSP, ISO (27000 series) aan bod komen. We zullen bij deze standaarden gaan nagaan welke aandacht ze besteden aan security policy en hoe zij evoluties opvangen. Dit is belangrijk in het kader van de eerder besproken trends.

4.2.1 Control Objectives for Information and related Technology

4.2.1.1 Wat is Cobit?

Cobit is een praktische handleiding die kan worden gebruikt om beveiliging in de onderneming te implementeren. Cobit zal het volgende doen:

'Cobit provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts.They are strongly focused more on control, less on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.'

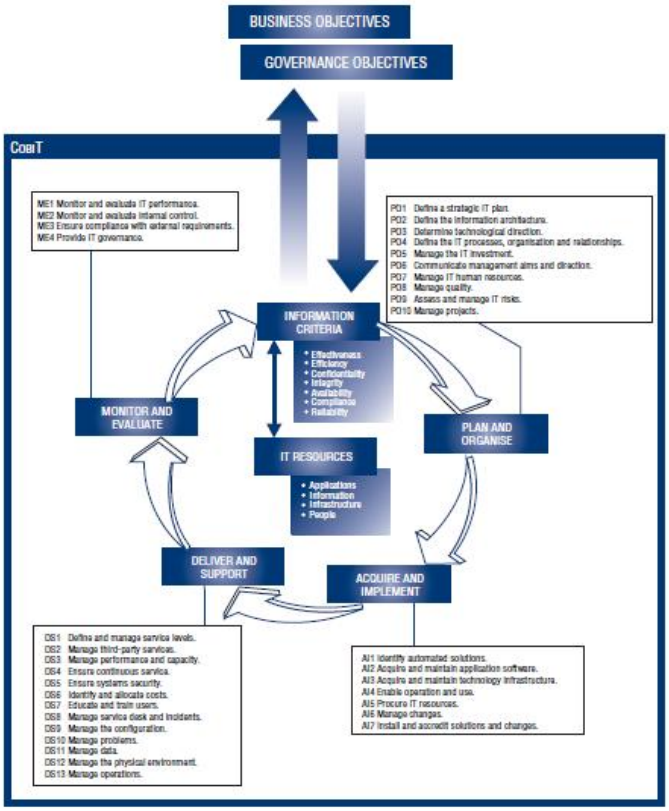
De richtlijn vormt een geheel van raadgevingen die zijn voortgekomen uit consensus van een aantal experts. Ze focussen op de controle door de manager, in mindere mate op het uitvoerende aspect. Ze bieden een houvast aan de managers zodat ze kunnen bepalen wanneer er iets misloopt.

Cobit is gebaseerd op het concept IT governance. Er wordt gefocust op een vijftal sleutelgebieden: strategic alignment, value delivery, resource management, risk management en performance measurement.

Het basisprincipe van de van het Cobit framework is: *'To provide the information that the enterprise requires to achieve by its objectives, the enterprise needs to invest in and manage and control IT resources using an structured set of processes to provide the services that deliver the required enterprise information. '*

Uit het basisprincipe kan worden geconcludeerd dat het cruciaal voor de onderneming is dat zij weet waarmee zij bezig is. De perfomance metrics spelen hierin een cruciale rol. Hierover later meer.

In de onderstaande figuur vindt u een overzicht van het Cobit framework. Hierbij valt op dat het een constante cyclus is die nooit stopt. Achtereenvolgens zullen de information criteria bepaald worden binnen de onderneming, men stelt een planning op en organiseert in functie van de informatiecriteria, men implementeert het systeem en levert daarna support op het systeem en als laatste stap zal men constant een oogje in het zeil houden en evualeren. Op basis van deze laatste verzamelde gegevens zal men verbeteringen aanbrengen.



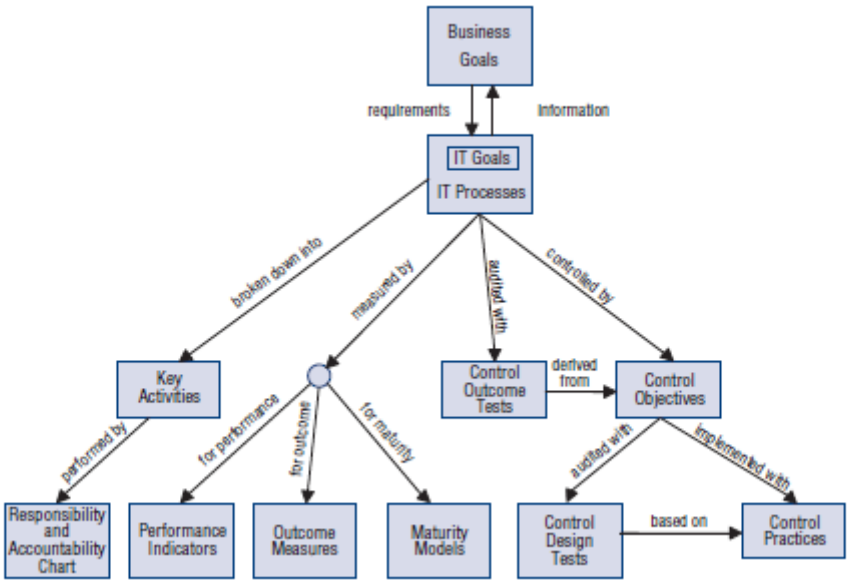
Figuur 10: Algemene Cobit framework (IT Governance Institute, 2007)

Cobit gebruikt dat framework als een kapstok om zijn verschillende tools aan op te hangen. Ook deze zijn in de figuur weergegeven. Opvallend is ook hoe de doelen, een zeer cruciale rol spelen in het bepalen van de informatie criteria.

4.2.1.2 Voordelen

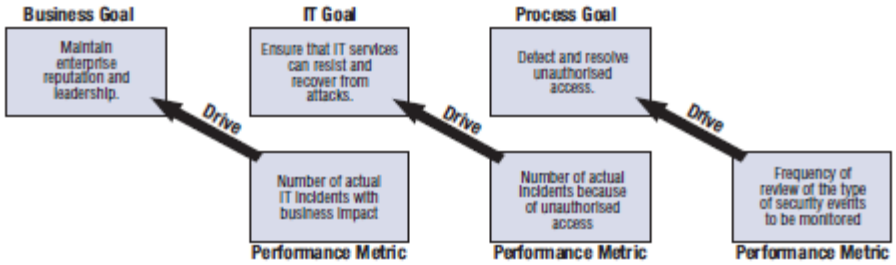
Een van de grote voordelen van Cobit is dat dit framework een end-to-end view aanbiedt van IT. Men kan met behulp van Cobit plannen, bouwen, het in gebruik nemen en het geheel in het oog houden. (IT Governance Institute, 2007) Cobit maakt daartoe gebruik van een groot aantal componenten. Deze componenten zijn aan elkaar gerelateerd en zullen interageren. Voorbeelden van zulke componenten zijn RACI-charts, Maturity models,… Hier kan u het praktische concept ook uit afleiden.

Een ander sterk punt bij COBIT is de aansluiting bij de ondernemingsdoelstelling zoals blijkt uit figuur 8. Bovenaan de piramide worden de business goals geplaatst. Deze vormen het startpunt.



Figuur 11: Interrelationships of Cobit Components (IT Governance Institute, 2007)

Men zal van de onderneming haar doelen voor de IT afdeling afleiden en de processen eveneens daarop baseren. Daarop baseert men de perfomance indicators, outcome measures, maturity models, … Perfomance metrics hebben een sleutelrol in het vaststellen hoe goed de onderneming het doet. Uit volgende figuur kan u afleiden waarom dit zo is.



Figuur 12: Perfomance drivers (IT Governance Institute, 2007)

Elke perfomance metric zorgt voor het 'driven' naar een doel, goal. Met behulp daarvan kan men specifieker naar een doel toewerken en weet men precies wanneer een doel al dan niet bereikt is.

Een vaak terugkomend concept binnen Cobit zijn de maturitymodels. Aan de hand van de maturity models kan de onderneming gaan bepalen in welk stadium zij zit en hoe ze naar het volgende stadium kan werken. In het kader van dit hoofdstuk is het interessant kort de verschillende stadia aan te halen die Cobit definieert voor de 'policies, plans and procedures'. U vindt de verschillende stadia in onderstaande tabel.

Tabel 2: Maturity stages policies, plans and procedures (IT Governance Institute, 2007)

Fase	Policies, plans and procedures
Fase 0	Non-extistent
Fase 1	Initial/ad Hoc
Fase 2	Repeatable but intuitive
Fase 3	Defined
Fase 4	Managed and Measurable
Fase 5	Optimised

4.2.1.3 Conclusie Cobit

Cobit geeft een framework dat vooral aandacht schenkt aan controle en hoe men metingen kan implementeren om een houvast te bieden wanneer zaken fout lopen. Aan de hand daarvan kan men een aantal management scorecards ontwikkelingen om te detecteren wanneer het misloopt. Met andere woorden kan worden geconcludeerd dat COBIT zeer praktisch georiënteerd is.

Dit model biedt echter geen specifieke houvast die aandacht biedt aan mobiele toestellen. Cobit zal dus geen specifieke aandacht schenken hoe men als onderneming oplossingen kan bieden voor nieuwe bedreigingen zoals die van mobiele toestellen. Zij zal wel voorzien in een continue high level beschrijving van een cyclus die dergelijke evoluties opvangt.

Aan de hand van Cobit kan de onderneming de risico's vaststellen en dus ook ervoor zorgen dat zij zichzelf ervan vrijwaart. In het kader van mobiele toestellen en de beveiligingsproblemen die deze toestellen met zich meebrengen kan de onderneming aan de hand van dit framework een afdoende manier van beveiliging gaan uitdokteren. Hoewel Cobit een houvast biedt zal het niet in de details specifiëren wat er zal moeten gebeuren. Cobit is high level van karakter en zal dus niet in detail treden.

4.2.2 Generally Accepted System Security Principles

4.2.2.1 Wat is Gassp?

Gassp, Generally Accepted System Security Principles, is een geheel van algemeen aanvaarde principes. De bijdrage van Gassp tot een security policy is minimaal. Er wordt selchts een uitwerking gegeven van een security policy met behulp van een voorbeeld. Volgens Gassp is het van belang dat de informatie binnen de organisatie wordt beschermd, en dit moet consistent zijn met het belang van de informatie en de mate waarin deze informatie risico loopt. Gassp stelt vast dat in deze optiek sommige informatie overbeschermd is en dat sommige informatie te weinig beschermd: *'To assure that information assets are effectively and uniformly secured consistent with their value and associated risk factors, management must clearly articulate its security strategy*

and associated expectations. In the absence of this clarity, some resources will be undersecured that is, ineffective; other resources will be oversecured — that is, inefficient.'

Gassp zal, eveneens als Cobit, aangeven dat het van belang is dat de policies een reflectie geven van hoe de onderneming haar doelen bereikt. De policy zou de missie van de onderneming moeten reflecteren. Meer nog, volgens Gassp moet de policy ook de confidentialiteit, beschikbaarheid en integriteit van de gegevens moeten reflecteren tegenover de relevante partijen. Dit geldt ook voor derden.

Men spreekt binnen Gassp ook van een hiërachie van policies. Zonder deze hiërarchie zou de onderneming er niet in slagen de gegevens binnen de onderneming te beveiligen. Sommige informatie moet immers meer beveiligd worden dan andere informatie. Tevens zal de hiërachie voor diegene die enig belang hebben bij de informatie een duidelijke leidraad geven zodat de gegevens effectief en effciënt beveiligd zijn.

4.2.2.2 Principes

Gassp is opgebouwd rond een aantal principes. Deze principes zorgen ervoor dat drie cruciale 'eigenschappen' van informatie (vertrouwelijkheid, beschikbaarheid en integriteit) worden verzorgd. In de Gassp richtlijn worden deze verschillende principes achtereenvolgens besproken. Enkele voorbeelden zijn: accountability, awareness,… volgens de Gassp (2010).

Gassp zal wel geen specifieke aanpak voorzien voor mobiele toestellen. Dit kan men duidelijk afleiden uit het doel*: 'The GASSP Committee seeks the creation, maintenance, monitoring of, and adherence to the GASSP for information security in the broadest context, on an international level, unifying and expanding upon existing authoritative sources.'* Gassp is bedoeld om elk security probleem aan te pakken, maar ze zal daartoe geen gedetailleerde informatie geven, in de richtlijn althans omdat deze te snel evolueren en constant aangepast moeten worden.

Doch zal Gassp ook rekening houden met nieuwe evoluties. Het principe information risk management houdt in feite rekening met nieuwe bedreigingen. Zo zal Gassp ervoor zorgen dat nieuwe risico's worden aangepakt en dat men hun risico inschat.

4.2.2.3 Conclusie

Gassp geeft een algemene weergave van informatie systeem beveiliging. Deze uiteenzetting is high level: ze treedt niet in detail. In vergelijking met Cobit zal ze geen praktische tools aanbieden zoals een RACI model, maar ze zal wel voorbeelden aanhalen ter verduidelijking van het nut van bepaalde onderdelen.

4.2.3 International Organisation for standardization: ISO 27002

4.2.3.1 Wat is ISO 27002?

De ISO 27000 series is in feite de voormalige BS7799 standaard. (Whitman & Mattord, 2009)In het jaar 2000 is deze standaard overgegaan van een Britse tot een algemene internationale standaard, de zogenaamde ISO standaard. Zo zal het door de jaren verder gaan evolueren. Van deze standaarden is ISO 270002 van belang voor het werk. ISO 27002 is een model dat is opgebouwd rond de PDCA cyclus. Deze Plan-Do-Check-Act cyclus is een cyclus welke evoluties en veranderingen kan opvangen. In vergelijking met Gassp is dit model een cyclus, net zoals het model van COBIT. Deze standaard is minder praktisch dan de COBIT standaard. Hoewel, een versie van de standaard uit 2003 de standaard weergeeft in de vorm van een checklist. Men kan daarop aangeven wat de status is en in welke mate de onderneming 'compliant' is met de standaard. Deze standaard kan dus ook in een praktischere vorm verkregen worden.

Er wordt een volledig hoofdstuk gewijd aan Security Policy. Daaruit kan u het belang afleiden van de security policy binnen de standaard.

4.2.3.2 Conclusie ISO 27002

ISO 270002 is een standaard die evoulties kan opvangen met behulp van PDCA-cyclus. Er wordt ook meer aandacht besteed aan de security policy in vergelijking met de Gassp standaard. De ISO 270002 standaard is in mindere mate praktisch. COBIT stelt een aantal tools ter beschikking die daadwerkelijk gebruikt kunnen worden.

4.3 IT security policy gerelateerd aan mobile computing

4.3.1 Het belang van een issue specific security policy

Zoals kan worden vastgesteld zullen de meeste internationale standaarden gaan werken op high level. Sommige standaarden zullen dieper ingaan op security policy, anderen beschouwen het slechts als een kleiner onderdeel. In dit deel zal er speciefiek worden gekeken hoe in enkele papers de security policy wordt aangepakt als men spreekt over mobiele toestellen.

De onderneming zal best, conform de standaarden die hierboven besproken zijn, een aantal security policies opstellen. Deze zullen algemeen van aard zijn wat betreft het onderscheid tussen mobiele en niet-mobiele toestellen, met andere woorden dit onderscheid is zeer beperkt. Het is aan te raden dat de onderneming een aparte policy opstelt voor mobiele toestellen. Een voorbeeld van zo'n policy kan u in bijlage 1 vinden. Deze policy, in bijlage 1, behandelt het gebruik van mobiele toestellen.

Het is dus nuttig dat de onderneming specifiek per toestel gaat kijken wat de beste manier van beveiliging is. Een high level security policy biedt geen antwoorden op toestelspecifieke bedreigingen. Afhankelijk van het type probleem dat men wil addresseren stelt men een ander type policy op. Zoals eerder reeds aangehaald zijn er een drietal typen polcies.

In tegenstelling tot niet mobiele toestellen, zoals de gewone desktop computer voor de werknemer, zullen mobiele toestellen uiteenlopend zijn van aard. Vaak worden deze toestellen zelfs

aangeschaft door de werknemer zelf en zal verlies of diefstal van de toestellen niet meteen gemeld worden. Dit kan voor problemen zorgen. Daarom moet de onderneming zoals KBC (zie lager) eigen toestellen aan werknemers geven met een bijpassende issue specific security policy. KBC heeft gekozen voor toestellen van RIM, Research In Motion. Dit zijn de zogenaamde Blackberry toestellen. Deze toestellen worden vaak in professionele omgeving gebruikt. Omdat deze toestellen zeer uitgebreid te beveiligen zijn, heb ik besloten in deze thesis mij uitsluitend te richten op deze toestellen.

4.3.2 Blackberry security policy

Wanneer de onderneming gebruik maakt van Blackberry applicaties, dan kan met behulp van Blackberry Enterprise Server een policy worden toegepast. (Research In Motion, 2010) Met behulp van deze software kan de onderneming haar IT afdeling specifiek voor verschillende groepen werknemers in de onderneming een aparte policy voorzien. Volgens de Blackberry Policy Reference Guide 4.1 (2009) kan er een groot aantal regels worden gedefinieerd. Deze regels zijn enorm uiteenlopend en uitgebreid. Hierop wordt later dieper ingegaan, wanneer er een oplossing wordt aangereikt.

4.4 Conclusie IT security policy

We kunnen concluderen uit dit hoofdstuk dat een algemene, high level, security policy onontbeerlijk is. De standaarden geven niet meteen, toch niet specifiek, weer hoe bepaalde evoluties moeten opgevangen worden. Maar een standaard zoals de COBIT richtlijn geeft wel een geheel van hulpmiddelen om evoluties op te vangen.

Men kon ook vaststellen dat COBIT praktischer is, daar waar andere standaarden eerder theoretisch zijn van aard. Het is nu het doel te gaan zoeken hoe een issue specific security policy eruit zou zien voor het probleem van mobile learning in combinatie met een smartphone.

5 Beveiliging mobile computing

5.1 Inleiding mobile computing

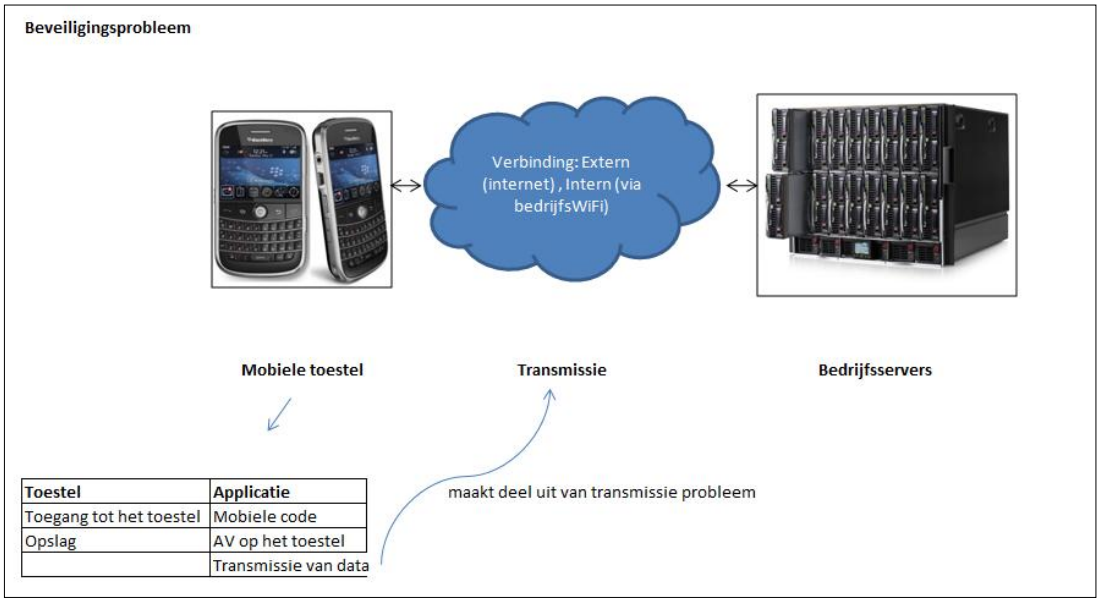
In 2001 werd in een onderzoek door the UK Home Office vastgesteld dat mobiele telefoons en PDA's vaak werden gestolen, men raamt het grosso modo op een 700 000 toestellen. (Harrington & Mayhew, Home office research study 235: mobile phone theft, 2001) Dit is een aanzienlijk aantal en vermits er meer en meer kritieke data op dat type toestellen wordt opgeslagen is het van belang mobiele apparaten te beveiligen en zeker ook de mobiele toepassingen die hierop worden gebruikt. Zo wordt er volgens Allen(2005) ongeveer een 80% van de dagelijks gewijzigde data en kritieke data opgeslagen op mobiele toestellen, hierbij horen ook notebooks. De algemene vaststelling is dat mobiele apparaten in opmars zijn en dit resulteert in beveiligingsproblemen die moeten worden aangepakt.

Mobiele apparaten zijn door hun 'natuur' kwetsbaar voor bedreigingen zoals diefstal of het toevallig kwijtspelen. Ze zijn wat beveiliging betreft niet matuur. (Botha, Furnell, & Clarke, 2009) Er wordt ook gebruik gemaakt van een steeds groter wordend aantal dat gecombineerd wordt met netwerktransfers. E-mail, web browsing, spread sheets, tekstverwerkers en instant messaging vormen geen uitzondering. Ook informatie zoals adressen van klanten, leveranciers of agenda's van bepaalde vergaderingen worden vaak opgeslagen op mobiele apparaten. (Botha, Furnell, & Clarke, 2009)

In dit hoofdstuk worden de bedreigingen verder uitgediept met betrekking tot mobiele apparaten, meer specifiek pda's en smartphones. In hoofdstuk 7 zal u een implementatie gaan vinden die een antwoord biedt op deze bedreigingen die zo meteen worden beschreven. Tevens wordt er een beschrijving gegeven van oplossingen, conceptueel, van de problemen die in dit hoofdstuk zullen worden besproken.

5.2 Overzicht bedreigingen mobile computing

In dit hoofdstuk zullen de bedreigingen worden besproken waaraan een mobiel toestel zoals een smartphone of een PDA onderhevig zijn. In de volgende figuur kan u vaststellen welk de situatie is samen met de overkoepelende problemen.



Figuur 13: Het beveiligingsprobleem

Het beveiligingsprobleem wordt zoals in de figuur 13 weergegeven in drie onderdelen. De problemen zijn afhankelijk van het type van mobiel toestel, de manier van transmissie en de bedrijfsservers en de netwerken. Zo moet ondere andere de volgende delen worden beschermd:

- De toegang tot het toestel en de opslag op het toestel
- De applicaties
    - Transmissie van applicatiedata
    - De applicaties hun (tijdelijke) data op het toestel
    - De mobiele code, die wordt uitgevoerd op het toestel met behulp van de browser of e-mailclient, moet veilig zijn en er moet malware beveiliging zijn
- De transmissie van andere data

Dit is dus een uitgebreid probleem. Maar eerst zullen we de problematiek algemeen aanpakken om op die manier niets uit het oog te verliezen.

Mobiele toestellen zijn aan dezelfde bedreigingen onderhevig als een gewone desktop of server. (NIST, 2008) De extra bedreigingen zijn meestal een gevolg van hun grootte en draagbaarheid of van de draadloze methoden om te communiceren. Wanneer we specifiek gaan kijken naar toestellen zoals PDA's of smartphones, dan brengt dit nog extra gevaren met zich in vergelijking met mobiele toestellen zoals laptops.

Volgens het NIST (2008) zijn de grootste bedreigingen voor mobiele apparaten:

- Verlies, diefstal of het weggooien
- Ongeauthoriseerde toegang
- Malware
- Spam
- Electronisch meeluisteren
- Electronisch tracken
- Cloning
- Server-resident data

De bedreigingen hier beschreven zijn deels te wijten aan het toestel en deels aan de applicaties die zich hierop bevinden. Verlies, diefstal, het weggooien, ongeauthoriseerde toegang zijn toestel georiënteerd terwijl de andere bedreigingen applicatie geörienteerd zijn.

Volgens Hoffman (2007) zijn smartphones onderhevig aan de volgende bedreigingen:

- Malware
- Direct Attack
- Data-Communication Interception
- Authentication Spoofing and Sniffing
- Physical Compromise

Hoffman (2007) geeft een algemener beeld weer van de mogelijke bedreigingen, daar waar NIST (2008) specifiekere bedreigingen weergeeft. Een mix van beide zullen hier nu besproken worden.

5.2.1 Verlies, diefstal of het afschrijven

Een smartphone is een klein toestel. Het toestel moet draagbaar zijn en is bijgevolg zeer licht. Als gevolg daarvan verliest men het apparaat sneller. De gebruiker moet zich ervan bewust zijn en moet steeds oplettend zijn. Omwille van dezelfde reden is het ook makkelijk voor kwaadwillenden om het toestel te stelen. Wanneer een van beiden gebeurt, kunnen belangrijke gegevens van de onderneming zomaar buiten de onderneming terecht komen en toegankelijk worden voor iedereen.

Hetzelfde geldt wanneer men een toestel stopt te gebruiken. Het is van belang dat wanneer men stopt een toestel te gebruiken, dat het op de juiste manier vrijgemaakt wordt van alle gegevens. Resetten is vaak niet genoeg. (NIST, 2008) Gegevens zijn nog steeds op de harde schijf aanwezig en daarom leesbaar voor onbevoegde personen. Het is zaaks om gegevens permanent te verwijderen. Hiervoor bestaan gespecialiseerde programma's die de gegevens definitief verwijderen.

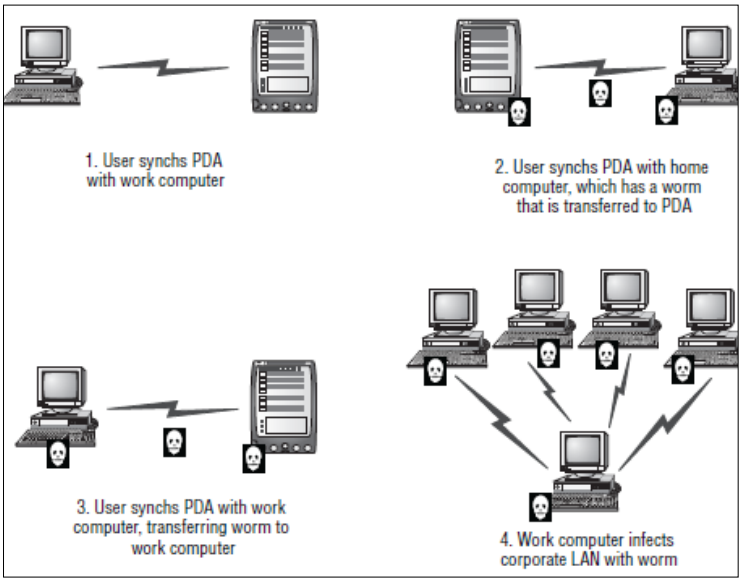
5.2.2 Malware

Malware is een synoniem voor malicous code zoals virussen. Het is een verzamelnaam voor alle code die ontworpen is voor het beschadigen, vernietigen of het laten weigeren van service van een doelsysteem. (Whitman & Mattord, 2009)

Malware wordt typisch meer gericht op toestellen waar er SDK's beschikbaar voor zijn. SDK staat voor Software Development Kit. Dit zijn programma's voor ontwikkelaars waardoor deze makkelijker applicaties kunnen ontwikkelen voor een bepaald platform, in dit geval een PDA of een ander mobiel apparaat. (F-Secure, 2007) Men kan als gevolg daarvan de volgende redenering maken: des te makkelijker men applicaties kan maken (met behulp van SDK's), des te meer applicaties voor een bepaald OS, des te meer malicious code er zal bestaan voor een bepaald OS. Dit is een van de redenen waarom er zoveel malware voor Microsoft Windows bestaat.

Malware zijn schadelijke stukjes software die 'binnendringen' via de internetverbinding of op een andere manier op de PDA terecht komen. Dat kan onder andere via internet downloads, e-mail, (NIST, 2008) messaging services (sms, mms) of via de bluetooth communicatie indien de PDA daarover beschikt.

Malware kan zich op tal van manieren gedragen. Zo kan malware alle handelingen die gebeuren op een apparaat afluisteren, gevoelige informatie stelen, informatie vernietigen op een apparaat of het apparaat onklaar maken. (Mcwilliams, 2005) Ook kan het zich kopiëren naar andere toestellen in het netwerk om zijn effect dan nog eens te verergeren. Een vaak voorkomend doel van malware is: het stelen van data. (NIST, 2008) Malware is een van de grootste redenen van dataverlies in organisaties, volgens een rapport van het Computer Security Institute. Daarom is het van belang om er professioneel aandacht aan te besteden om dit te voorkomen. Maar toch wordt dit vaak niet gedaan. (Hoffman, 2007) Volgens Hoffman gebeurt dit omwille van twee redenen: '*The first is that they simply don't know any better. Why would a Blackberry or cell phone need antivirus protection? The second is that they don't know of the appropriate solution to implement; the malware threat is realized, but what can be done about it on mobile devices?'* Het is cruciaal ook hier dus beveiliging te gaan overwegen. Smartphones worden vaak gekoppeld aan desktops ter synchronisatie en via deze weg kan malware binnendringen en het bedrijfsnetwerk besmetten. In de volgende figuur vindt u dit scenario even verduidelijkt.



Figuur 14: Hoe kan een PDA of smartphone een netwerk infecteren. (Hoffman, 2007)

De werknemer synchroniseert zijn smartphone zowel met desktop van het bedrijf als met de thuisdesktop. Op de thuisdesktop bevindt er zich een virus. Dit virus wordt gesynchroniseerd met de smartphone. Eens de werknemer terug op het werk is zal deze zijn mobiel toestel terug synchroniseren. Alle bestanden inclusief malware worden overgezet. Vanaf dit punt infecteert de desktop de rest van het netwerk. Een goede malware beveiliging is dus onontbeerlijk.

5.2.3 Spam

Spam is een bedreiging die, net zoals op desktops, vaak voorkomt op PDA's en smartphones. Maar wanneer men ermee wordt geconfronteerd op een smartphone, die gebruik maakt van een trage en dure transferverbinding, dan kan dit voor extra problemen zorgen.

Volgens webopedia (2010) is spam *: 'Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup.'* Op dezelfde manier zoals e-mail met reclame voor gewone desktopcomputers kan er voor smartphones ongewilde e-mail en ongewilde sms'en worden ontvangen. Een onaangenaam gevolg is dat er in dit geval ook voor moet worden betaald in de vorm van een datatransmissiekost. Indien de onderneming veel last heeft van spam mails dan kan de datatransmissiekost aardig oplopen. (NIST, 2008) Stel dat e-mails lokaal naar de smartphone

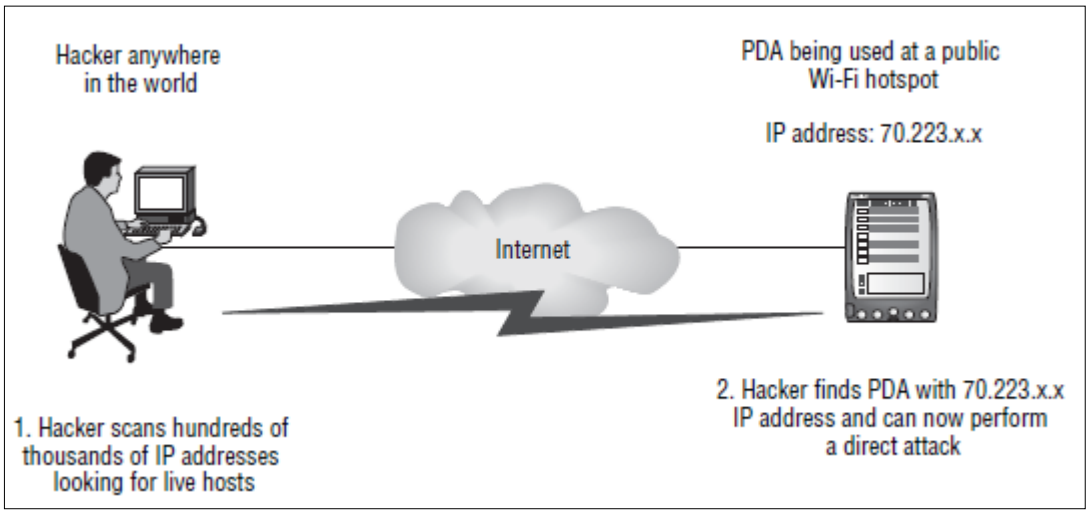
worden gedownload, en de inbox bevat veel spam: dan kan dit resulteren in een grote kost vermits toegestane maandelijkse datatransfervolumes klein zijn. Een oplossing voor dit probleem is gebruik maken van webmail waarbij gegevens niet worden gedownload. Toch vormt dit geen oplossing voor het probleem. De IT-afdeling zorgt best voor een goede filtering van de e-mails.

5.2.4 Direct attack en ongeauthoriseerde toegang

Het onderdeel ongeauthoriseerde toegang hangt sterk samen met direct attacks. Ongeauthoriseerde is een vorm van direct attack waarbij de kwaadwillende ofwel fysiek het toestel in handen heeft of dit op een andere manier doet, bijvoorbeeld via een internet aanval. U vindt lager een uitvoerige uiteenzetting over ongeauthoriseerde toegang in het onderdeel 'Device-level authentication'. Nu wat meer over direct attacks.

Direct attacks zijn de meest gevaarlijke aanvallen voor mobiele toestellen. Volgens Hoffman (2007): '*One of the most dangerous ways a mobile device can be exploited is by a direct attack, in which a hacker finds the device and takes deliberate actions to exploit it.'* Voorbeelden van direct attacks zijn: attacks wanneer men gebruik maakt van een publieke hotspot of wanneer een gebruiker publiek gebruik maakt van het toestel. In het geval van de publieke hotspot is de smartphone kwetsbaar voor aanvallen omdat de verbinding niet beveiligd is bij publieke hotspots. In het andere geval is de smartphone kwetsbaar omdat de aanvaller kan zien welk type smartphone het is en op die manier weet hij welke 'exploit' hij kan toepassen. Volgens Hoffman (2007) zijn er weinig situaties te bedenken waarbij de gebruiker kwetsbaarder is voor een aanval.

De connectie tot het internet kan ook volstaan om een aanval uit te lokken. Het toestel beschikt dan immers over een IP-adres. Hackers zullen scannen naar mogelijke IP-adressen om dan een aanval uit te voeren. U vindt daarvan een voorbeeld in de volgende figuur.



Figuur 15: Het zoeken naar een doel. (Hoffman, 2007)

Wanneer zulk een direct attack succesvol is, dan kunnen alle gegevens die op het toestel staan worden gestolen.

Enkele voorbeelden van zaken die kunnen worden gedaan met toestellen waartoe men toegang heeft (Hoffman, 2007):

- Verwijderen van data op het toestel, wijzigen van data op het toestel
- Het toestel buiten werking stellen
- Het toestel misbruiken
- Wijzgigen van de configuratie van het toestel
- Uploaden van data zoals malware naar het toestel

Enkele voorbeelden van attacks die door het NIST(2008) werden aangehaald zijn: elektronisch afluisteren, elektronisch tracken en cloning.

5.2.4.1 Elektronisch afluisteren

Elektronisch afluisteren is het afluisteren van een persoon met behulp van bijvoorbeeld en PDA. Wanneer een kwaadwillende de PDA van een persoon wil afluisteren zal hij een software applicatie installeren die alle bewegingen bijhoudt die op de PDA gebeuren. Deze kwaadwillende kan dan aan

de hand daarvan alle acties bekijken die door de gebruiker worden gedaan. (Magic Spysuite, 2009) Op de PDA gaat men soms zelfs zo ver tot het op een afstand inschakelen van de recorder zodat men gesprekken op een afstand kan afluisteren. Hierbij hoort ook het elektronische tracken, zie lager.

5.2.4.2 Elektronisch tracken

Met behulp van de ingebouwde GSM module in een PDA kan de werkgever bijhouden waar zijn werknemers zich bevinden. Doch dit kan ook voor kwaadwillende personen die de gebruiker zijn whereabouts in het oog wil houden. Door een korte periode van onoplettendheid kan op een makkelijke manier de PDA zo gemanipuleerd worden dat dit tot de mogelijkheden behoort. (FollowUS, 2003) Een oplossing zou zijn dat er aan de gebruiker na een bepaalde hoeveelheid tijd een bericht wordt getoond dat aangeeft dat hij 'getrackt' wordt. Maar ook dit is natuurlijk omzeilbaar.

5.2.4.3 Cloning

Bij cloning zal een kwaadwillende proberen een PDA te 'clonen'. Dit betekent dat hij een tweede PDA zal doen laten lijken op de origineel door het overnemen van de identificatiegegevens naar de tweede PDA. Hierbij heeft hij wel een fysieke toegang tot het toestel nodig. (Beam, 2007) De gebruiker zal onwetend gebruik maken van de op zijn lijkende PDA. Zo kan de kwaadwillende talloze gevoelige informatie vergaren.

5.2.5 Server resident data

Volgens het NIST (2008) betekent server resident data het volgende: *"Data such as electronic mail maintained for a user by a network carrier as a convenience, may expose sensitive information through vulnerabilities that exist at the server."* De data die dus wordt bijgehouden door de telecomoperator kan voor lekkage zorgen. Wanneer de operator een slechte beveiliging

toepast kan er via deze weg data weglekken. Belangrijke berichten kunnen op die manier onderschept worden of gewoon publiek worden gemaakt.

5.2.6 Transmission security: voorkomen van data-communication interception

Mobiele apparaten worden vaker standaard uitgerust met een mogelijkheid om draadloos verbinding, al dan niet te maken met een netwerk. Transmission security is een van beveiligingsrisico's die door het NIST werden buiten beschouwing gelaten, maar toch niet te onderschatten is.

5.2.6.1 Personal Area Network

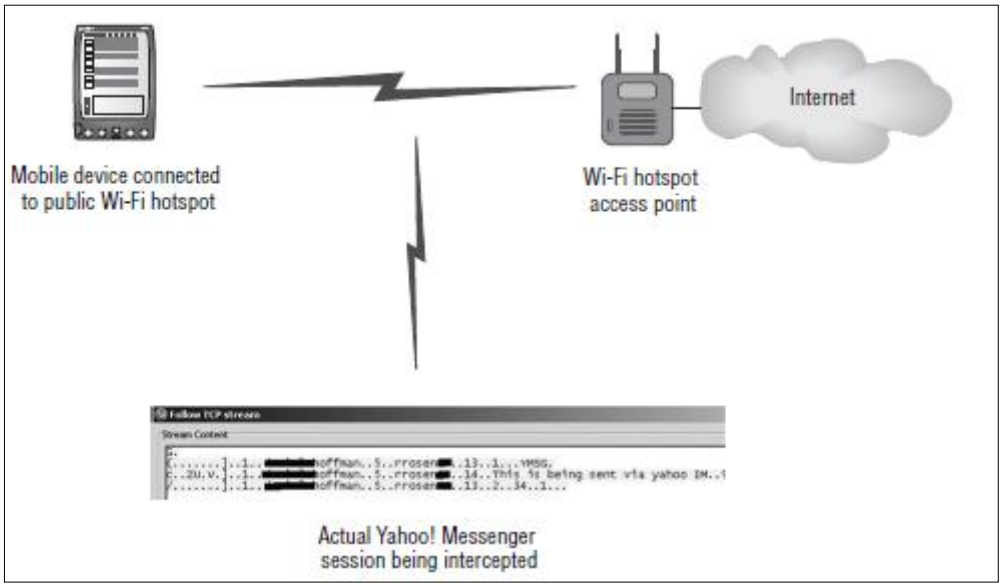
De technologie die wordt gebruikt in het persoonlijke netwerk is infrarood en bluetooth transmissie. (Botha, Furnell, & Clarke, 2009) Op sommige toestellen is dit het geval wanneer men gebruik wil maken van infrarood transmissie dat de bluetooth transmissie ook automatisch wordt ingeschakeld. Dit kan een probleem vormen. Wanneer men hiervan niets af weet en men wil een transmissie starten via infrarood kan een kwaadwillende toegang verschaffen via bluetooth. Bluetooth heeft een groter bereik dan infrarood en is daarom kwetsbaarder om aangevallen te worden. (Botha, Furnell, & Clarke, 2009) Het is daarom ook noodzakelijk om de gebruiker via een icoon op het display te laten weten indien bluetooth is ingeschakeld of niet. Zo kan ongeautoriseerde toegang tot files voorkomen worden. Volgens Potter (2004) kan bluetooth tot diverse aanvallen of andere kwetsbaarheden leiden: bluesnarf, backdoor attacks, DoS attacks.

Volgens bluetooth.com (2009) worden per week meer dan 1 miljoen toestellen met bluetooth verscheept. Kwaadwillende zullen daarvan gebruik gaan maken: *'The vast majority of these devices are cell phones, however Bluetooth radios can be found in laptops, PDA's, cars, and even some household automation equipment. With such rapid deployment, the security community (attackers and defenders alike) are turning their attention to this up and coming PAN protocol.'*

(Potter, 2004) Het is daarom niet onbelangrijk daarmee rekening te houden en eventueel deze mogelijkheid uit te schakelen.

5.2.6.2 Local Area Network en Wide Area Network

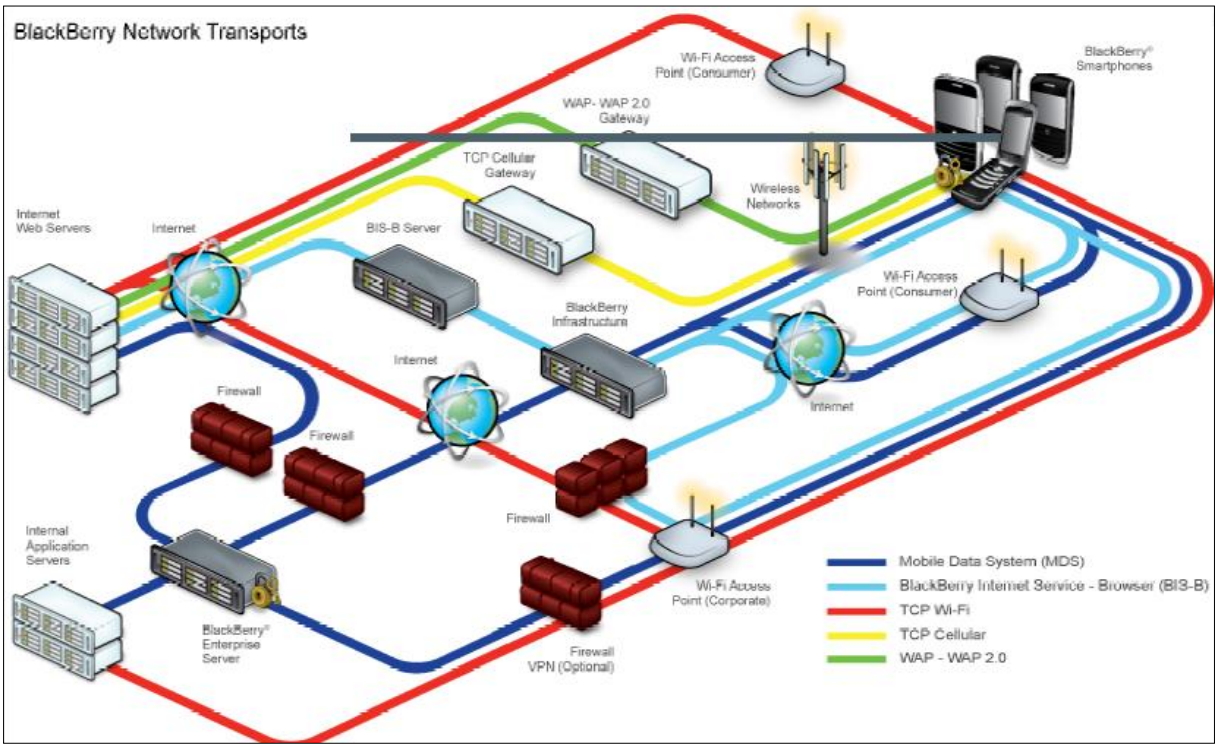
Draadloze netwerken zijn van nature moeilijker te beveiligen zijn. Er is geen fysische controle. Als men zich in de buurt van het draadloze accesspoint bevindt, kan men indien er geen beveiliging voor handen is inloggen. Tevens zijn publieke toegangspunten een probleem. De encryptietechnieken die dit voorkomen zijn zwak. WEP, wireless encryption protocol, is geen sluitende beveiliging. Soms wordt er eerder gekozen om dit niet te implementeren omdat het alleen maar extra werk met zich meebrengt. (Ashely, 2004) Hoffman (2007) stelt het volgende vast in bedrijven: *'When mobile devices connect to public Wi-Fi hotpots, enterprises generally ignore the threat and pretend there really isn't any of their data being transmitted from mobile devices over unprotected wireless networks. Clearly, not admitting there is a problem doesn't make it go away.'* Dit is een onwaarschijnlijke aanpak welke in problemen kan resulteren. De volgende figuur illustreert een situatie waarbij een kwaadwillende gaat sniffen wanneer een onwetende werknemer gebruik maakt van een publieke, onbeveiligde, hotspot.



Figuur 16: Sniffen van data bij gebruik van een publieke hotspot (Hoffman, 2007)

Men probeert aan dit probleem een mouw te passen door de WPA technologie te implementeren. WPA, Wi-Fi protected acces, biedt meer veiligdheid en is moeilijker te kraken. (Ashely, 2004) Ook hierin bestaan verschillende typen. Maar zelfs dit protocol is niet onkraakbaar. (Network Security, 2010)

Er is ook sprake van de uitgebreide problematiek met smartphones. Mobiele telefoons zoals smartphones kunnen op tal van manieren connectie maken met het telefoonnetwerk. Er zijn verschillende typen van connectiemethoden: bluetooth, Wifi, LAN, GSM-netwerken. U vindt u op de volgende figuur een voorbeeld van het de diversiteit van connectiemethoden.



Figuur 17: Meerdere typen netwerken (Research In Motion, 2010)

Het is voor de IT-afdeling een uitdaging om al deze verschillende technologiën op goede, doch eenvoudige manier te beveiligen.

Volgens Xirasagar en Mojtahed (2010) kan er gebruik worden gemaakt van IPsec, zowel in applicaties als in draadloze applicaties. IPsec zorgt voor het veilig stellen van vertrouwelijkheid,

integriteit van het bericht, authenticatie, autorisatie en anti-replay beveiliging. Op deze manier kan er veilig worden gewerkt. In hoofdstuk 7 zal u een uitgebreidere uiteenzetting vinden om dit probleem aan te pakken. De software, Blackberry Enterprise Server Express, maakt gebruik van een universele aanpak zodat mobiele toestellen connectie kunnen maken via verschillende netwerken en toch op een veilige manier. Maar hierover later meer.

5.2.6.3 Conclusie transmission security

We kunnen besluiten dat draadloze netwerken van nature minder veilig zijn dan bedrade netwerken omwille van het vrije karakter. Daarenboven zijn de beveiligingstechnieken, ter beveiliging van draadloze netwerken, ook niet altijd even sluitend. Men moet opletten welke technieken worden toegepast alvorens men echt zeker kan zijn van de veiligheid ervan.

De problematiek met de verschillende typen netwerken is ook niet makkelijk te behandelen voor de onderneming. Dit blijkt een ingewikkeld probleem te zijn.

5.2.7 Bedreigingen mobiele applicaties

Vandaag de dag worden applicaties vaak in een mobiele context gebruikt. Zoals al eerder aangegeven zullen applicaties vaker en vaker benaderd worden via het internet. Hiervan is SaaS een voorbeeld. Maar ook webapplicaties in de vorm van HTML en PHP. Deze applicaties vormen een nieuwe bedreiging. Deze laatste vorm van applicaties bevat code welke lokaal op de clients wordt uitgevoerd. Cross (2007) zegt hierover het volgende:" *Mobile code passes across a network and is executed on a destination machine. The programs designed to provide services can be any one of a variety of forms, such as scripts within documents and e-mail, or code objects running within Web pages. Because of the way mobile code is written, the same piece of code can sometimes run on multiple platforms. Mobile code is excellent for distributing applications across networks or the Internet."* In deze mobiele code wordt er vaak uitvoerbare code gestopt in de vorm van een stukje Javascript of VBscript. Ook deze code wordt lokaal uitgevoerd maar in deze uitvoerbare code kan code zitten die schadelijk is. Cross (2007) stelt het volgende vast: "*As you can imagine, additional steps need to be taken by end users to further ensure security, as e-mail messages and programs*

that include mobile code can now be "carriers" for malicious viruses." Dit vormt dus het grootste probleem in verband met applicaties die via een mobiel toestel worden benaderd. Niet alleen mails kunnen dus voor problemen zorgen, maar ook het gewoon openen van een 'geïnfecteerde' pagina via de mobiele browser kan al voldoende zijn.

5.2.7.1 Attacks via mobiele applicaties

Volgens Cross (2007) zijn de twee grootste typen bedreigingen: browser attacks en mail client attacks. Browsers komen vaker in contact met mobiele code dan e-mail applicaties, doch HTML e-mail wordt sneller en sneller de norm. (Cross, 2007) Browsers voeren lokaal code uit. Deze code kan al dan niet schadelijk zijn voor het systeem. Zo kan er schadelijke code in de vorm van VBScript, JavaScript op een webpagina zitten. Iedereen, dus ook kwaadwillenden, kunnen schadelijke code op het internet zetten. Net daarom is het van belang deze bedreiging niet te onderschatten. E-mail clients vormen ook een grote bedreiging in de vorm van de code die wordt uitgelezen. Enkel het openen, de attachments buiten beschouwing gelaten, kan al voldoende zijn om schadelijke code uit te voeren. In HTML-mails kan er schadelijke code ingevoerd zijn. Deze schadelijke code hoeft enkel uitgelezen te worden. Dan is er nog de bedreiging van de bijlagen. Een virusscanner is vereist welke schadelijke bijlagen eruit filtert door eerst te scannen op virussen.

Een mogelijke oplossing voor gevaarlijke websites en e-mails is de zogenaamde whitelist techniek, welke ook wordt toegepast bij KBC. (Van den Driessche, When data goes up and out: Data Leakage Prevention in a Financial Organisation, 2009) Wanneer men een whitelist toepast zal enkel een aantal websites, welke met zekerheid veilig zijn, worden toegelaten. Deze techniek beperkt de veiligheid, maar op die manier is de data binnen de onderneming met zekerheid veilig. Het concept van deze techniek kan ook toegepast worden op het e-mail verkeer. Een e-mail die wordt ontvangen van een onbekende afzender moet met voorzichtigheid worden geopend. Zo kan men opteren om scripts of bijlagen niet uit te voeren of te openen voor onbekende afzenders, een mogelijkheid die reeds bestaat binnen bepaalde programma's. Een voorbeeld daarvan is Microsoft Office Outlook 2007. (Microsoft, 2010)

5.2.7.2 Achtergebleven data op de mobiele toestellen

De onderneming moet ook nodig opletten met de data die achterblijft na een surfsessie met het mobiel toestel. Er kan tevens ook data achterblijven na het gebruik maken van applicaties. Volgens Research In Motion (2010): *'Examples of sensitive data include sensitive data in the cache for the key store browser, unencrypted data from email messages, LDAP authentication passwords, and data from certificate and key searches.'* In het geval van webmail blijft er soms data achter in de vorm van een geopende bijlage. Deze bijlage werd eerst gedownload om nadien te worden geopend. Maar indien men de tijdelijke versie niet verwijderd zal deze nog achterblijven op het geheugen van de smartphone.

Als voorbeeld van de browser attacks en achtergebleven data op het toestel zal ik in dit hoofdstuk mobile learning verder uitdiepen. Indien er een mobile learning toepassing wordt uitgevoerd op een mobiel toestel zal deze meestal via de browser worden geopend. Zulk een applicatie voert dus code uit via de browser en de applicatie downloadt bijlagen indien de gebruiker dit wenst. Een mobile learning applicatie is met andere woorden onderhevig aan het merendeel van de bedreigingen. Daarom is dit een goed uitgangspunt. Dit wordt tevens als uitgangspunt gekozen voor de volgende hoofdstukken.

5.2.7.3 Mobile learning

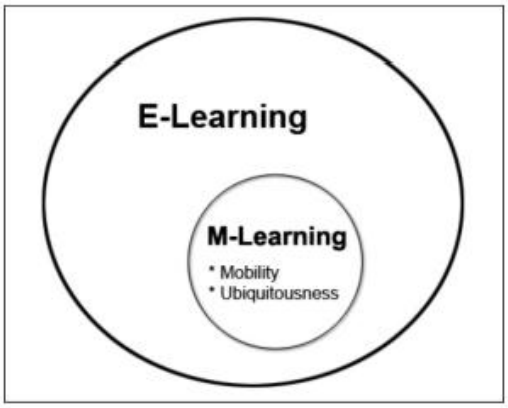
5.2.7.3.1 Mobile learning: wat is het?

De globalisering zorgt ervoor dat men als zakenman vaker moet reizen. (Norberg, 2002) Klanten en leveranciers kunnen geografisch sterk verspreid zijn. De werknemers moeten daarom erop toezien dat zij deze contacten onderhouden. Dit brengt veel reizen met zich mee, ze spenderen veel tijd in 'transit'. Deze tijd is vaak verloren tijd, maar men kan dit ook op een andere manier proberen aan te wenden. Literatuur over time-management raadt aan om deze reistijd te benutten.

Maak gebruik van een draagbare computer, PDA of soortgelijk toestel. (Hindle, 1998) Dit toestel kan gebruikt worden om enkele cursussen of boeken door te nemen.

In de huidige zakenwereld maakt men vaker en vaker gebruik van mobiele apparaten. (McNurlin, Sprague, & Bui, 2009) Gebruikers van deze toestellen staan dus ook onder weg in verbinding met het internet en kunnen berichten versturen met behulp van deze apparaten. De onderneming kan gebruik maken van deze trends. Zo kan ze bijvoorbeeld toegang verlenen tot documenten op de servers in de onderneming. Gebruikers kunnen de tijd die ze doorbrengen in de terminals, wachtend op hun vliegtuig, gebruiken om te leren. Deze nieuwe manier van leren wordt mobile learning genoemd. (Motiwalla, 2005) Dit is een manier van leren die vaker wordt toegepast volgens Leung en Chan (2003*): 'One recent and significant change in learning environment is the demand of mobility.'*

Mobile learning is een uitbreiding van e-learning, elektrical learning. (Leung & Chan, 2003) E-learning beslaat een groter veld dan m-learning, het is algemener van aard. E-learning slaat op elke elektrische manier om te leren, terwijl mobile learning extra fixeert op het mobiele aspect. U kan dit concluderen uit figuur 12.



Figuur 18: M-Learning en E-learning (Leung & Chan, 2003)

Er zijn ook danig wat verschillen tussen e-learning en m-learning. In de volgende tabel ziet u de grootste verschillen opgesomd.

Pedagogy	e-Learning class	m-Learning class
Course location	HTML website	WML website
Class materials	Online notes, URLs and presentation slides	URL links to course website
Class experience	Whiteboards, group touring, virtual demos, chat rooms, discussion boards, and e-mail	SMS, alerts, discussion boards, course calendar
Assignments/projects	E-mail attachment or posting with web forms	Instant messaging for project coordination
Student assessment	On-line exams, chat room/ discussion board participation	On-line exams, chat room/ discussion board participation

Tabel 3: Een vergelijking tussen e-learning en m-learning (Leung & Chan, 2003)

Maar er is controverse rond het topic mobile learning. Men vraagt zich af of het wel toepasbaar is. Leerlingen zouden volgens het constructive learning model moeten kunnen ageren en reflecteren op een bepaalde manier. (Motiwalla, 2005) Zonder mobile learning zou dit al niet mogelijk zijn onder weg. Volgens de conversation theory moet de leerling tevens ook kunnen communiceren waarbij er reply moet komen van de andere kant. (Motiwalla, 2005) Dit is cruciaal in het leerproces. Met behulp van mobile learning technologieën kan de leerling te allen tijde in contact staan met diegene die de cursus geeft conform de twee eerder genoemde modellen.

Zal de reiziger temidden al het lawaai in de terminal zich wel kunnen toeleggen op data die hij ter beschikking krijgt gesteld? (Motiwalla, 2005) Er is onderzoek naar verricht indien dit effectief wel een toegevoegde waarde kon bieden. Volgens Motiwalla (2005), die een survey die gedurende 2 semesters ondernam waarbij studenten gebruik konden maken van hun gsm om digitaal toegang te krijgen tot een discussieforum en andere documenten met betrekking tot een aantal vakken, was het mogelijk. De studenten waren hierover zeer te spreken: er waren tal van toepassingen. Zo konden ze bijvoorbeeld met behulp van alerts worden gewaarschuwd indien een er opdracht moest worden ingediend, ze konden gebruik maken van een forum om vragen te stellen. Het vormde een uitbreiding op het digitaal platform dat destijds al beschikbaar was.

In de onderneming kunnen werknemers op dezelfde manier als de leerlingen profiteren van zulk een systeem. Ze zullen over de mogelijkheid beschikken om te allen tijde toegang te hebben tot

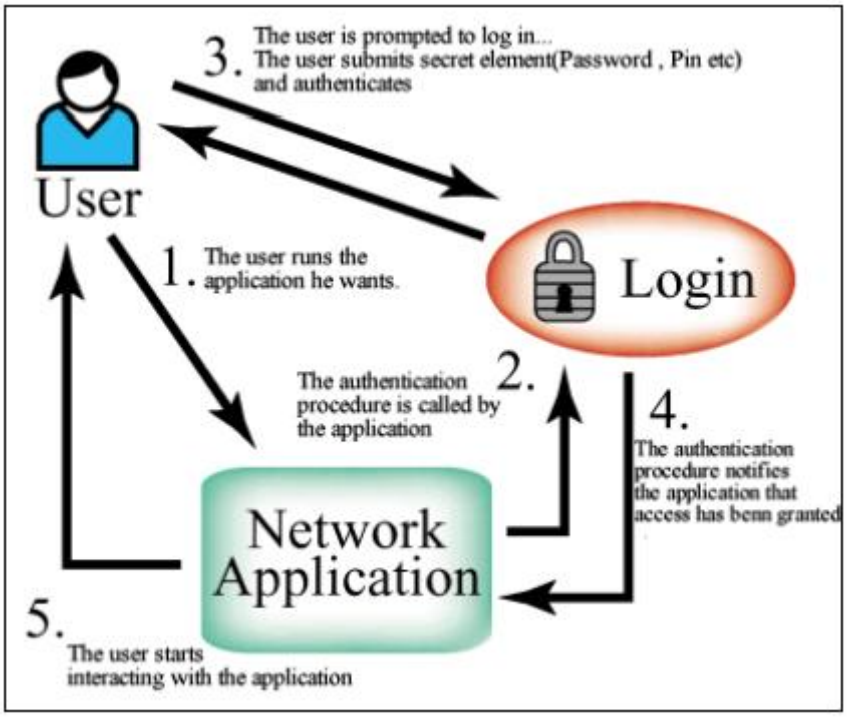
een digitaal leerplatform en het leerplatform kan de werknemers op de hoogte houden van tal van interessante zaken met behulp van notifications.

Een cruciale vraag die de ondernemer zich in dit geval kan stellen is hoe het zit met de beveiliging. De onderneming zal cruciale informatie die door de werknemers kan worden geraadpleegd om te studeren ter beschikking stellen. Waarom is het zo belangrijk de gegevens te beschermen? Tsiantis, Stergiou en Margariti (2007) zeggen hierover het volgende: "*In security terms, information ownership can determine access and manipulation rights. Issues of ownership, therefore, relate to both confidentiality and integrity. However, it is important to note that the users' concept of ownership is closely intertwined with that of privacy. It is essential, to understand users' perceptions of information ownership, usage and privacy when developing on-line learning systems. Privacy and intellectual property rights rely on our perception of them. As well as how well we are protected, it is also important that we perceive ourselves and our information to be safe and private.Therefore identifying users' perceptions of privacy and ownership are an important element in identifying what needs to be protected and how best to protect it."* De perceptie van hoe de gebruiker het ownership ziet is verweven met de privacy. Sommige gebruikers vinden bepaalde gegevens cruciaal en andere gebruikers vinden de gegevens dan weer van minder belang. Bij het ontwikkelen van de mobile learning applicaties moeten ontwikkelaars daarbij rekening houden opdat de privacy niet wordt geschaad.

5.2.7.3.1 Mobile learning: beveiligen

Wanneer men gebruik maakt van een mobile learning systeem, dan is men als onderneming geïnteresseerd in twee kernpunten met betrekking tot beveiliging: authenticatie en privacy. (Tsiantis, Stergiou, & Maragariti, 2007) De gebruiker wenst met andere woorden dat hij, en hij alleen toegang heeft tot het leersysteem. Er moet dus een manier worden gevonden waarbij zijn identiteit wordt geïndentificeerd. (authenticatie) Ten tweede wenst de gebruiker afdoende bescherming van zijn privacy terwijl hij gebruik maakt van het leersysteem

Figuur 19 geeft u een overzicht hoe het authenticatie systeem werkt. Met behulp van zulk een mechanisme kan de gebruiker zijn ware identiteit bewijzen en op die manier kan hij inloggen op het systeem. Het proces bestaat uit een vijftal stappen. In stap 1 zal de gebruiker de gewenste applicatie openen, in dit geval de m-learning applicatie. De applicatie zal de authenticatie procedure oproepen. De authenticatie procedure zal op één van de drie manieren die hier lager zijn beschreven de gebruiker authenticeren. Daarna zal het authenticatiesysteem zijn fiat geven om de gebruiker al dan niet toe te laten tot het systeem. In stap 5 kan de gebruiker de applicatie beginnen gebruiken. Dit is de algemene werking van een authenticatie procedure.



Figuur 19: Het authenticatie mechanisme (Tsiantis, Stergiou, & Maragariti, 2007)

Men kan zoals hoger reeds aangehaald overgaan tot het gebruik van een drietal manieren om zich te authenticeren. Deze zijn een knowledge-based authenticatie systeem, een token-based authenticatie systeem of een biometrisch systeem. (Tsiantis, Stergiou, & Maragariti, 2007) Bij know-ledge based systemen wisselt de gebruiker iets uit dat enkel hij weet. Bij een token gebaseerd beschikt de gebruiker over een token. Aan de hand van dit token kan de gebruiker

bewijzen wie hij is. Biometrische systemen zijn iets geavanceerder. De gebruiker moet aan de hand van een lichaamsdeel bewijzen wie hij is, bijvoorbeeld zijn ogen.

Het tweede probleem, de privacy, moet worden opgelost. Met behulp van de implementatie van een authenticatiesysteem kan de onderneming praktisch met zekerheid weten wie toegang tot de applicatie wenst. Maar derden kunnen, indien de transmissiestroom van de data slecht beveiligd is, meekijken. Een mogelijke oplossing vormt de verbinding encrypteren. Indien het gaat om een webapplicatie kan de onderneming gebruik maken van SSL. Zoals McNurling et all. (2009) stelt: '*The RSA method is incorporated into all major Web browsers and is the basis for the Secure Socket Layer used in Internet Communications.'* Wanneer er gebruik wordt gemaakt van dit type beveiliging wordt het voor derden al moeilijker om de gegevenstransfer in te kijken.

Het is een gecompliceerd probleem dat bestaat uit drie hoofdcomponenten: device-level authentication, transmissie beveiliging en security van het bedrijfsnetwerk (binnen de onderneming zelf).

5.3 Conclusie beveiliging mobile computing

Mobile computing is onderhevig aan een groot aantal bedreigingen zoals hierboven besproken. De onderneming mag dit niet onderschatten. De belangrijkste bedreigingen zijn malware, diefstal van het toestel, het verliezen van het toestel, een direct attack en transmission security. (Hoffman, 2007) De onderneming moet actie hiertegen ondernemen. Zoals uit deel 7.2 blijkt is er ook vaak een verandering in aanpak nodig. De security policy moet op deze bedreigingen voorbereid zijn.

6 Case KBC: security management bij KBC

Dit onderdeel is het resultaat van een interview met the Head of Information Risk Management van KBC, Noël Van den Driessche. De bedoeling was een uitgebreider inzicht te krijgen in hoe men bij KBC beveiliging van mobiele toestellen aanpakt. Tevens proberen we een beter inzicht te krijgen in het risico management van de onderneming, hoewel dit eerder beperkt was.

6.1 Beveiligen van grote hoeveelheden gegevens: een probleem

In de banksector maakt men dagelijks gebruik van een enorme hoeveelheid aan data. Men moet allerlei gegevens bijhouden over de bankrekeningen van de klant en alle andere producten van de klant zoals bijvoorbeeld verzekering, aandelen, enz. Dit resulteert in enorme hoeveelheden gegevens. Bij KBC komt dit neer op een 500TB aan data, dit is 500.000 GB aan gegevens. De hoeveelheid data die moet worden beschermd is dus aanzienlijk, zoniet te groot. Hoe zal men de beveiliging aanpakken bij KBC? Heeft KBC hier speciale benaderingen voor die de zaken in een nieuw perspectief plaatsen?

Zoals reeds eerder aangehaald beschikt KBC over grote hoeveelheden gegevens. Deze grote hoeveelheden gegevens worden gebruikt door de werknemers op een bijna dagelijkse basis. Ter bescherming van deze gegevens kan men gebruik maken van allerlei encryptiemechanismen om op die manier de gegevens te versleutelen maar dit brengt met zich de kost van het decrypteren mee indien de gegevens terug moeten worden gebruikt. Dit kost telkens tijd, afhankelijk van de manier waarop de gegevens worden beschermd. In het geval van KBC is een dergelijke situtie niet houdbaar. Alle werknemers verspreid over een geografisch groot gebied maken constant gebruik van die gegevens en de gegevens op zulk een manier beschermen is geen oplossing. Het kost teveel tijd, en teveel processing time om de data telkens de encrypteren en decrypteren. Hierbij zou de gewone klant die buiten aan de atm staat niet gediend zijn, hij moet immers wachten op de

decrypteren van de gegevens. Men moet een afweging maken tussen de graad van bescherming en kost die deze beveiliging met zich meebrengt.

Een voorbeeld van de grote hoeveeheid gegevens bij KBC zijn de e-mails. Dagelijks worden er bij KBC een 1.500.000 mails ontvangen en minstens evenveel verzonden. Men zou deze mails ook allemaal moeten scannen opdat ze geen gevoelige data bevatten (scannen op vertrouwelijkheid) om deze dan te beschermen en indien nodig te filteren. Maar dit is niet meteen een optie, het zou namelijk teveel tijd kosten om dit te doen. Filtering tegen malicious code wordt natuurlijk wel gedaan. Virussen en andere gevaarlijke code worden op die manier wel geweerd. Maar hoe wordt dataverlies bij KBC dan tegengegaan? Om dit te kunnen uitdiepen moeten op de eerste plaats alle risico's worden onderzocht.

6.2 De risico's

Alvorens men weet als onderneming wat men moet beschermen moet KBC de risico's vaststellen. Daar waar de meeste ondernemingen gebruik gaan maken van wiskundige formules en kansberekeningen, zal men bij KBC gebruik maken van een zeer interessante aanpak om risico's in te schatten.

Men liet zijn IT- officers het risico inschatten van de bedreigingen en daaraan gekoppeld de mogelijke impact. Ze deden dit met behulp van een excel werkblad. U vindt hiervan een voorbeeld in bijlage 2 deel 1. Des te hoger een item zich bevindt, des te hoger de impact (in monetaire termen) en des te meer naar rechts, des te groter de kans dat het incident voorkomt. Zo had men een overzicht op wat de IT - officers bedreigend achtten. Op basis van deze bevragingen kon men dan een gemiddelde berekenen. Zo heeft men een startpunt. Aan de grootste bedreigingen kan men het eerst en meer aandacht geven en ook meer middelen toewijzen ter beveiliging. Zoals u dus kan vaststellen is het een delicate evenwichtsoefening tussen graad van beveiliging, graad van risico en middelen. U vindt de uitkomst van de schakeringen in bijlage 2 deel 2.

6.3 Hoe gaat men beschermen?

Het grote probleem is dat KBC moet weten hoe men de beveiligingsstrategie gaat aanpakken. Men heeft twee opties:

- Men kan de data beschermen
- Men beschermt de perimeter

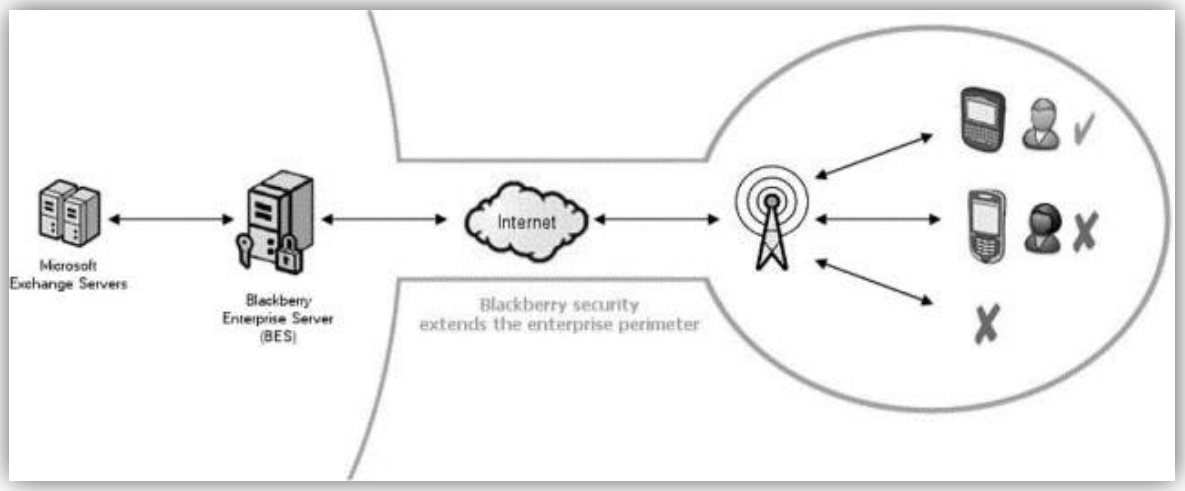
De eerste optie is zeer complex en vraagt veel werk. Men moet elk stukje data gaan beschermen en men moet gebruikers enkel toelaten wat ze 'mogen'. Deze optie stelt voor om een allesomvattende beveiliging te creëren die volledige encryptie biedt van elk stuk data en men moet als beheerder alles hebben geschat want men moet op elk mogelijke manier alles afschermen in de onderneming. Zoniet, zullen gebruikers of kwaadwillenden er misbruik van maken en datalekkage zal het resultaat zijn.

Een andere optie is de perimeter beschermen. Omdat er, zoals hoger al aangegeven, een grote hoeveelheid aan data wordt gebruikt en omdat deze constant in beweging is het moeilijk om de data constant te beschermen. Daarom is een andere aanpak vereist. Men zal als onderneming nog steeds er alles aan doen om de gegevens te beschermen, maar tot op een bepaald niveau. Men vraagt hierbij de medewerking van de gebruikers, de werknemers en de klant dus. De werknemers dienen in deze optie achtzamer om te springen met de gegevens. Het is de bedoeling dat men de perimeter beschermt. Maar wat is de perimeter?

De perimeter in KBC was vroeger makkelijk te omschrijven: elke computer op 'de premises' behoorde tot de perimeter en deze moest worden beschermd, daarbuiten behoort een computer niet tot de perimeter. Maar met de evoluties in de huidige ICT - omgeving is deze manier van denken niet langer houdbaar. De perimeter is nu uitgebreid. Bijvoorbeeld een gebruiker die gebruik maakt van een laptop op zijn hotelkamer in Madrid behoort tot de perimeter.

In feite is elke gebruiker een deel van de perimeter en men moet de beveiliging hierop ook afstellen. De gebruiker moet dus meer aandacht besteden aan wat hij doet. Als de gebruiker in het

buitenland gebruik maakt van een Blackberry dan behoort dit hele gegeven tot de perimeter. Blackberry biedt een mogelijkheid tot bescherming van deze perimeter. Hierop zal later, in hoofdstuk 7, dieper worden ingegaan. In de volgende figuur kan u de perimeter zien die met behulp van Blackberry software kan worden gebouwd.



Figuur 20: Blackberry Security Perimeter Overgenomen uit (Lambert, 2005)

Zoals u kan vaststellen uit de figuur kan met behulp van Blackberry Eneterprise Server(BES) een extensie van de perimeter worden gebouwd. Deze zorgt voor een toename in de veiligheid. KBC maakt ook gebruik van de Blackberry Enterprise Server voor beveiliging van haar mobiele toestellen.

6.4 De gebruiker als firewall

KBC gaat ervan uit dat de gebruiker als firewall fungeert om dataverlies tegen te gaan. Dit is een andere manier van denken dan die in de meeste ondernemingen wordt toegepast. Traditioneel wordt ervan uitgegaan dat men alles in het werk stelt om de werknemer te beletten dat hij data lekt uit de organisatie. Maar op grote schaal is die manier van werken onmogelijk, er is immers altijd wel een lek. KBC zal daarom zijn werknemers beschouwen als een soort van firewall. Zij

moeten mee helpen met het voorkomen van dataverlies. De gebruiker heeft immers toegang tot de ICT infrastructuur en hoe goed men de systemen beveiligt, het is onmogelijk om elke vorm van gegevenslekkage te voorkomen.

Dit betekent natuurlijk niet dat er niet in de gaten wordt gehouden wat er gebeurt in de onderneming. KBC monitort werknemers, maar ook dit kan ze niet te ver doordrijven. Het monitorren levert ook een grote hoeveelheid aan data op met daarbij incidenten en een zinnige analyse daaruit maken kost enorm veel tijd en moeite.

KBC introduceert daarom een nieuwe manier van denken in de onderneming. Traditioneel werd er gedacht in de vorm van: kan ik iets, dan mag het ook. Maar dit is natuurlijk niet waar. Een voorbeeld: op de weg kan men in theorie gezien links gaan rijden zonder dat dit een probleem met zich mee brengt terwijl het verboden is. Natuurlijk is men dan automatisch een gevaar voor de andere automobilisten en jezelf, maar het is mogelijk. Dit is net hetzelfde in de IT wereld. Als werknemer bij KBC kan men allerlei dingen doen, zoals files binnenbrengen in de onderneming die de onderneming schaadt of men kan afwijken van beveiligingsregels. Dit zal negatieve gevolgen hebben voor de onderneming. Maar natuurlijk heeft dit als consequentie dat het op bepaald moment fout kan lopen. De werknemer bij KBC zal in dat geval de gevolgen moeten dragen, hij zal op het matje worden geroepen. Dus in KBC probeert men andere manier van denken, een andere cultuur, te introduceren. Het is niet omdat iets mogelijk is, dat men het ook moet gaan misbruiken zelfs al is er niet meteen een politieagent in de buurt die sanctioneert. Zo'n verandering in de cultuur van de onderneming is vanzelfsprekend niet makkelijk. Maar het is wel de moeite waard.

In KBC maakt men gebruik van procedures om een groot aantal misdrijven te voorkomen. Hier speelt het geheel van policies een belangrijke rol. Elke soort van policy zoals beschreven in het hoofdstuk 4 van dit werk zijn cruciaal. Uit deze policies worden procedures geschreven. Deze kunnen dan binnen de onderneming worden toegepast en leiden tot een betere beveiliging. Bijvoorbeeld het gebruik van externe gegevensdragers. Men zal bij KBC gebruik mogen maken van externe gegevensdragers, maar om het gegevens lekken te voorkomen mag er niets worden op geschreven, enkel inlezen. (in het laatste geval mag er vanzelfsprekend nog virus op zitten of dergelijke) Men probeert op die manier het besmetten van de bedrijfsinformatiesystemen te

voorkomen. Dit voorbeeld kan men natuurlijk technisch voorkomen door de clientcomputer te configureren. Toch zal de werknemer door bestanden te e-mailen gegevens kunnen lekken. De verantwoordelijkheid ligt dus bij de werknemers.

6.5 Onder controle

De vraag is nu wanneer de gegevens onder controle zijn, wanneer zijn ze niet gelekt uit de onderneming?

KBC heeft hiervoor een drietal vereisten opgesteld:

- Ze moeten gebruikt worden voor het juiste doel,
- Ze moeten door de juiste persoon worden aangewend,
- Ze moeten met behulp van de juiste technologie worden gebruikt

Indien op een of meer van deze drie vereisten niet positief kan worden geantwoord, dan zal KBC beschouwen dat de data niet meer onder controle is. Ze is met andere woorden gelekt uit de onderneming en men is de controle dus kwijt.

Een voorbeeld hierop toegepast is een vertrouwelijke attachment in een e-mail. KBC eist dat zijn gebruikers confidentiële informatie niet op hun eigen thuiscomputer openen. Wanneer een werknemer dan de bijlage opent op een Blackberry is er geen probleem. De Blackberry staat immers op de whitelist (hierover lager meer) bij KBC en confidentiële informatie kan worden geopend hierop, ze wordt immers niet lokaal op de Blackberry opgeslagen. Dus op de Blackberry wordt ze door de juiste persoon aangewend, ze wordt voor het juiste doel gebruikt en ze wordt met behulp van de juiste technologie geaccessed. Maar wanneer de werknemer de informatie op een groter scherm wil zien en dus doorstuurt naar zijn eigen thuiscomputer zal de een van de drie voorwaarden niet meer vervuld zijn, namelijk de technologie waarmee het bestand wordt geaccessed wordt is niet meer zoals KBC het vooropgesteld had.

Men maakt in KBC gebruik van Blackberry. Slechts een klein aantal van de werknemers bij KBC maakt hiervan gebruik. Het zal het vooral het hoger management zijn dewelke vaak hun e-mails moeten oproepen. Het gebruik van de Blackberry is gestandaardiseerd. KBC geeft dus ondersteuning en heeft dit platform volledig uitgewerkt. Hiermee wordt bedoeld dat KBC procedures heeft geschreven over wat mag en wat niet en regels zijn opgesteld.

6.6 De security policy bij KBC

Bij KBC maakt men gebruik van een zogenaamde whitelist. Een whitelist is een lijst waarop staat wat is toegestaan in de onderneming en wat volgens de regels is. Dit is een lijst waarbij men steeds voorop loopt en waarbij de onderneming duidelijk de regels stelt. Dit in tegenstelling tot een blacklist. Een blacklist is een lijst die allerlei regels van wat wordt gebannen in de onderneming. Een nadeel van de blacklist methode is dat men constant achterop loopt en dat men dwingend overkomt. Men loopt bij deze methode achterop omdat men als onderneming alles toelaat totdat men zegt dat het niet meer mag. De onderneming onderzoekt niet op voorhand indien iets wel veilig alvorens het 'los' te laten in het netwerk. De meeste gebruikers zullen in de onderneming dan al gebruik maken van bijvoorbeeld een stuk software en zullen zich dan begrensd voelen wanneer men het verbiedt. Dit terwijl bij de whitelist dit net andersom is. Men gaat hierbij uit van een algemene beperking en hetgeen op de whit list staat is volledig toegestaan en wordt ondersteund.

Tabel 4: Black - en whitelist

Black list	Whitelist
Men loopt als onderneming constant achterop	Men loopt vooruit
Men komt als onderneming verbiedend over	Minder restrictief

In KBC kan men dus met behulp van de Blackberry mails lezen en attachments openen. Maar andere zaken, zoals software installeren is niet toegestaan. Dit is een voorbeeld van wat wel en wat niet mag voor een bepaalde gebruiker. Sommige gebruikers, met meer rechten, mogen wel software installeren.

Verder zal KBC voor het beveiligen van zijn gebruikers met een Blackberry gebruik maken van de software die RIM hiervoor levert. In KBC bevindt er zich een server met Blackberry software, Blackberry Enterprise Server, die ervoor zorgt dat indien gebruikers een connectie met het netwerk willen maken dit gebeurt op een beveiligde manier. De transmissie van gegevens wordt beveiligd met behulp van een tunnel. Deze software zorgt dus voor het opzetten van een point 2 point tunnel.(eindpunt naar eindpunt) Zo zal geen enkele andere kwaadwillende de packets kunnen onderscheppen die worden verstuurd met behulp van een sniffer.

Natuurlijk wordt de Blackberry slechts beperkt gebruikt. Dit wil zeggen dat men geen uitgebreide software zal gaan draaien op een de kleine handheld. Men zal zich zoals eerder al aangehaald beperken tot een beperkte aantal toepassingen. Stel dat men uitgebreider wil 'thuis' werken, dan zal men de werknemer gebruik laten maken van een laptop. De filosofie van laptops verschilt wel met die van de Blackberry. Een Blackberry wordt bij KBC beschouwd als een uitbreiding. Men kan mails lezen en versturen, dit is de meest gebruikte toepassing. Maar een laptop vormt een uitbreiding. De laptop kan voor allerlei toepassingen worden gebruikt. De laptop maakt als het ware deel uit van het interne netwerk. Wanneer een ondernemer gebruik maakt van een laptop dan zal deze laptop zich gedragen als een ware client net als een desktop die binnen in de kantoren staat in een KBC vestiging. KBC zal de roaming van zijn gebruikers zeer serieus nemen en elke gebruiker kan met behulp van een laptop, op afstand dus, elke toepassing uitvoeren alsof deze binnen de 'premises' van KBC zit.

6.6.1 Het belang van opleiding en awareness

Zoals ik reeds hoger heb aangegeven in het hoofdstuk over policy is het ondersteunen van de gebruikers bij de implementatie van een policy onontbeerlijk. Dit werd ook benadrukt in het interview. Men kan met andere woorden zoveel mogelijk beveiligingsmaatregelen nemen als onderneming, ze zullen enkel effectief zijn wanneer de gebruiker ze respecteert en de beveiligingsmaatregelen in acht neemt. Daarom is het 'aware' maken van de werknemers nuttig.

In KBC zal men de werknemers aware maken met behulp van een aantal uren onderwijs daarin. Zo zullen de werknemers voldoende afweten van hoe en wat en waarom. Zo zullen werknemers niet langer gefrustreerd raken wanneer ze een voor de 'zoveelste keer' hun paswoord moeten ingeven, maar ze zullen begrijpen dat dit een doel heeft: het beschermen van de gegevens van de klant.

6.7 Conclusie case KBC

KBC houdt er een speciale aanpak van problemen op na. Deze aanpak is onder andere een resultaat van de schaal waarop KBC werkt. De onderneming kan anticiperen op bedreigingen, nog voordat ze zich voordoen. Het perimeter concept, de whitelist aanpak, de manier hoe men 'risks' inschat zijn daarvan voorbeelden.

Het strikte beheer, zoals men bij KBC toepast, van mobiele apparaten zoals laptops en pda's zorgt voor een veiligere omgeving. Men staat immers bij KBC niet toe dat werknemers zelf laptops, smartphones aanschaffen en gebruiken voor het werk. Men probeert op die manier te voorkomen dat confidentiële informatie op de onveilige mobiele apparaten terecht komt. Men zal de verantwoordelijkheid dan ook bij de gebruiker leggen (de werknemer) en niet bij de afdeling IT van de onderneming. Dit is cruciaal. De werknemer helpt in feite de onderneming te beveiliging. Hij is in feite de firewall.

7 Advies voor het beveiligingsbeleid van een onderneming bij implementatie van mobiele toepassingen op een Blackberry platform

7.1 Inleiding

De hoofdvraag in dit werk luidde als volgt: *'Hoe moet de organisatie haar beveiligingsbeleid aanpassen om tegenmoet te komen aan de nieuwe bedreigingen als gevolg van de technische evoluties? Meer bepaald, hoe moeten de policies binnen de onderneming worden aangepast?'*

In het kader van dit werk werd de aandacht gevestigd op het deelonderwerp: beveiliging van mobiele telefoons (meer bepaald smartphones). Met smartphones worden Blackberry toestellen geopteerd omdat deze vaak in een bedrijfsomgeving worden gebruikt (Lopez, Succesful Mobile Deployments Require Robust Security, 2009) en vermits deze toestellen beschikken over uitgebreide beveiligingsmogelijkheden.

Mobile computing is een interessante evolutie die zich voordoet, zoals uit hoofdstuk 3 al gebleken is. Daarna was het ook interessant om te kijken naar het volgende: *'Hoe moeten de policies binnen de onderneming worden aangepast, als gevolg van de evoluties in dit geval: mobile computing.'* Dit in combinatie met een aantal oplossingen welke de onderneming kan gebruiken om haar systemen te beschermen.

Het probleem wordt gestructureerd aangepakt. Eerst wordt er gekeken naar wat de problemen zijn met mobile mobile computing. In tweede instantie zal er worden gekeken, per probleem, wat een oplossing kan zijn zodat het probleem kan worden aangepakt. In het achterhoofd wordt gehouden dat dit moet worden geïmplementeerd in een professionele omgeving.

7.2 Een verandering in aanpak

In het verleden gingen bedrijven naar buiten kijken. Ze beschouwen het 'onbekende externe' als grootste bedreiging. (Hoffman, 2007) Men probeerde zoveel mogelijk barrières op te richten tussen de bedreiging en hetgeen men wilde beschermen. Maar dit is niet langer de juiste redenering. Door

de evolutie van mobile computing is dit niet langer de juiste aanpak. De onderneming moet haar manier van denken wijzigen. Volgens Hoffman (2007):

- Enterprises need to change their strategies from protecting only their LAN to putting policies and systems in place to protect the mobile devices.
- Enterprises need to put into place policies and systems to protect and control their data, wherever it may reside.

Er zijn twee cruciale wijzigingen nodig. Enerzijds de wijziging in strategie waarbij men ook de mobiele toestellen moet gaan incorporeren. Anderzijds moet er bij de ontwikkeling van een security policy worden van uitgegaan dat men data moet beschermen waar deze zich ook mag bevinden. Hoffman (2007) haalt tevens ook enkele redenen aan waarom deze wijziging alsnog niet heeft plaatsgevonden:

- Apathy. This one drives me nuts. Security personnel and executives understand the threat, realize it can be addressed, and do nothing.
- Common perception is that it's cheaper to do nothing than to address the threats.
- Mobility presents unique challenges that many enterprises simply do not know how to address.

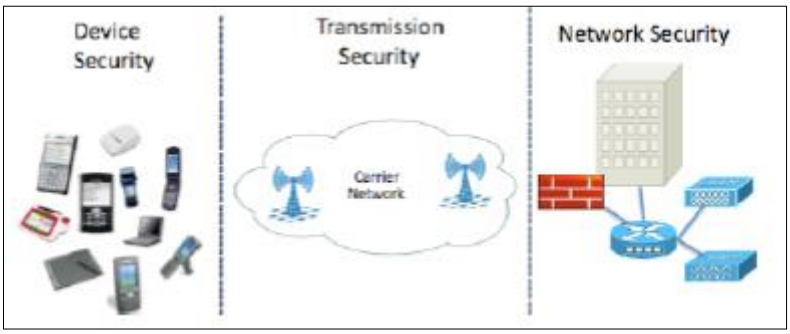
De onderneming moet nodig actie ondernemen en zorgen voor een verandering in mentaliteit enerzijds en een wijziging in strategie samen met de security policy anderzijds.

7.3 Deelproblemen en oplossingen

Het probleem kan worden opgesplitst in deelproblemen:

- lokale data en applicatiedata(statisch, vluchtige data behoort tot deelprobleem (3)), toegang tot het toestel en het digitaal leerplatform en applicaties op het toestel**(1)**,
- malware en hackers**(2),**
- datatransmissie**(3)**

Deze redenering is deels gebaseerd op de volgende figuur. (waar ook drie onderscheiden op te zien zijn) In ons geval zullen we als eerst het linker en centrale onderdeel van naderbij bekijken: lokale data, applicatiedata, applicaties en toegang tot het toestel (uiterst links) en datatransmissie (middenste deel).

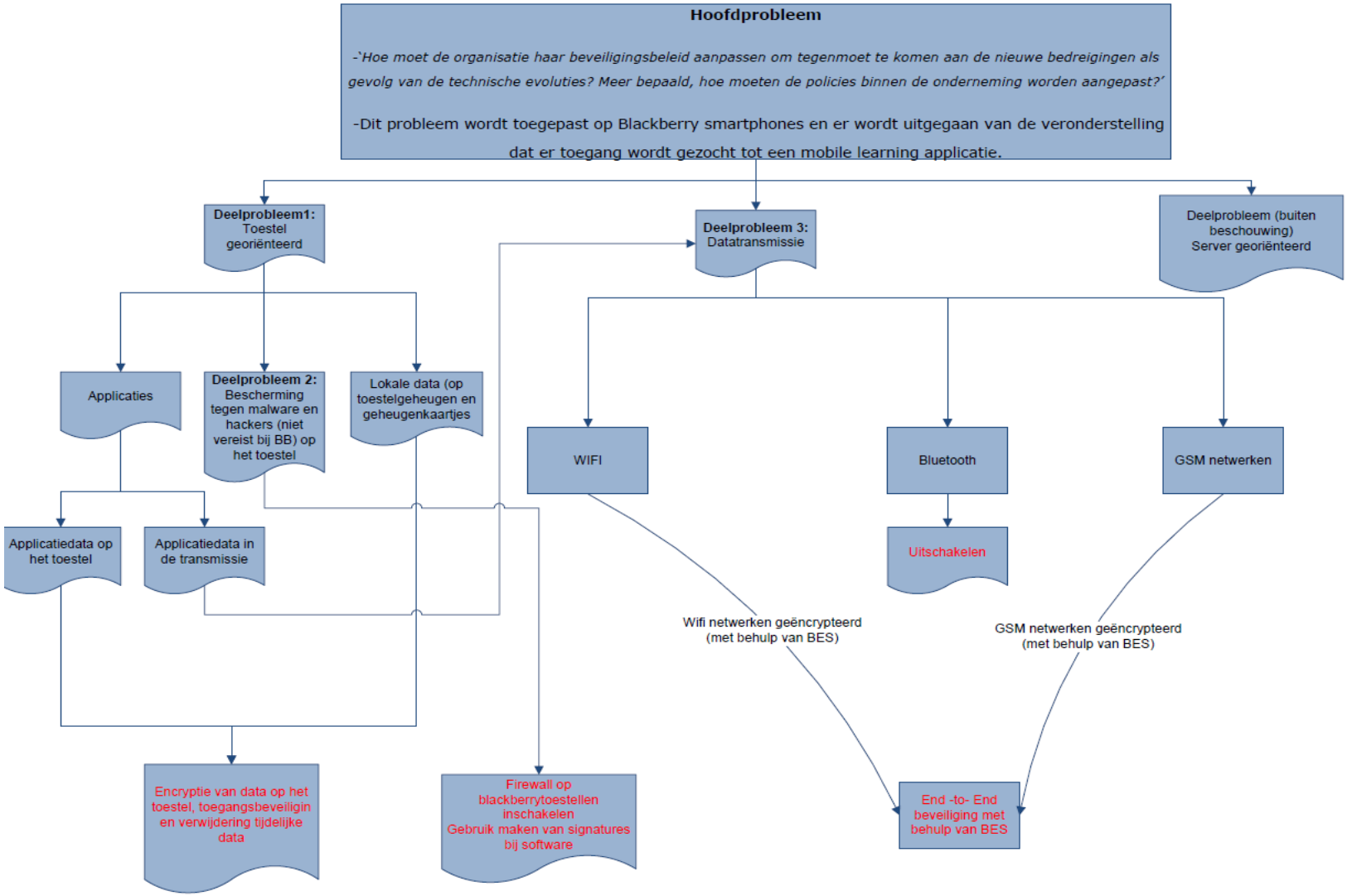


Figuur 21: De structuur die moet worden afgeschermd (Lopez, Succesful Mobile Deployments Require Robust Security, 2009)

Malware en hackers zullen ook worden behandeld maar op een andere manier, maar hierover later meer uitleg. Hierna gaan we kort kijken naar de aanpak van de applicaties op het mobiele toestel. Er wordt ook kort gesproken over de applicaties in deelprobleem 1.

Er is sprake van twee soorten data. Men heeft enerzijds de lokale data en de data op de servers (waartoe men toegang wil). Dit moet behandeld worden, want dit verschil is fundamenteel op het gebied van hoe men dit moet beveiligen. Men kan bij de data die beschikbaar is op de servers nogmaals een onderscheid maken, maar in feite is dit dezelfde data waarmee toegang wordt gezocht. Als de datatransmissie beveiligd is, dan is dat probleem ook opgelost.

In de volgende tabel kan u de aanpak van het hoofdprobleem vinden. U kan uit de tabel de opsplitsingen aflezen waarin het hoofdprobleem wordt opgedeeld samen met een korte uitleg van de oplossing. Wanneer u dit hoofdstuk zal lezen zal de oplossing per deelprobleem duidelijker worden. Deze tabel geeft een overzicht, ter verduidelijking. Tevens vindt u in figuur 22 een gestructureerd overzicht in de vorm van een schema van de verschillende problemen. De deelproblemen worden benoemd en uitgesplitst in subproblemen. De oplossingen worden kort in een rode kleur weergegeven.



Figuur 22: Probleemstelling

Tabel 5: Probleemaanpak

<table>
<tr><td colspan="7">Hoofdprobleem:
-‘Hoe moet de organisatie haar beveiligingsbeleid aanpassen om tegenmoet te komen aan de nieuwe bedreigingen als gevolg van de technische evoluties? Meer bepaald, hoe moeten de policies binnen de onderneming worden aangepast?’
-Dit probleem wordt toegepast op Blackberry smartphones en er wordt uitgegaan van de veronderstelling dat er toegang wordt gezocht tot een mobile learning applicatie.</td></tr>
<tr><td colspan="5">Toestel georiënteerd</td><td colspan="1">Deelprobleem 3:
Datatransmissie</td><td>Deelprobleem 4: Netwerk georiënteerd / Server georiënteerd</td></tr>
<tr><td colspan="3">Deelprobleem 2: Bescherming tegen malware en hackers.</td><td colspan="2">Deelprobleem 1: Data op het toestel</td><td>WiFi / GSM netwerken</td><td rowspan="3">Wordt buiten beschouwing gelaten.</td></tr>
<tr><td>Malware</td><td colspan="2">Hackers</td><td>Applicaties</td><td>Alle typen geheugens op BB-toestel</td><td rowspan="2">Maak gebruik van BES technologie voor het zorgen van end-to-end beveiliging

Meer uitleg in onderdelen:
7.6 en deelcategoriën

BES voorbeeld:
7.8.3.2 en deelcategoriën</td></tr>
<tr><td rowspan="2">Er moet indien de onderneming gebruik maakt van applicaties die digitaal werden ondertekend geen gebruik gemaakt worden van specifiek anti-virus protectie.

Opnemen van een whitelist, zoals bij KBC, is een goede oplossing.

Voorkomen dat software kan worden geïnstalleerd op de Blackberry toestellen.

Op tijd distribueren van updates.

Meer uitleg in onderdeel: 7.5 en deelcategorieën</td><td>Transmissie van data</td><td>Toegang tot het toestel</td><td rowspan="2">Dit is specifiek per applicatie, wordt algemeen behandeld.

Meer uitleg in onderdelen:
7.4;
7.4.2.1 en deelcategorieën;
7.4.3;
7.4.4;
7.8.4

BES voorbeeld:
7.8.3.1;
7.8.3.2 en deelcategorieën;
7.8.3.3</td><td rowspan="2">Maak gebruik van encryptie, (is aanwezig op de Blackberry toestellen) memorycleaning inschakelen.

Meer uitleg in onderdelen:
7.4.2.1 en deelcategorieën;
7.8.4

BES voorbeeld:
7.8.3.1;
7.8.3.3</td></tr>
<tr><td>Hackers voorkomen door gebruik te maken van VPN technologie bij transfers.

Meer uitleg in onderdelen:
7.5; 7.6 en deelcategorieën

BES voorbeeld:
7.8.3.1;
7.8.3.2 en deelcategorieën</td><td>Gebruik maken van goede beveiliging om toegang tot het toestel te voorkomen: oa. BB device firewall

Meer uitleg in onderdelen: 7.5 en deelcategorieën

BES voorbeeld:
7.8.3.1;7.8.4</td></tr>
</table>

7.4 Deelprobleem 1: De data, applicaties en applicatiedata op het toestel

7.4.1 Inleiding deelprobleem 1

De data op het toestel moet worden beschermd van kwaadwillende personen. Denk bijvoorbeeld aan de situatie waarbij een mobiel toestel wordt ontvreemd en belangrijke data op het toestel wordt gekopieerd zoals bijvoorbeeld agenda's, klanteninformatie,… Er moet een manier zijn ter beveiliging van de toegang tot de smartphone. Dit wordt meestal gedaan via het ingeven van een paswoord of PIN code. (Botha, Furnell, & Clarke, 2009) Zulk een beveiliging vormt een relatieve barrière maar ze is wel kraakbaar door een vindingrijke gisser van het paswoord. Men kan tevens ook een zogenaamde 'brute force attack' uitvoeren waarbij een programma alle mogelijke combinaties uitprobeert. Toch is het een vaak gebruikte manier van beveiligen, ze wordt ook gebruikt op desktop computers.

Een van de grootste verschillen met desktops is dat men een afweging moet maken. Wanneer men met een desktop computer werkt is het makkelijk een paswoord in te geven. Maar wanneer hetzelfde moet worden gedaan op een mobiel apparaat zoals een PDA kan dit wel eens een lastige taak zijn. Met andere woorden de authenticatie methode moet net zo makkelijk zijn als hoe vaak het wordt gebruikt. De authenticatie methode moet makkelijker zijn van aard indien ze vaak wordt gebruikt. (Botha, Furnell, & Clarke, 2009) Anders laat de consequentie zich al raden: de gebruikers gaan de beveiliging achterwege laten. Volgens een onderzoek door Clarke en Furnell (2005) werd er vastgesteld dat 34% van 297 ondervraagden geen gebruik maakten PIN beveiliging. Men geloofde dat er niet echt iets van waarde diende te worden beveiligd. Een andere vaststelling was dat indien er gebruik werd gemaakt van een PIN, deze PIN vaak ongewijzigd bleef tijdens de volledige gebruiksduur van het toestel. Zo bleek 42% van gebruikers de PIN niet te wijzigen. (Clarke & Furnell, 2005)

Er werd door de tijd gezocht naar een andere manier om een gebruiksvriendelijkere methode van beveiliging te vinden. Deze werd gevonden in de vorm van biometrische beveiliging. (Aufrieter, 2002) Een voorbeeld hiervan is dat de software 'kijkt' naar het handschrift van de gebruiker die probeert toegang te krijgen tot de PDA. De gebruiker zal een woord schrijven met behulp van een

stylus op het aanraakgevoelige scherm van de smartphone in kwestie en de software op de smartphone beoordeerld op basis van vorm en snelheid van het schrijven indien het de rechtmatige gebruiker is. Volgens een survey die werd gedaan in 2005 werd er vastgesteld dat gebruikers eerder een biometrische vorm van authenticatie prefereerden boven een PIN code of paswoord. Maar er bestond niet meteen een overeenkomst over welke soort: handschriftherkenning, irisscanning, stemherkenning,... (Clarke & Furnell, 2005)

Een andere manier van beveiliging is via een 'token'. (Aufrieter, 2002) Men kan bijvoorbeeld met behulp van een smart card toegang krijgen tot het toestel. Maar deze manier van authenticatie zou het toestel vergroten en verzwaren. Dit zijn twee grote contra's. En een derde contra is dat ook de token wel eens verloren kan gaan. Tevens het opzetten van een token structuur binnen de onderneming kan duur zijn. (Tsiantis, Stergiou, & Maragariti, 2007)

Dit was een verkenning van de mogelijkheden tot aanpak van het probleem. Nu zullen we overgaan geven van een oplossing voor het eerste deelprobleem.

7.4.2 Applicatiedata, toesteldata en data op geheugenkaartjes

Bij mobile learning applicaties wordt, indien nodig, data gedownload. Dit gebeurt immers ook bij andere mobiele applicaties. Dit zal in de vorm van geluidsfragmenten of andere content die nodig zodat de 'leerling' kan studeren (beluisteren of bekijken). Bij andere applicaties die een verbinding vereisen met het bedrijfsnetwerk, zoals webmail, wordt er een beperktere hoeveelheid data heen en weer gezonden. Er worden tevens ook geen of minder files lokaal opgeslagen: eventueel een bijlage kan worden gedownload en lokaal opgeslagen.

Mobiel leren maakt dus gebruik van twee typen data: statische data dewelke op het toestel na het sluiten van de applicatie achterblijft en vluchtige data die enkel over en weer wordt gezonden. Deze twee typen data moeten behandeld worden. Er moet in de beveiligingspolicy een oplossing gevonden worden voor de data op het systeem zelf en de transmissie van de data van de applicaties.

Omwille van de bovenstaande redenen is het nodig dat de onderneming alle geheugens op het toestel beveiligd met behulp van encryptie ofwel deze tijdelijke data verwijderd. Encryptie kan door

externe programma's worden gedaan of door ingebouwde mogelijkheden op het toestel, als die aanwezig zijn. Er moet ook voorzien worden in toegangsbeveiliging tot het toestel.

7.4.2.1 Voorkomen van stelen van data

Er zijn aldus 2 typen data die moet worden afgeschermd, afgeleid uit het vorige onderdeel:

- De statische lokale data en de tijdelijke lokale data: op geheugenkaartjes of geheugen van het toestel
- De data in de transmissie (wordt lager besproken) bij deelprobleem 3

Men moet als onderneming de toegang tot de toestellen afschermen om zo te voorkomen dat onbevoegden zomaar toegang hebben tot het toestel.

7.4.2.1.1 Toegang tot het toestel

Toegang tot het toestel kan op een aanvaardbare manier worden beveiligd met behulp van Blackberry Enterprise Server zoals blijkt uit Research In Motion (2010):

"The Blackberry Enterprise Solution extends corporate security to the wireless device and provides administrators with tools to manage this security. To secure information stored on Blackberry smartphones, password authentication can be made mandatory through the customizable IT policies of the Blackberry® Enterprise Server. By default, password authentication is limited to ten attempts after which the device's memory is erased.

Additionally, system administrators can create and send wireless commands to remotely change Blackberry smartphone passwords and lock or delete information from lost or stolen Blackberry smartphones."

De toegang kan worden beveiligd met behulp van een paswoord. Tevens kan met behulp van de IT policy alle data worden beschermd door middel van encryptie toe te passen. Indien de situatie zich voordoet kan op afstand de data van het toestel zelfs worden verwijderd opdat de data niet in de foute handen terecht komt.

7.4.2.1.2 Het uitlezen van data

Voor de data die men enkel 'uitleest' kan men een regel opnemen in de vertrouwelijkheidspolicy (een voorbeeld vindt u in bijlage 1), dit is een policy die gebruikers van de systemen verplicht zijn te volgen. Bijvoorbeeld: de data mag niet gedeeld worden met derden of op enig andere manier openbaar worden gemaakt (zo mogen er bijvoorbeeld geen printscreens worden genomen). De gebruiker is in dit geval de firewall. Hij vormt de buffer die moet voorzien dat hij geen data openbaar maakt of lekt. KBC past dit systeem ook toe. De onderneming kan immers niet ten allen tijde voor de bescherming van haar gegevens zorgen. Dit zou een onmogelijke situatie zijn. Ze moet een deel van de verantwoordelijkheid bij de gebruikers leggen.

7.4.2.1.3 Tijdelijke data op het toestel

Meestal bewaart de gebruiker weinig op het toestel, althans niet bewust. Maar er zal meer data achterblijven op een toestel dan de gebruiker kan vermoeden. Zo zijn er tijdelijke bestanden en er zijn bestanden die hij downloadt. (Research In Motion, 2010) In beide gevallen is er een beveiliging vereist.

Tijdelijke bestanden, de statische data, kunnen worden beschermd met behulp van encryptie van het geheugen van de toestellen. Dit kan door middel van een applicatie te installeren op het toestel, of kan op een Blackberry worden bekomen door dit zo te configureren. (deze optie is immers al aanwezig maar is niet ingeschakeld) Deze applicatie zal het geheugen encrypteren. Met behulp van de Blackberry security policy kan worden afgedwongen dat deze applicatie wordt geïnstalleerd op het Blackberry toestel alvorens hij verbinding maakt met het bedrijfsnetwerk. (Research In Motion, 2010) Meer nog, er kan worden afgedwongen dat er in combinatie met de mobile learning applicatie een encryptieapplicatie aanwezig moet zijn op het toestel. Op dezelfde manier kunnen andere bestanden, zoals pdf's, worden beveiligd. Tevens kan met behulp van de Blackberry internet service worden afgedwongen dat tijdelijke bestanden worden verwijderd. Deze functie kan worden ingeschakeld op het Blackberry toestel. In de volgende tabel vindt u een uitgebreide beschrijving.

Tabel 6: Memory cleaning (Research in motion, 2010)

Memory cleaning is designed to delete sensitive data from the temporary memory on your Blackberry® device. Examples of sensitive data include sensitive data in the cache for the key store browser, unencrypted data from email messages, LDAP authentication passwords, and data from certificate and key searches. When memory cleaning is turned on, the memory cleaning application is designed to delete sensitive data automatically in the following situations: • when you insert your device in a holster • when you do not use your device for a specified period of time • when you synchronize with your computer • when you change the time or the time zone for your device • when you lock your device

Om de bestanden op het toestel te beschermen, diegene die niet tijdelijk zijn, moet encryptie worden ingeschakeld. Sommige harde schijven zullen encryptie in de hardware al gebakken hebben, zoals bijvoorbeeld in het artikel van Moor (2008) werd aangetoond. Diegene die het mobiele toestel dan onrechtmatig ter zijner beschikking heeft zal dan niet aan de gegevens op de harde schijf of het geheugen raken. Als dat niet voor handen blijkt te zijn kan men te allen tijde gebruik maken van het encrypteren van de data die tijdelijk beschikbaar moet zijn. Er zijn talloze fabrikanten die zulke encryptiesoftware aanbieden die dit doet. Een voorbeeld daarvan is PGP. (PGP, 2010) Fabrikant Research In Motion (2010) zal extra inspanning doen wat de encryptie betreft: *"Local encryption of all data (messages, address book entries, calendar entries, memos and tasks) can also be enforced via IT policy. And with the Password Keeper, Advanced Encryption Standard (AES) encryption technology allows password entries to be stored securely on the device (e.g., banking passwords, PINs, etc.)."* Zo wordt het voor een kwaadwillende al heel wat moeilijker om gevoelige informatie te bekomen.

7.4.2.1.4 Het verwijderen van het toestel

Wanneer het toestel wordt verwijderd moet men als onderneming er ook zeker van zijn dat de data definitief verwijderd is. Dit moet in de vertrouwelijkheidspolicy worden opgenomen. Afgedankte toestellen moeten door de afdeling die daarvoor bevoegd is volledig vrijgemaakt worden van gegevens. Een voorbeeld van zulk een policy kan in bijlage 1 worden gevonden.

7.4.3 Ongewenste applicaties of out-dated applicaties op het toestel

De applicaties die op het toestel al dan niet kunnen worden geïnstalleerd kunnen ook voor problemen zorgen. Zo kunnen sommige applicaties niet up-to-date zijn of zo kunnen er zich op het toestel applicaties bevinden die er niet thuishoren. Dit probleem kan worden opgelost door het invoeren van een zogenaamde whitelist. Op deze whitelist staan een aantal applicaties welke toegelaten zijn. Alle andere applicaties worden niet toegestaan op het toestel. Dit is tevens de aanpak die bij KBC ook wordt toegepast.

Indien het toestel beschikt over een applicatie die niet up-to-date is kan de men beslissen in de policy om het toestel beperkte rechten te geven zolang de applicatie niet up-to-date is. Vanaf het moment dit gecorrigeerd is beschikt het toestel terug over volledige capaciteiten.

U vindt een verdere uitleg over dit onderdeel 7.8.3.3 over de applicaties op het toestel.

7.4.4 De toegang tot de mobile learning applicatie

Zoals al eerder aangehaald in dit werk:'*Wanneer men gebruik maakt van een mobile learning systeem, dan is men als gebruiker geïnteresseerd in twee kernpunten met betrekking tot beveiliging: authenticatie en privacy.* ' (Tsiantis, Stergiou, & Maragariti, 2007) Het is van belang dat men de toegang tot de applicaties beveiligd. In dit geval werd er een uitvoerige bespreking gedaan over dit topic in hoofdstuk 5.2.7.3.1: mobile learning applicatie en de toegang tot dit soort applicaties beveiligen.

7.5 Deelprobleem 2: Bescherming tegen malware en hackers

7.5.1 Inleiding deelprobleem 2

Twee grote problemen die voorkomen zijn: malware, hackers. Hoe kunnen deze problemen worden vermeden?

Malware kan te allen tijde geïntroduceerd worden, via het netwerk of via het toestel zelf, en men moet hierop voorbereid zijn. Het installeren van een virusscanner en firewall op het toestel kan een oplossing bieden. Het probleem is dan wel dat men als gebruiker een afweging moet maken tussen

'processorkracht' die gebruikt wordt ter beveiliging van het toestel en batterij die gebruikt wordt daarvoor, zoals eerder reeds aangegeven.

De onderneming moet ook het probleem van hacken via bluetooth in het oog houden. Volgens Munro (2008): *"Research has highlighted the possibility of hacking Bluetooth devices regardless of which mode they are in. It has also demonstrated that an attacker can pair an external device with a target using no more than a patched dongle and some doctored software."* Ook hierop moet een oplossing worden gevonden, deze optie uitschakelen is aan te raden.

7.5.2 Aanpak deelprobleem 2

De oplossing voor malware is volgens Research In Motion (2010): *"The Blackberry solution focuses on containing malicious programs. The Blackberry software and core applications are digitally signed to ensure integrity and control access to the Application Programming Interfaces (APIs). Thus, the core Blackberry functionality cannot be directly accessed by other applications.*

You can use the application controls on your Blackberry device to prevent the installation of specific third-party applications and to limit the permissions of third-party applications."

De oplossing van Blackberry focust dus op het voorkomen van malicious code en programma's door zoveel mogelijk gebruik te maken van programma's die eerst goedgekeurd werden. Blackberry maakt gebruik van een digitale handtekening. Aan de hand van deze handtekening kan men vaststellen indien het al dan niet een veilig programma is om te installeren. Men kan ook gebruik maken, als systeem administrator, van de controle om te voorkomen om applicaties te installeren en dus ook malicious code te vermijden op de toestellen.

Alvorens we een oplossing geven voor hacking moeten we vaststellen via welke wegen het toestel kan benaderd worden door een hacker. Er kan worden gehackt via een drietal toegangswegen:

- Fysische aanwezigheid aan het toestel
- Bluetooth
- Andere manieren van connectie: GSM netwerken, WiFi verbinding

Toegang tot het toestel werd eerder al behandeld in onderdeel 7.4.2.1.1. Men kon concluderen dat er voldoende beveiliging aanwezig moest zijn opdat men makkelijke toegang aan kwaadwillenden kan ontzeggen.

De twee eerste delen (fysische aanwezigheid en bluetooth) worden verholpen door middel van de device security policy zoals u later kan terugvinden in dit werk. U kan dit voorbeeld terugvinden onder hoofdstuk 7.8.2. Bluetooth wordt hier ook aangepakt, de beste optie is gewoon de functie uitschakelen.

Door Research In Motion wordt ook de optie gegeven de smartphone te beschermen met behulp van een firewall. Deze firewall heet de Blackberry device firewall. Deze kan worden ingeschakeld opdat het toestel meer beschermd zou zijn tegen aanvallen van buitenaf.

De transmissiebeveiliging wordt verder behandeld in het volgende deelprobleem.

7.6 Deelprobleem 3: Transmissie data

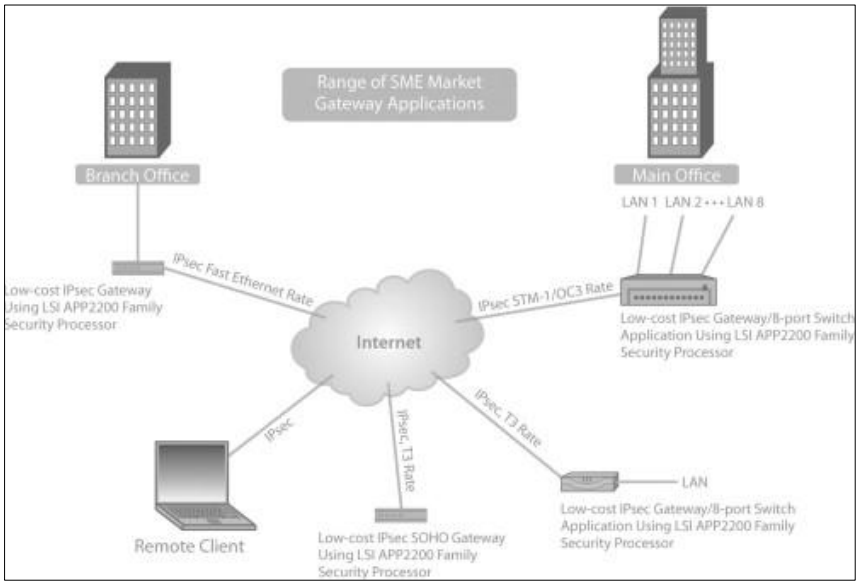
7.6.1 Inleiding deelprobleem 3

De datatransmissie is het derde deelprobleem. De onderneming moet niet enkel de toestellen zelf beveiligen, maar ook de transmissie tussen de toestellen en het bedrijfsnetwerk. Hackers kunnen, als deze verbinding niet goed beveiligd is, data onderscheppen. Hacking wordt uitgesloten wanneer er een veilige tunnel wordt gecreëerd van de Blackberry naar het bedrijfsnetwerk. De hacker kan in dat geval enkel inbreken op het systeem door fysiek het systeem in zijn bezit te hebben en het zo te proberen kraken, dit is reeds beschreven in deelprobleem 1. De andere manier van hacken is een aanval via het netwerk. Maar wanneer men een tunnel opzet, zoals lager beschreven zal worden, is men als onderneming veiliger. Met behulp van zulk een tunnel kan men een VPN bouwen, Virtual Private Network. (Harmon, 1997)

Gebruikers zullen soms gebruik maken van onveilige draadloze accesspoints wanneer ze zich niet achter hun bureau bevinden. Het is daarom cruciaal dat de verbinding die wordt opgezet veilig is. Stel dat dit niet mogelijk is, moet best voorkomen worden dat men verbinding kan maken. Dit kan in de beveiligingspolicy worden opgenomen. Maar soms wordt deze optie niet verkozen.

7.6.2 Aanpak deelprobleem 3

Wanneer men toch gebruik maakt van onveilige verbindingen, dan kan men een zogenaamde veilige tunnel opzetten opdat er een veilige verbinding wordt gecreëerd met het bedirjfsnetwerk. Zo kan de transmissie data end – to – end worden beveiligd. In de volgende afbeedling vindt u een voorbeeld waar op IPsec gebaseerde tunnels worden geïntegreerd. (Mojtahed & Xirasagur, 2009) Zo kan men de mobile learning applicatie beveiligen, vermits de connectie wordt beveiligd op die manier. In de figuur worden alle connecties in de wolk, die het internet of een ander soort WAN voorstelt, beveiligd met behulp van IPsec.



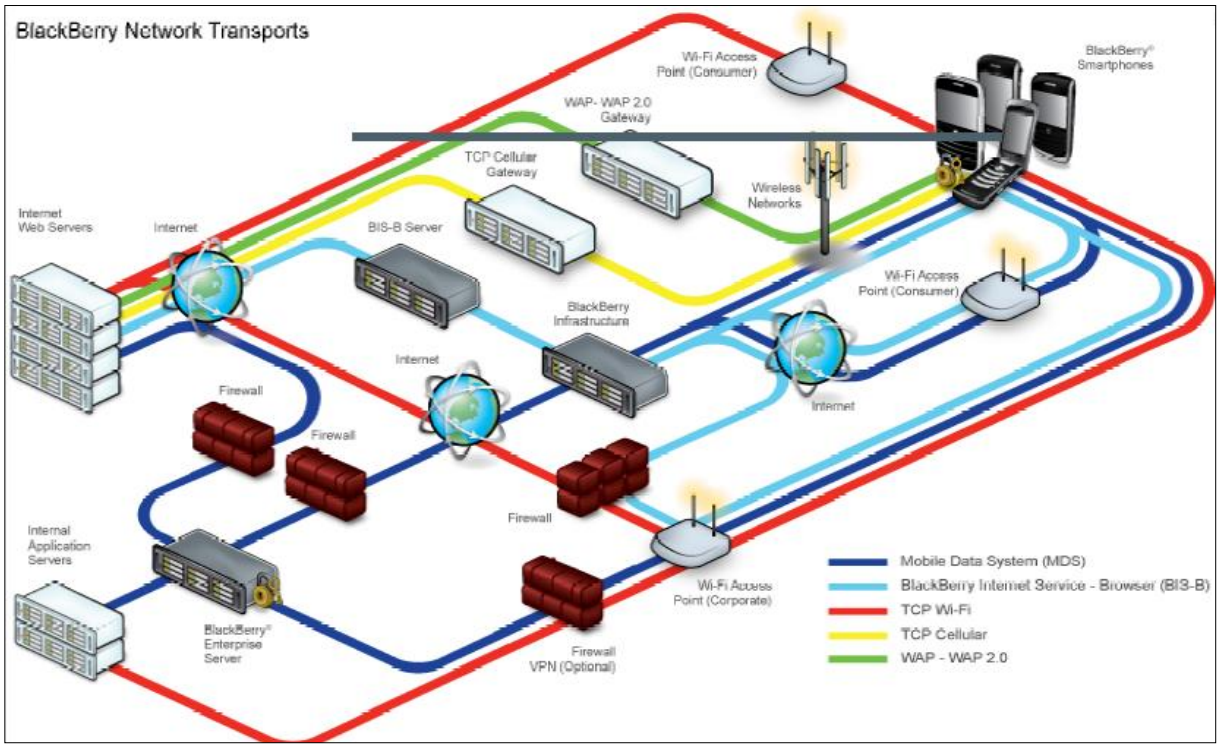
Figuur 23: *IPsec in enterprise applications*

IPsec verzorgt de volgende 4 eigenschappen opdat de verbinding zeker veilig is (Mojtahed & Xirasagur, 2009):

- De gegevens worden confidentieel gehouden
- De integriteit van de gegevens wordt verzekerd
- De gebruikers worden geauthoriseerd en geauthenticeerd
- Anti-replay beveiliging moet aanwezig zijn

Deze IPsec-technologie kan ook worden toegepast voor draadloze verbindingen van verschillende typen en lost op die manier een cruciaal probleem op: beveiligen van meerdere typen netwerken.

U ziet de verschillende typen netwerken welke moeten worden beveiligd in deze onderstaande figuur.

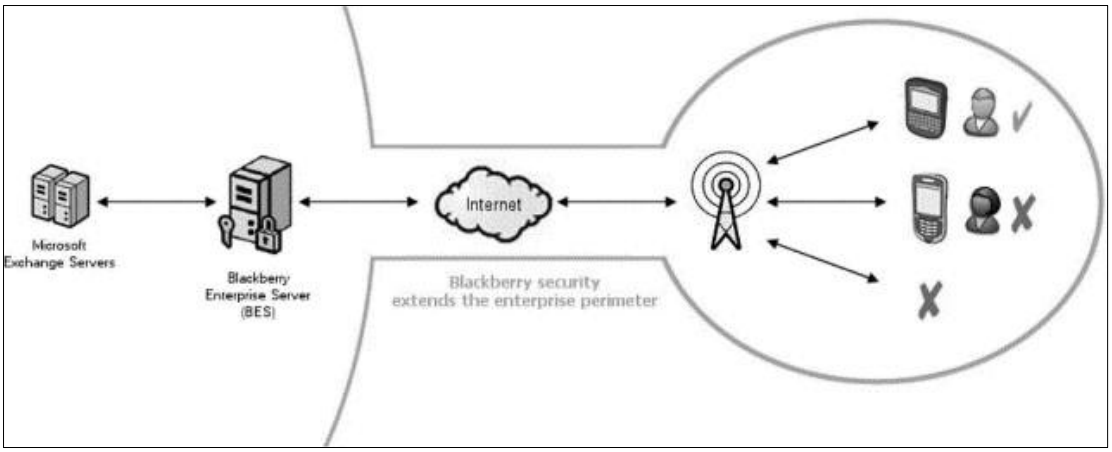


Figuur 24: Meerdere typen netwerken (Research In Motion, 2010)

Wanneer een mobiel toestel verbinding maakt met het bedrijfsnetwerk vanop afstand, dan kan dit dus via verschillende typen netwerken. Het toestel kan gebruik maken van een WiFi-verbinding, een 3G-verbinding,… Een van de kenmerken welke deze netwerken gebruiken is dat ze allen gebaseerd zijn op het internet protocol. Elk IP-netwerk(internet protocol) kan gebruik maken van IPsec protocol ter beveiliging. (Mojtahed & Xirasagur, 2009) De verschillende netwerken waarmee connectie kan worden gemaakt zijn: TCP (WiFi), TCP(cellular), WAP(of WAP2.0). (Research In Motion, 2009) Al deze manieren van toegang tot het netwerk moeten worden beveiligd. Dit is een aanzienlijke uitdaging voor de IT-afdeling binnen de onderneming. Maar met BES, Blackberry Enterprise Server, kan dit probleem aangepakt worden. Daarom werd ook gekozen een voorbeeld implementatie te maken met behulp van BES. U vindt deze lager terug in onderdeel 7.8.2.

Research In Motion zal de transmissie van gegevens beschermen met behulp van Blackberry Enterprise Server. Deze software zorgt voor het opzetten van een tunnel gecreëerd beschreven door Majtahed & Xirasagur (2009). Op die manier zorgt de Blackberry Enterprise Server voor een uitbreiding van het veilige netwerk zoals aangegeven in de onderstaande figuur. BES zorgt voor

een verwijding van de zogenaamde perimeter. De perimeter, waarvan er sprake was in het interview met KBC, is nu inclusief het Blackberry toestel.



Figuur 25: Secure perimeter door Blackberry Enterprise Server (Research In Motion, 2010)

De verdere implementatie van de draadloze beveiligingen kan u vinden in het onderdeel transmission security, 7.8.3.2.

7.7 Conclusie beveiligingsconcepten deelproblemen

Dit was een bespreking van de achterliggende beveiligingsproblemen en concepten waarmee de onderneming geconfronteerd wordt wanneer ze een mobiel leerplatform wil implementeren in de onderneming en in combinatie van smartphones wil gebruiken. Het probleem bestaat uit drie deelproblemen: de data en de applicaties op het toestel, bescherming tegen malware en hackers en het transmissieprobleem. De verschillende problemen werden aangekaart en er werd een oplossing aangereikt, dewelke in het algemeen een uitkomst biedt.

In het volgende onderdeel zal er een voorbeeld worden gegeven hoe de onderneming een veilige implementatie kan verwezenlijken van een (leer)applicatie in combinatie met BES Express, exchange server, een blackberrytoestel en Windows Server 2003.

7.8 Een uitgewerkte mobiele security policy

7.8.1 Inleiding uitwerking mobiele security policy

Het doel van dit onderdeel is een implementatie te maken van een server die de veilige verbinding verzorgt met mobiele toestellen, in dit geval een Blackberry Curve. De keuze voor het Blackberry georiënteerde omgeving werd gemaakt omdat grote bedrijven, zoals KBC, hiervan ook gebruik maken. In de literatuur werd al aangetoond dat Blackberry toestellen een zeer groot arsenaal aan mogelijkheden hebben om een veilige connectie te maken. Tevens werd in de literatuur ook gevonden dat Blackberry toestellen 'van nature' veiliger zijn. (Lopez, 2009) Er is ook niet meteen nood aan virusscanners op de de Blackberry toestellen net omdat ze reeds veilig zijn. Dit bespaart tevens ook processing power en batterijverbruik, twee bronnen die beperkt voor handen zijn. Met het oog op het opzetten van een professionele omgeving leek de keuze voor RIM omgeving dan ook logisch.

Lopez (2009) stelde *: "RIM has built three levels of security into the product consisting of:1) security within the device, 2) a secure connection between the device and the BES and 3) a secure connection between the BES and the NOC"* Het probleem van de drielaagse beveiliging wordt op die manier reeds aangepakt. Met behulp van de RIM architectuur wordt er een drielaagse beveiliging voorzien:

- De data op het toestel en de applicatiedata, applicaties (deelprobleem 1),
- Deelprobleem 2 hoeft niet meteen behandeld te worden omdat Blackberry toestellen van nature uit veilig zijn en hiervoor al een oplossing hebben: het digitaal ondertekenen van programma's zoals besproken in 7.5 de firewall op het toestel moet worden ingeschakeld,
- De datatransmissie wordt ook behandeld(deelprobleem 3)

Tevens wordt door Blackberry Enterprise Server ten allen tijde aan drie basisprincipes binnen beveiliging voldaan, dewelke eerder reeds werden aangehaald in dit werk. U vindt deze in de volgende tabel samen met de manier hoe de BES dit aanpakt.

Tabel 7: De basisprincipes beveiliging binnen BES voor Microsoft Exchange Server. Overgenomen: (Research In Motion, 2010)

Principles	Description
confidentiality	The Blackberry Enterprise Solution uses symmetric key cryptography to help make sure that only intended recipients can view the contents of email messages.
integrity	The Blackberry Enterprise Solution uses symmetric key cryptography to help protect every email message that the Blackberry device sends and to help prevent third parties from decrypting or altering the message data. Only the Blackberry Enterprise Server and Blackberry device know the value of the keys that they use to encrypt messages and recognize the format of a decrypted and decompressed message. The Blackberry Enterprise Server or Blackberry device reject a message automatically that is not encrypted with keys that they recognize as valid.
authenticity	Before the Blackberry Enterprise Server sends data to the Blackberrydevice, the Blackberry device authenticates with the Blackberry Enterprise Server to prove that the Blackberry device knows the device transport key that is used to encrypt data.

Op deze manier wordt vertrouwelijkheid, integriteit en authenticiteit van de gegevens te allen tijde gewaarborgd.

7.8.2 Uitwerking

In dit onderdeel vindt u een volledig gedetailleerd uitgewerkt praktijk voorbeeld waarvan gebruik wordt gemaakt van de volgende software pakketten:

- Microsoft Windows 2003 Server Enterprise
- Microsoft Exchange Server 2003
- Research In Motion Blackberry Enterprise Server Express
- Symantec forefront security 2010 (firewall en anti-virus) for exchange server

Als opmerking bij dit onderdeel: in bijlage 4 vindt u een handig schema met daarop de deelproblemen en de plaats waar u de oplossing vindt in dit werk. Zo heeft u een overzicht naast tabel 5.

De bedoeling is zo veilig mogelijk te werken in een professionele omgeving. De server omgeving, Microsoft Windows 2003 Server Enterprise R2, wordt buiten beschouwing gelaten. Hetzelfde geldt voor Microsoft Exchange Server 2003 omdat dit te ver zou gaan in het kader van dit werk. Deze

worden op een zo veilig mogelijke manier opgezet, maar er zijn werken die hier gedetailleerder op ingaan. Dit valt buiten het bestek van dit werk.

Een van de voordelen van deze setup is dat de Blackberry Enterprise Server kan worden geïntegreerd met de Active Directory van Microsoft Windows 2003. Dit betekent dat gebruikers die reeds een account hebben om toegang te krijgen via hun desktop tot het computer domein, deze account ook kunnen gebruiken om op afstand verbinding te maken via hun Blackberry toestel. Dit is een win-win situatie voor zowel de gebruiker als voor de onderneming zelf. De gebruiker moet immers slechts 1 paswoord onthouden en voor de onderneming kunnen gebruikers simpel via de active directory van Windows Server beheerd worden.

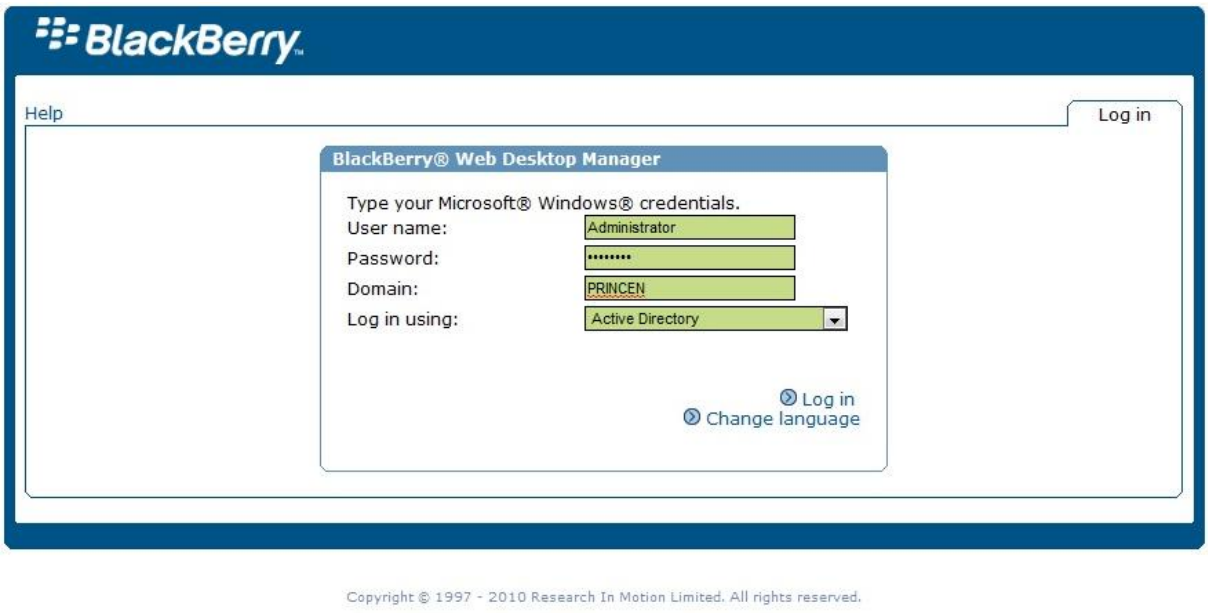
Active directory is een eigen implementatie van het LDAP protocol. Dit is een zeer veilig systeem en wordt in bedrijfsomgevingen die met Microsoft Windows werken vaak toegepast. Active directory zorgt voor grotere flexibiliteit en een gereduceerde total cost of ownership. (Microsoft, 2002) Volgens Microsoft (2002) zorgt het systeem ook voor een betere veiligheid*: "Additional security features make it easier to manage the multiple forests and cross-domain trusts. Cross forest trust provides a new type of Windows trust for managing the security relationship between two forests—greatly simplifying cross-forest security administration and authentication."* Dit draagt dus bij tot totale veiligheid van het in deze case geïmplementeerde systeem en zorgt ervoor dat er makkelijk mee gewerkt kan worden.

7.8.3 Blackberry Configuratie

De BES kan makkelijk worden ingesteld met behulp van webdesktop admin. U vindt daarvan een screenshot in de volgende figuur.

Figuur 26: Webdesktop Admin

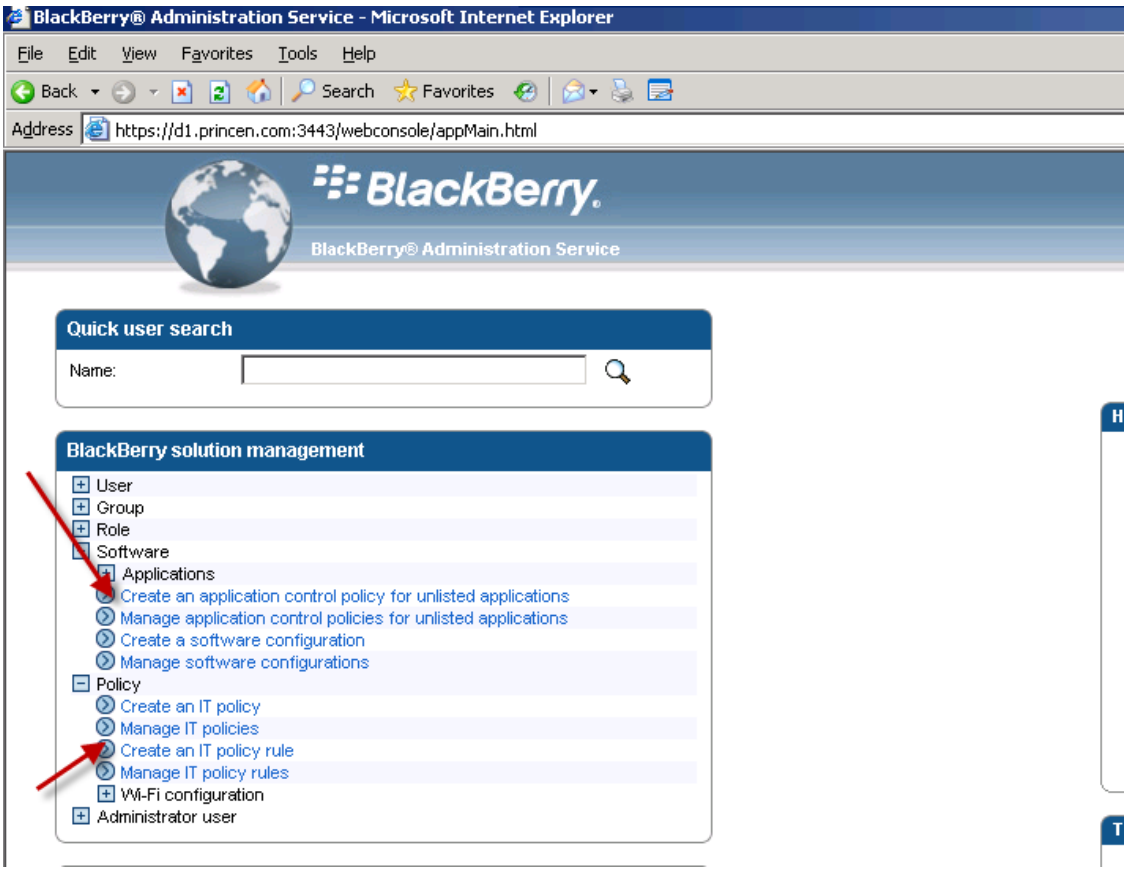
De gebruiker zelf kan makkelijk inloggen met behulp van het volgende scherm in de volgende figuur. Dit scherm kan worden benaderd met behulp van de mobiele browser.



Figuur 27: Het inlogscherm voor de gebruiker

Ik zal nu overgaan tot het bespreken van de configuratie van de beveiligingspolicy. Conform aangetoond in de specifieke probleembeschrijving (hoger) moet er een drielaagse implementatie zijn van de beveiliging: het toestel, de transmissie en de netwerkbeveiliging. Blackberry Enterprise Server laat dit ook toe. BES verzorgt de configuratie van het toestel en zorgt ook voor de beveiliging van de transmissie. De bedrijfsservers dienen door een ander systeem te worden beveiligd.

Blackberry Enterprise Server maakt een onderscheid tussen het toestel en de applicaties die op het toestel geïnstalleerd staan. Zo kan men applicatiespecifiek gaan werken, hetgeen voor sommige ondernemingen wel cruciaal is vermits verschillende applicaties verschillende eisen hebben. Sommige applicaties hebben immers geen toegang tot het netwerk nodig. Waarom zou deze dan ook toegelaten moeten worden? Zulke problemen kan men behandelen met behulp van de applicatie specifieke policy. U kan deze benaderen via de verschillende tabs, dit kan u vaststellen in de volgende figuur.



Figuur 28: Onderscheid applicatie policy en device policy

Zoals u ook kon vaststellen uit de probleembeschrijving moet de transfer van gegevens ook beveiligd worden. Ook hiervoor is er een aparte policy. BES organiseert de beveiliging voor de transfer van gegevens ook apart. Maar hierover later meer.

7.8.3.1 Device security policy

U vindt een screenshot van de device security policy in de volgende figuur terug. De device security policy zal de meeste zaken behandelen die nuttig zijn in het kader van dit werk zoals bluetooth, camera,enz. Ik zal nu overgaan tot de uitleg van de regels. De belangrijkste delen van de security policy worden in tabellen in het rood weergegeven.

De naam van de security policy: 'Algemeen'. Vermits ik slechts met een klein aantal toestellen werk in het voorbeeld.

U kan de hoofdopties, dewelke kunnen aangepast worden, aflezen bovenaan in de volgende figuur. Ik zal de belangrijke onderdelen bondig uitleggen.

Figuur 29: Regels

Achtereenvolgens zal: bluetooth, camera, common, device only, email messaging, password, S/MIME application, security, user defined, VPN, VoIP, Wi-Fi, Wired Software Updates en Wireless Software Upgrades worden besproken.

Tabel 8: Bluetooth

Bluetooth:
DISABLED

Volgens Potter (2004) bevat bluetooth toch wat kwetsbaarheden. De voordelen van bluetooth zijn miniem. Daarom wordt bluetooth uitgeschakeld.

Tabel 9: Camera

Camera:	
Photo Camera:	NOT DISABLED
Video Camera:	NOT DISABLED

Er is hier niet meteen een gevaar voor het informatiesysteem met betrekking tot de camera van het Blackberry toestel. Daarom wordt deze dan ook niet uitgeschakeld.

Tabel 10: Common

Common:	
MMS:	DISABLED

MMS wordt uitgeschakeld. Zo kan er via deze weg geen informatie worden gelekt. Bij KBC werd aangehaald dat er op talloze manieren data kan worden gelekt. Het lekken van data wordt op die manier geminimaliseerd. (Van den Driessche, When data goes up and out: Data Leakage Prevention in a Financial Organisation, 2009)

Tabel 11: Device only

Device only:	
Password required:	YES
Minimum password length:	6
User can disable password:	NO
Maximum Security timeout:	10 (minutes)
Maximum Password age:	30 (days)
User can change timeout:	NO
Password Pattern Checks:	At least 1 upper-case alpha, 1 lower-case alpha,
Allow SMS:	NO

Er moet voor toegang tot het toestel best een paswoord worden gebruikt opdat dit soort risico wordt uitgesloten. De minimale lengte van het paswoord wordt ingesteld op 6. Er wordt hier best een afweging gemaakt tussen de lengte (meer karakters is veiliger) en gebruiksgemak (korter is makkelijker). De gebruiker krijgt niet de macht om het paswoord uit te schakelen. Deze optie is dan ook uitgeschakeld.

Tevens wordt er ook een security timeout ingesteld. De security timeout staat in voor het opnieuw vragen van een paswoord na inactiviteit. Deze werd ingesteld op een redelijk niveau: 10 minuten. Maandelijks wordt er een nieuw paswoord vereist. Volgens KBC kan er data lekken uit het informatiesysteem. Dit moet zoals eerder al aangegeven worden geminimaliseerd. Zo kan er worden geredeneerd indien de SMS functie wordt uitgeschakeld, de kans op het lekken van

informatie wordt geminimaliseerd. Er kan dan wel in vraag worden gesteld waarom het toestel wel wordt gebruikt vermits MMS en SMS geadviseerd wordt uitgeschakeld te worden. De onderneming kan, indien de werknemers hierop aandringen, toch beslissen om de functie in te schakelen. Maar de meest veilige optie is het uitschakelen van deze twee.

Tabel 12: Password

Password:	
Set Password Timeout:	10
Set Maximum Password Attempts:	3
Set Maximum Password Echo:	NO
Maximum Password History:	3
Forbidden Passwords:	/

Na een drietal keer wordt de gebruikersaccount uitgeschakeld. Als gebruiker mag men maximaal 3 keer een fout paswoord ingeven. De gebruiker wordt dan voor 10 minuten weerhouden tot toegang tot de server.

Met password echo wordt bedoeld dat er op het toestel de karakters worden weergegeven van het paswoord. Nu deze is uitgeschakeld wordt het paswoord voorgesteld met behulp van asterixen. Zo kunnen geen onbevoegden meekijken.

Met behulp van de password history wordt ingesteld in welke mate men zijn paswoord kan herhalen. Deze werd ingesteld op 3 keer. Dit betekent dat de laatste drie paswoord verschillend moeten zijn.

Met behulp van de laaste regel kan er een aantal verboden paswoorden worden opgegeven. Dit wordt leeg gelaten. Hier kan indien dat nodig mocht zijn de naam van de gebruiker worden ingegeven om op die manier simpele paswoorden te voorkomen.

Tabel 13: S/MIMI Application

S/MIME Application:	
S/MIME Force Encrypted Messages:	YES
S/MIME Allowed Content Ciphers:	AES(256-bits)

S/MIME is een manier om e-mail berichten te encrypteren, het is een uitbreiding van MIME. MIME, Multipurpose Internet Mail Extensions, is een manier om formats van bestanden te beschrijven. (Panko, 2005) Deze manier van encryptie gebeurt op basis van een publieke sleutel.

AES, advanced encryption security, is een encryptiemechanisme. Ik heb in dit geval gekozen voor sterkste vorm die kon worden ingesteld van deze manier van encrypteren, 256-bits.

Tabel 14: Security

Security:	
Disallow third Party Application Downloads:	YES
Force Lock When Holstered:	NO
Content Protection Strength:	Strongest
Disable IP Modem	/
Disable External Memory:	NO

External File System Encryption Level Required Password Pattern: Encrypt to User Password and Device Key	/
Required Password Pattern:	/
Encryption On On-Board Device Memory Media Files:	Required

Er wordt niet toegelaten om applicaties van derden te downloaden. Zo kunnen ongewenste applicaties vermeden worden. Wanneer de Blackberry in een houder wordt gezet, zal het toestel automatisch worden gelocked opdat een toevallige passant niet toegang kan verkrijgen tot het toestel. De encryptie die dan voor de content van het toestel wordt toegepast is ingesteld op het 'hoogste' niveau.

Extern geheugen wordt niet uitgeschakeld omdat gebruikers hun geheugen wel eens wensen uit te breiden. De geheugenkaartjes worden wel met onder andere het gebruikerspaswoord beveiligd. Het on-board geheugen wordt 'vereist ' te worden geëncrypteerd.

Tabel 15: VPN

VPN:	
VPN User Name:	xxxx
VPN User Password:	xxxxxxxxxxx

Hierbij wordt de gebruikersnaam en het paswoord opgegeven voor de VPN connectie die moet worden gemaakt. De VPN connectie wordt op die manier afgedwongen.

Tabel 16: WIFI

WiFi:	
Disable Wi-Fi:	NO

Wi-Fi wordt niet uitgeschakeld omdat dit een technologie, hoewel hoger al gebleken is dat ze onveilig is, vaak wordt gebruikt door werknemers om e-mails te checken en toegang tot het bedrijfsnetwerk te verkrijgen. De problematiek wordt aangepakt met behulp van de encryptie.

Tabel 17: Wired Software Upgrades

Wired Software Upgrades:	
Allow Web-Based Software Loading:	YES
Cryptographic Services Backup:	YES

Met behulp van webbrowser wordt toegestaan om de Blackberry te updaten. Zo kan de gebruiker overal ter wereld, waar er internet voor handen is, zijn Blackberry updaten en ervoor zorgen dat er geen beveiligingslekken zijn in het OS van de handheld.

Met behulp van de cryptographic services backup worden gegevens tijdens de upgrade, hierboven beschreven, gebackupt. Dit kan van belang zijn indien er iets misloopt.

Tabel 18: Wireless Software Upgrades

Wireless Software Upgrades:	
Disallow Patch Download Over Roaming WAN:	NO

Met behulp van deze regel wordt het updaten via draadloze netwerken (dus ook gsm netwerken) niet uitgeschakeld. Zo is de Blackberry te allen tijde up-to-date als hij kan connectie maken met bedrijfsnetwerk.

7.8.3.2 Transmission Security

Dit onderdeel behandelt vooral de instellingen met betrekking tot deelprobleem 3. Het biedt dus antwoorden op beveiligingsrisico's zoals hackers en dergelijke.

7.8.3.2.1 WiFi Instellingen

De instellingen voor Wifi zijn kan u vinden in de volgende tabel.

Tabel 19: WIFI

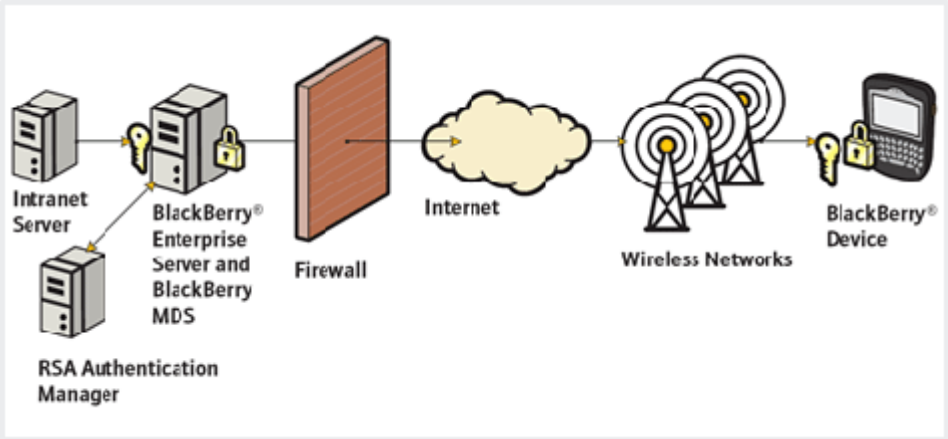
WIFI	
Wi-Fi Allow Hanheld Changes:	/ niet van toepassing in versie 5 van BES
Wi-Fi Link Security:	/
Wi-Fi Default Key ID:	1
Wi-FI WEP Key 1:	'een willekeurige numerieke waarde'
Wi-Fi SSID:	Blackberry Netwerk

Volgens Rowan (2010) is WEP voorbijgestreefd. Het is een makkelijk te kraken mechanisme. Daarom is het beter te opteren voor een andere beveiliging. Als standaard sleutel heb ik

willekeurige nummerieke waarde verkozen. Tevens wordt de connectie, zoals in het volgende onderdeel wordt besproken, geëncrypteerd end-to-end zodat WEP in mindere mate nodig is.

7.8.3.2.2 Andere draadloze verbindingen

Alle draadloze verbindingen worden beveiligd met behulp van SSL of TLS. In de volgende figuur ziet u dat de BES alle verbindingen op eenzelfde manier behandelt. Dit wordt toegelaten door het MDS-systeem van Blackberry. De Blackberry enterprise software oplossing zorgt voor een **end-to-end** beveiliging welke gebruik maakt van meerdere opties ter encryptie, zoals blijkt uit het volgende van Research In Motion (2010): *"The Blackberry Enterprise Solution offers two transport encryption options, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES)*, for all data transmitted between Blackberry® Enterprise Server and Blackberry smartphones."* Er wordt gewerkt volgens het principe*: "Blackberry MDS Services act as a secure gateway between the wireless network and corporate intranets and the Internet. They leverage the Blackberry AES or Triple DES* encryption transport and also enable HTTPS connections to application servers."* Men kan dit principe dan ook vaststellen in figuur 21.

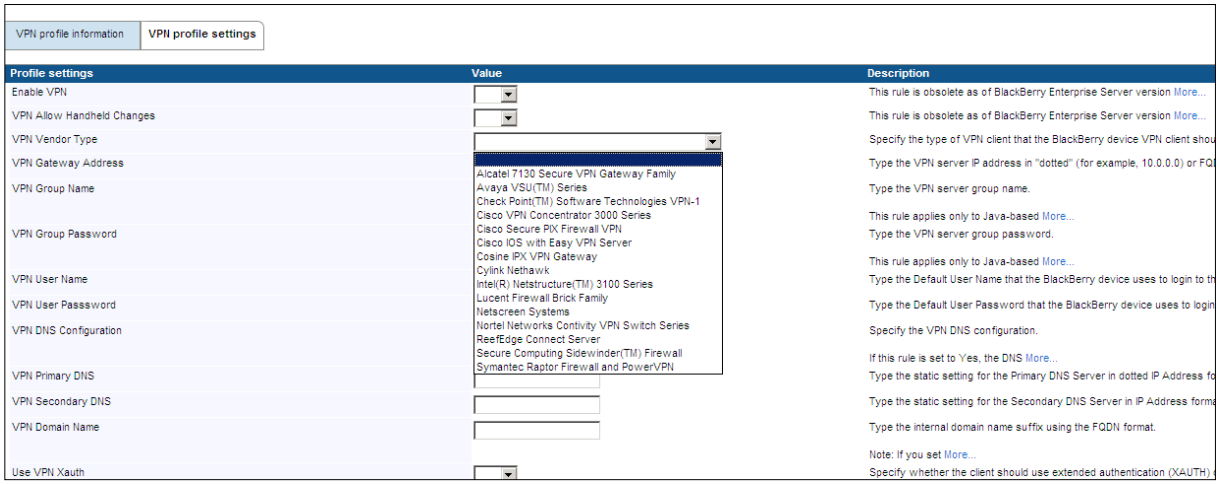


Figuur 30: Blackberry opzet (Research In Motion, 2010)

7.8.3.2.3 VPN verbinding

Om tot een optimale beveiligingsstrategie te komen moet de transmissie van data gebeuren via het opzetten van VPN, zoals hoger reeds aangehaald. Maar de implementatie van een VPN in de IT security policy moet in samenspraak gedaan worden met een compatibele router die VPN toestaat. Vermits de hardware hiervoor niet voor handen is kan dit ook niet geïllustreerd worden. U kan dit

concluderen uit de volgende figuur. Slechts een beperkt aantal routers kunnen samenwerken met Blackberry Enterprise Server.

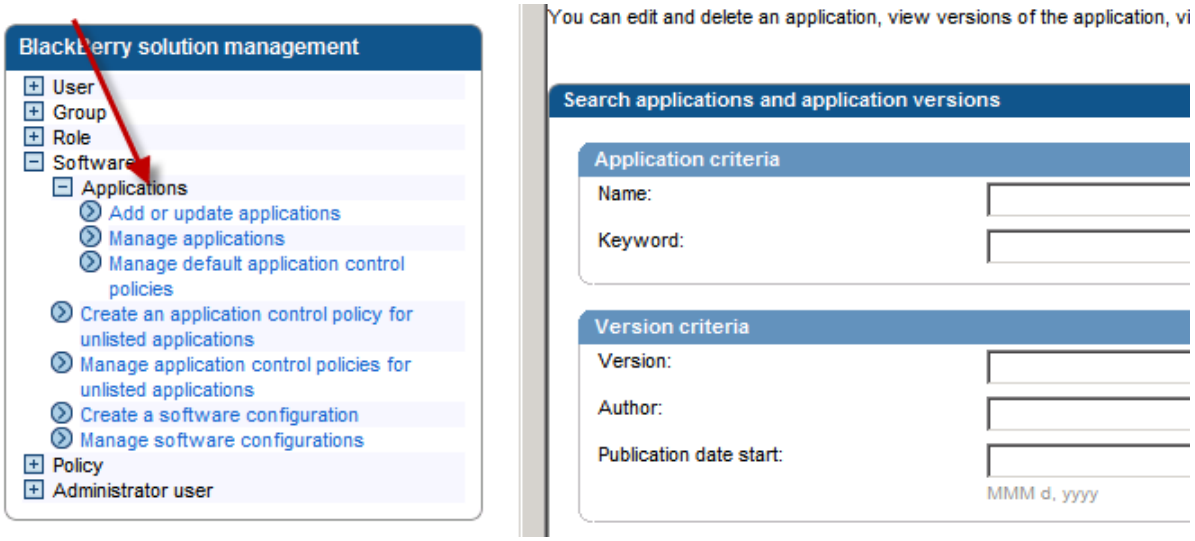


Figuur 31: BES compatibele routers

In combinatie met zulk een router kan BES een VPN verbinding opzetten naar de smartphones. Zo kunnen zij een veilige verbinding opzetten met het bedrijfsnetwerk.

7.8.3.3 Applicatie niveau

Met behulp van de Blackberry Enterprise Server Express kunnen bepaalde pakketten worden ingesteld van software. Zo kan er bepaalde software worden toegelaten die 'required' of 'optional' is. Men kan met behulp van applications tab instellen welke versie de applicaties moeten hebben alvorens de client volledige toegang tot het netwerk heeft. In de volgende figuur wordt de tab aangeduid met behulp van een rode pijl.



Figuur 32: De tab met applicaties

Zo kunnen applicaties worden toegevoegd die dan automatisch worden verdeeld via het netwerk naar toestellen die proberen connectie te maken met de server en dus ook het netwerk. Hier is het 'push principe' van toepassing. Dit is een handig principe. Indien de virusdefinities niet up-to-date zijn dan kunnnen die eerst in orde worden gemaakt alvorens het toestel volledige rechten in het netwerk verkrijgt. Men kan in de onderneming beslissen al dan niet een anti-virus applicatie te implementeren op de toestellen.

Indien de onderneming andere applicaties wenst toe te voegen tot de blakcberry toestellen, dan kan dit op deze manier dus gedaan worden. Wat de beveiliging van de applicaties betreft hoeft de onderneming zich geen zorgen te maken vermits de applicaties los staan van de beveiliging. De verbinding wordt immers beveiligd, zo kan men op een efficiënte manier applicaties toevoegen zonder ingewikkelde beveiligingsproblemen te creëren. Het enige waar de onderneming moet in voorzien is de toegang tot de applicaties afschermen opdat enkel de juiste gebruikers toegang hebben tot de applicaties.

7.8.4 Configuratieopties op het Blackberry toestel

Sommige configuratie-instellingen moeten worden ingesteld op het smartphone zelf. Twee belangrijke instellingen waarvoor dit cruciaal is zijn:

- Toestelfirewall
- Opschonen van het geheugen (tijdelijke data op het toestel)

De aangeraden configuratie kan u terugvinden in de volgende tabel.

Tabel 20: toestelfirewall

Status	Ingeschakeld
Inkomende berichten blokkeren:	
SMS	JA
MMS	JA
E-mail	JA
Behalve berichten van:	
Contactpersonen uit het adresboek	
	(Indien anders geconfigureerd)

U kan vaststellen dat de firewall wordt ingeschakeld en zorgt voor het blokkeren van SMS'en, MMS'en en E-mails indien de afzender niet gekend is in het adresboek. Zo worden berichten van onbekende personen geblokkeerd. Dit kan soms voor problemen zorgen indien gegevens niet gekend zijn voor contactpersonen maar het is een veiligere manier van werken.

Het opschonen van het geheugen wordt ook ingeschakeld. Telkens wanneer het toestel wordt geblokkeerd zal er een opschoning plaatsvinden van het geheugen. Zo worden tijdelijke bestanden verwijderd en er wordt geheugen vrijgemaakt.

7.9 Conclusie advies

Er werd getracht een advies op te stellen ter beveiliging van de implementatie van mobiele (leer) applicaties op een Blackberry toestel. Dit beveiligingsprobleem werd opgesplitst in 3 deelproblemen: de data en applicaties op het toestel, de bescherming tegen malware en hackers en de transmissie data. Elk probleem werd voorzien van een oplossing. Encryptie en onder andere pinbeveiliging bracht een antwoord op deelprobleem 1. Deelprobleem 2 werd deels opgelost door de Blackberry architectuur zelf. Research In Motion biedt namelijk software aan die beschikt over een digitale handtekening indien deze veilig is. Daarenboven kan er gekozen worden voor het inschakelen van de firewall op het toestel om attacks te voorkomen. Het derde deelprobleem is uitgebreider van aard omdat elk type van datatransmissie moet worden beveiligd. Blackberry Enterprise Server zorgt echter voor uniforme aanpak van dit probleem: encryptie van de verschillende typen datatransmissie op dezelfde manier. Later werd er in dit hoofdstuk een voorbeeld implementatie gedaan van een Blackberry Enterprise Server in combinatie met Windows 2003 Server Enterprise en Exchange Server 2003 als voorbeeld. Dit voorbeeld geeft weer hoe de eerder aangereikte concepten kunnen worden omgezet in een IT security Policy.

8 Algemene conclusie

De onderneming moet een goed overzicht opbouwen van alle mogelijke bedreigingen die relevant zijn. In hoofdstuk 2 werd een breed spectrum aan bedreigingen vastgesteld. Ze konden worden gecategoriseerd binnen de twee volgende categorieën: interne bedreigingen, externe bedreigingen. Daarbinnen kan de categorie van attacks als zeer belangrijk worden bestempeld.

In hoofdstuk 3 werd er een overzicht gegeven van de belangrijkste evoluties. Deze ingrijpende trends zullen het ICT-landschap voor altijd wijzigen. (Arend, et al., 2009). Dit zal een impact hebben op de manier waarop zaken worden gedaan in de onderneming. Ondernemingen zullen hierbij rekening gaan moeten houden, willen of niet. Indien ze daarbij geen rekening houden zullen ze hopeloos achterop raken en dit kan negatieve implicaties hebben.

De onderneming moet de bedreigingen die eerder in hoofdstuk 2 werden vastgesteld prioritiseren, net zoals KBC dit doet bij de risk assessment in hoofdstuk 6. Als alle risico's zijn vastgesteld die een negatieve impact kunnen hebben gaat men best over naar het plannen van het omgaan met die risico's. Men moet een beveiligingsbeleid of een security policy uitzetten. De security policy kan veel problemen voorkomen. Door het uitvoerig plannen kan er op voorhand geanticipeerd worden. Omdat de security policy een belangrijk onderdeel is in het anticiperen op bedreigingen werd in hoofdstuk 4 een uitvoerige bespreking gegeven van de internationale standaarden rond de IT security policy.

We kunnen concluderen uit hoofdstuk 4 dat een algemene, high level, security policy onontbeerlijk is. De standaarden geven niet meteen, toch niet specifiek, weer hoe bepaalde evoluties moeten opgevangen worden. Maar standaarden zoals de COBIT richtlijn geeft wel een geheel van hulpmiddelen om evoluties op te vangen. Men kon ook vaststellen dat COBIT praktischer is, daar waar andere standaarden eerder theoretisch zijn van aard.

Mobile computing is onderhevig aan een groot aantal bedreigingen zoals werd besproken in hoofdstuk 5. De onderneming mag dit niet onderschatten. De belangrijkste bedreigingen zijn malware, diefstal van het toestel, het verliezen van het toestel, een direct attack en transmission security. (Hoffman, 2007) De onderneming moet actie hiertegen ondernemen. Zoals uit deel 7.2

blijkt is er ook vaak een verandering in aanpak nodig. De security policy moet op deze bedreigingen ingespeeld zijn.

In hoofdstuk 6 konden we een een betere kijk krijgen op hoe ondernemingen zoals KBC omgaan met bedreigingen. KBC heeft een speciale aanpak van problemen. Deze aanpak is onder andere een resultaat van de schaal waarop KBC werkt. De onderneming kan anticiperen op bedreigingen, nog voordat ze zich voordoen. Het perimeter concept, de whitelist aanpak, de manier hoe men 'risks' inschat zijn voorbeelden van van de speciale aanpak van problemen door KBC.

Het strikt beheer van mobiele apparaten zoals laptops en PDA's zorgt voor een veiligere omgeving. Men staat immers bij KBC niet toe dat werknemers zelf laptops, smartphones aanschaffen en gebruiken voor het werk. Men probeert op die manier te voorkomen dat confidentiële informatie op de onveilige mobiele apparaten terecht komt. De eindverantwoordelijkheid zal dan ook bij de gebruiker worden gelegd (de werknemer) en niet bij de afdeling IT van de onderneming. Dit is cruciaal. De werknemer helpt in feite de onderneming te beveiligen. Hij is in feite de firewall.

Er werd getracht een advies op te stellen ter beveiliging van de implementatie van mobiele (leer) applicaties op een Blackberry toestel. Dit beveiligingsprobleem werd opgesplitst in 3 deelproblemen: de data en applicaties op het toestel, de bescherming tegen malware en hackers en de transmissie data. Elk probleem werd voorzien van een oplossing. Encryptie en onder andere pinbeveiliging bracht een antwoord op deelprobleem 1. Deelprobleem 2 werd deels opgelost door de Blackberry architectuur zelf. Research In Motion biedt namelijk software aan die beschikt over een digitale handtekening indien deze veilig is. Daarenboven kan er gekozen worden voor het inschakelen van de firewall op het toestel om attacks te voorkomen. Het derde deelprobleem is uitgebreider van aard omdat elk type van datatransmissie moet worden beveiligd. Blackberry Enterprise Server zorgt echter voor uniforme aanpak van dit probleem: encryptie van de verschillende typen datatransmissie op dezelfde manier. Later werd er in dit hoofdstuk een voorbeeld implementatie gedaan van een Blackberry Enterprise Server in combinatie met Windows 2003 Server Enterprise en Exchange Server 2003 als voorbeeld. Dit voorbeeld geeft weer hoe de eerder aangereikte concepten kunnen worden omgezet in een IT security Policy.

Lijst van geraadpleegde bronnen

Geraadpleegde surveys, boeken, publicaties, syllabussen en geïnterviewden

Academic Service Microsoft. (2000). *MCSE Trainings Kit: Microsoft Windows 2000 Server.* Schoonhoven: Academic Server.

Allen, M. (2005, november). *A day in the life of mobile data.* Opgeroepen op maart 29, 2010, van British Computer Society: http://www.bcs.org/server.php?show=conWebDoc.2774

Bayne, J. (2002). *An overview of Threat and Risk Assessment.* Opgeroepen op augustus 30, 2009, van Sans.org: http://www.sans.org/reading_room/whitepapers/auditing/overview-threat-risk-assessment_76

Bennett, C. (2003). *Challenges of Mobile Security.* Opgeroepen op september 7, 2009, van SearchCIO.com: http://searchcio.techtarget.com/tip/0,289483,sid182_gci952382,00.html

Bundesamt für Sicherheit in der Informationstechnik. (2000). *IT Baseline Protection Manual.* Bremen: BSI.

Campo, M., Epting, B., Heirdeis, M., Jeager, S., Koops, B., & Pohlmann, N. (2002). *Netwerk beveiliging.* Diepenbeek: SYNTRA.

Cohen, F. (1984). *Computer Viruses - Theory and Experiments* . Opgeroepen op augustus 28, 2009, van Fred Cohen & Associates: http://all.net/books/virus/index.html

Committee, J. I. (2001, februari 19). *Developing and Information Security Policy*. Opgeroepen op december 11, 2009, van JISC: http://www.jisc.ac.uk/aboutus/committees/subcommittees/pastcommittees/jcas/jcaspaperssecurity.aspx

Computer Security Institute. (2008). *CSI Computer Crime & Security Survey.* San Francisco, CA, USA: CSI.

Cross, M. (2007). *Web Application Security.* United States and Canada: O'Reilly Media, Inc.

Deloitte. (2006). *Protecting the digital assets - The 2006 Technology, Media & Telecommunications Security Survey.* Deloitte.

FollowUS. (2003). *Follow is to a smarter Method of Locating Your Mobile Workers.* Opgeroepen op maart 28, 2010, van FollowUS: http://www.followus.co.uk/Mobile.pdf

Gassp. (2010, april 21). *Gassp.* Opgeroepen op april 21, 2009, van infosectoday.com: http://www.infosectoday.com/Articles/gassp.pdf

Gocsi. (2008). *CSI Computer Crime & Security Survey 2008.* Opgeroepen op augustus 6, 2009, van Computer Security Institute: http://gocsi.com/survey

Goode Intelligence. (2009). *GI mSecurity Survey 2009.* London: goodeintelligence.com.

Harrington, V., & Mayhew, P. (2001). *Home office research study 235: mobile phone theft.* London: Crown Copyright.

Harrington, V., & Mayhew, P. (2001). *Mobile phone theft.* London: Home Office Research, Development and Statistics Directorate.

Hindle, T. (1998). *Manage Your Time.* United States: Dorling Kindersley Publishing Inc.

Hindocha, N. (2003, januari 13). *Instant Security: Security Issues of Instant Messaging*. Opgeroepen op augustus 30, 2009, van Security Focus: http://www.securityfocus.com/infocus/1657

Hoffman, D. (2007). *Blackjacking: security threats to Blackberry devices, PDAs, and cell phones int he enterprise.* Indianapolis, Canada: Wiley.

Huet, A., & Staquet, A. (2006). *Bussiness Risk Management.* Brussel: FEDICT.

Hunton, J. E., Bryant, S. M., & Braganoff, N. A. (2009). *Information Technology Auditing.* Belgium: Wiley.

Institute, B. S. (2009). *BS7799 Code of Practice for Information Security.* BSIgroup.com.

International Organisation for Standardisation. (2009). *About ISO*. Opgeroepen op maart 26, 2009, van ISO: http://www.iso.org/iso/about.htm

IT Governance Institute. (2007). *ISACA.* Opgeroepen op maart 5, 2010, van ISACA: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

Krishnan, S., & Bhatia, K. (2008). *SOAs for scientific applications: Experiences and challenges.* San Diego: San Diego Supercomputer Center, UC San Diego, 9500 Gilman Drive, La Jolla, CA 92093-0505, United States.

Laudon, K. C., & Laudon, J. P. (2006). *Bedrijfsinformatiesystemen 9th Edition.* Amsterdam: Pearson Education Benelux, Amsterdam.

Leung, C., & Chan, Y. (2003). *Mobile Learning: A new paradigm in electronic learning.* Proceedings of the The 3rd IEEE International Conference on Advanced Learning Technologies, Chinese University of Hong Kong, China.

Longman. (2005). *Longman Dictionary of Contemporary English.* Essex: Pearson Longman.

Lopez, M. (2009). *Succesful Mobile Deployments Require Robust Security.* Lopez Research LLC.

Magic Spysuite. (2009). *Spyphone software guide.* Opgeroepen op maart 29, 2010, van magicspysuite.com: http://www.magicspysuite.com/img/MagicSpySuite_symbian_0s_9.pdf

McNurlin, C. B., Sprague, R. H., & Bui, T. (2009). *Information Systems Management in Practice.* Upper Sadle River, New Jersey, 07458: Pearson Education Inc.

Mcwilliams, B. (2005, februari 22). How Paris got hacked? *O'Reilly Network* .

Meijers, W. (2007). *Service Oriented Architecture: Implementing the framework for Business-ICT alignment.* Nieuwegein, The Netherlands: Everett.

Mercken, R. (2009). *ICT-governance, syllabus.* Universiteit Hasselt: Universiteit Hasselt: Faculteit Toegepaste Economische Wetenschappen.

Microsoft. (2010, mei 25). *Geblokkeerde bijlagen in Outlook*. Opgeroepen op mei 25, 2010, van Office Online: http://office.microsoft.com/nl-be/outlook/HA012299521043.aspx?pid=CH100777061043

Microsoft. (2002, juli 24). *What's new in active directory*. Opgeroepen op april 3, 2010, van Microsoft.com: http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/activedirectory.mspx#ESC

Motiwalla, F. (2005). *Mobile Learning : A framework and evaluation.* Massachutts: University of Massachutts Lowell College of Management.

NIST. (2008). *Guidelines on Cell Phone and PDA Security.* Opgeroepen op februari 2, 2010, van National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

NIST. (2007). *User's Guide to Securing External Devices for Telework and Remote Access.* US Department of Commerce.

Norberg, J. (2002). *Leve de globalisering.* Amsterdam: Houtekiet.

OASIS group. (2010, mei 16). *OASIS SOA Reference Model TC*. Opgeroepen op mei 16, 2010, van OASIS: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm

O'Brien, J., & Marakas, G. M. (2005). *Security Measures.* International edition: Mc. Graw-Hill.

Olzak, T. (2006, juli 4). *Strengthen security with an effective security Awareness program*. Opgeroepen op december 16, 2009, van it.toolbox.com: http://it.toolbox.com/blogs/adventuresinsecurity/strengthen-security-with-an-effective-security-awareness-program-8707

Rosenthal, A., Mork, P., Li, M., Stanford, J., Koester, D., & Reynolds, P. (2008). *Cloud comptuing: A new business paradigm for biomedical information sharing.* The MITRE Corporation, Innovative Information Engineering and Biometrics.

Savill, J. (2008). *Complete Guide to Windows 2008 Server.* Boston: Pearson Education, Inc.

Schreurs, J., & Moreau, R. (2007). ICT Security Management. Diepenbeek, Limburg, Belgium.

SearchMobileComputing.com. (2008). *Mobile Security Policies.* London: Research in Motion Limited, Blackberry.

Securiteam.com. (1999, november 19). *Whisker*. Opgeroepen op september 26, 2009, van Whisker: a next generation CGI scanner: http://www.securiteam.com/tools/3R5QHQAPPY.html

Security Policy. (2009, 3 28). Opgeroepen op 3 28, 2009, van http://www.wikipedia.be: http://en.wikipedia.org/wiki/Security_policy

Software & Information Industry Association. (2001). *Software as a Service: Strategic Backgrounder.* Washington, DC 20036: Software & Information Industry Association.

Symantec, S. E. (2006). *Securing Instant Messaging.* Symantec Enterprise Security.

Symantec, Security Enterprise. (2006). *Symantec: Securing Instant Messaging.* Symantec Security Enterprise.

Tsiantis, L. E., Stergiou, E., & Maragariti, S. (2007). *Security Issues in E-learning systems.* Patra, Greece: Hellenic Open University.

Van den Driessche, N. (2009). When data goes up and out: Data Leakage Prevention in a Financial Organisation. *Marcus Evans Conference on Corporate Data Protection and Privacy Compliance.* KBC.

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security* , 275-279.

Webopedia.com. (2010, mei 25). *Spam*. Opgeroepen op mei 2010, 25, van webopedia.com: http://www.webopedia.com/TERM/S/spam.html

Whitman, E. M., & Mattord, J. H. (2009). *Principles of information security.* Canada: Thomson Course Technology.

Wilson, M., & Hash, J. (2003). *Building an Information technology Security Awareness and Training Program.* US Department of Commerce.

Artikels uit wetenschappelijke tijdschriften

Arend, O., Bellens, E., Gyssels, S., Lemmens, K., Van Oost, J., Van Leemputten, J., et al. (2009, Januari). Zeven trends voor 2009. *Smart Bussiness Strategies* , pp. 22 - 43.

Ashely, M. (2004). New practices in wireless security. *Communication News* , 30-33.

Aufrieter, R. (2002). New Needs on New Devices. *Mobile Security* , 2-3.

Beam, C. (2007, march 7). *How do you intercept a text message?* Opgeroepen op maart 9, 2010, van Slate Magazine: http://www.slate.com/id/2161402/

Blommestein, M. (2008, september 30). *Gartner: cloud is SaaS, niet iets anders.* Opgeroepen op september 23, 2009, van Techworld, Gartner: Cloud is Saas en niets anders: http://techworld.nl/technologie/5847/gartner-cloud-is-saas--niet-iets-anders.html#

Bluecoat. (2010, februari 3). *Top Ten Security Trends for 2009.* Opgeroepen op februari 3, 2010, van Bitpipe.com: http://viewer.bitpipe.com/viewer/viewDocument.do?accessId=11531448

Bluetooth.com. (2009). *Special Intrest group*. Opgeroepen op februari 12, 2010, van Bluetooth.com: http://www.bluetooth.com/Bluetooth/Fast_Facts.htm

Boni, B. (2000). The More Things Change, the More They Stay the Same!: Headline: "DTI Survey Finds Most UK Companies Experienced Security Breaches." Headline: "FBI Study Finds U.S. Losses to Computer Crime Increased 100%.". *Computer Security* , 18-19.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From dekstop tot moile: Examining the security experience. *Computers & Security* , 130-137.

Brodkin, J. (2008, juli 2). *Trip Report: Security and Risk Management Community*. Opgeroepen op september 29, 2009, van Security Central: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

Brooks, J. (2007, november 5). Virtual Security Crisis. *Eweek* , p. 12.

Busquiel, P. (2009). Een Bussiness continuïty plan in vijf stappen. *Bussiness ICT* , 50-53.

Clarke, N., & Furnell, S. (2005). Authentication of users on mobile telephones: A survey of attitudes and practices. *Computers & Security* , 519-527.

D. Richard Kuhn, T. J. (2005, januari). *Security Considerations for Voice Over IP Systems.* Opgeroepen op december 13, 2009, van National Institute for

Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

De Rooij, J. (2009, maart 16). *Bedrijven breken beveiliging af.* Opgeroepen op april 4, 2009, van Computable Headlines Security: http://www.computable.nl/artikel/ict_topics/security/2899177/1276896/bedrijven-breken-beveiliging-af.html

De Rooij, J. (2009, maart 3). *Cloud brengt nieuwe beveiligingsproblemen.* Opgeroepen op april 5, 2009, van Computable: http://www.computable.nl/artikel/ict_topics/security/2885340/1276896/cloud-brengt-nieuwe-beveiligingsproblemen.html

De Rooij, J. (2009, februari 20). *Mobiel OS fundamenteel onveilig.* Opgeroepen op april 2009, 2009, van Computable: http://www.computable.nl/artikel/ict_topics/security/2874320/1276896/mobiel-os-is-fundamenteel-onveilig.html

De Rooij, J. (2009, februari 23). *Offline werken maakt webapplicaties onveilig.* Opgeroepen op april 6, 2009, van Compuatable: http://www.computable.nl/artikel/ict_topics/security/2875731/1276896/offline-werken-maakt-webapplicaties-onveilig.html

De Rooij, J. (2009, maart 17). *Virtualisatie brengt nieuwe beveiligingsrisico's.* Opgeroepen op maart 30, 2009, van Computable Headlines: http://www.computable.nl/artikel/ict_topics/security/2899821/1276896/virtualisatie-brengt-nieuwe-beveiligingsrisicos.html

Doherty, N. F., & Fulford, H. (2006, februari). Aligning the information security policy with the strategic information systems plan. *Computers & Security* , 55-63.

Donaldson, S. (2009, september). Add a little SaaS to your company. *Techwatch* , p. 41.

Doucet, B. (2009, juni). *Behoefte aan veiligheid is allesbehalve virtueel*. Opgeroepen op december 3, 2009, van datanews.be: http://new.datanews.be/nl/business-ict/63-91-2244/virtualisatie--behoefte-aan-veiligheid-is-allesbehalve-virtueel.html

Elms, R. E., Laprade, J. D., & CPCU, C. M. (2008). Hacking of Corporate Information Systems: Increasing Threats and Potential Risk Management Techniques. *CPCU eJournal* , 1-9.

Fisher, M. A. (2005, september). Virtualised computing infrastructure. *BT Technology Journal* , 52-58.

Gibbs, W. (2009). How to steal Secrets without a Network. *Scientific American* , 58-63.

Gilliland, A. (2006, november). Understanding the IM Security Threat. *Information Systems Security* , pp. 16-20.

Gladstone, D. (2009, februari 26). *Next-Generation Netbooks: The New Ultra portables*. Opgeroepen op december 12, 2009, van PCWorld: http://www.pcworld.com/article/160156/netbooks_all_about_the_new_ultraportables.html

Graux, H. (2008, december). Tien vragen over privacybescherming. *Smart Bussiness Strategies* , pp. 64-66.

Gyssels, S. (2009). Alles uit de muur. *Smart Business Strategies* , 24-26.

Harmon, G. (1997). VPN provides sercure access. *Network Security* , 5.

Hayes, J. (2008, september 19). Have data? Will travel. *IT Security* , pp. 60-61.

Heslop, M. (2005). The key to network. *Communication News* , 24-39.

Hines, M. (2007, januari 22). Security at your service. *Eweek* , pp. 23-24.

Hoard, B. (2007, juli 13). *8M cell phones will be lost in 2007*. Opgeroepen op maart 29, 2010, van Computerworld Storage: http://www.computerworld.com/s/article/9026944/8M_cell_phones_will_be_lost_in_07_how_to_back_yours_up

Höne, K., & Eloff, J. (2002). Information secuirty policy - what do international information security standards say? *Computers & Security* , 402-409.

Joint, A., Baker, E., & Eccles, E. (2009, mei 19). Hey, you, get off that cloud. *Computer Law & Security Reviews* , pp. 270-274.

Kadam, A. (2007). Information Security Policy Developement and Implementation. *Information Systems Security* , 246-256.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems secuirty policies: a contextual perspective. *Computers & Security Volume 24, Issue 3* , 246-260.

Kim, G. (2008). Seven steps to a secure virtual environment. *Network Security* , 14-18.

Knapp, J. K., Morris, F. M., & Byrd, T. (2009). Information security policy: An organizational-level process model. *Computers & Security* , 493-508.

Kreamer, L. K., Dedrick, J., & Yamashiro, S. (2000). Refining and Extending the Business Model With Information Technology: Dell Computer Corporation. *The Information Society* , 5-21.

Lambert, M. (2005). Blackberry security. *Network Security* , 18-20.

Le Blanc, G. (2008, juni). Bussiness Advisory: Know SaaS issues before they impact operations. *Manufacturing Bussiness Technology* , pp. 18-23.

Lederer, & Sethi. (1996). Key prescriptions for strategic information systems planning. *Journal of Management Information Systems* , 35-62.

Manise, J.-L. (2008). De gevaren van Voice over IP. *Bussiness ICT* , 96-101.

Mansfield-Devine, S. (2008). Danger in the clouds. *Network Security* , 9-11.

Mansfield-Devine, S. (2008). OS X - is it time to start worrying? *Network Security* , 7-9.

Miller, A. (2004). PDA Security concerns. *PDA Security* , 8-10.

Mojtahed, M., & Xirasagur, S. (2009). Securing IP networks, part I. *Network security* , 10-14.

Moor, W. d. (2008, november 10). *Dell, Seagate en Mcafee werken samen bij versleutelen schijven*. Opgeroepen op september 24, 2009, van Tweakers.net: http://tweakers.net/nieuws/56675/dell-seagate-en-mcafee-werken-samen-bij-versleutelen-schijven.html

Munro, K. (2008). Breaking into Bluetooth. *Network Security* , 4-6.

Network Security. (2010). WPA cracking tool launched. *Network Security* , pp. 1-2.

News, D. (2008, december 8). ICT is Chinees voor ondernemers. *Knack* .

NIST. (2006). *An Introduction to Computer Security: The NIST Handbook.* U.S. Department of Commerce.

Panda Security. (2009). ID theft malware on the increase. *Network Security* , 1-2.

Panko, R. (2005). Datanetwerken en telecommunicatie. In R. Panko, *Datanetwerken en telecommunicatie: vijfde editie* (pp. 360-368). Amsterdam: Pearson Education Benelux.

Potter, B. (2004). Bluetooth vulnerabilities. *Network Security* , 4-5.

Rowan, T. (2010, februari). Negotiating WiFi security. *Network Security* , pp. 8-12.

Rowan, T. (2007). VPN technology: Ipsec vs. SSL. *Network Security* , 13-17.

Rubenking, N. (2008). Computing moves into the Cloud. *PC Magazine* , 79.

Rubenking, N. (2008, januari). Computing Moves Into the Cloud. *PC Magazine* , p. 79.

Schwartz, E. (2006, december 11). The Burden of SaaS. *infoworld.com* , p. 10.

Shaikh, S. A., Chivers, H., Nobles, P., Clark, J. A., & Chen, H. (2009). Toward scalable intrusion detection. *Network Security* , 12-16.

Siegel, C., Sagalow, T., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Information Security Journal: A Global Perspective* , 33 - 49.

Simon, H. A. (1957). *Administrative behaviour (2nd ed.).* New York: The Free Press.

Sloan, K. (2009). Security in a Virtualised World. *Network Security* , 15-18.

Sloddard, J. (2005, october). Big Software, Little Price. *www.FPAPracticeManagement.org* , pp. 6-7.

Solms, E. a., & Eloff, M. (2000). Information security management: a hierachical frame for various approaches. *Computers and Security Volume 19* , 243-256.

Straub, D. W. (1990). Effective IS security: an empirical study. *Information Systems Research* , 255-276.

Trend Micro. (2010). Back to the future. *Network Security* , 4-7.

Van Der Beek, P. (2007, augustus 6). *Helft bedrijven is slecht voorbereid op een ramp.* Opgeroepen op april 18, 2009, van Computable headlines: http://www.computable.nl/artikel/ict_topics/ictbranche/2077177/2379258/helft-bedrijven-is-slecht-voorbereid-op-een-ramp.html

Van Leemputten, P. (2009, maart). *Vlaamse baas kent niets van computerbeveiliging.* Opgeroepen op november 13, 2009, van Smart Bussiness Strategies: http://zdnet.be

Van Leemputten, P. (2009, januari 1). Werknemers stellen job veilig met gestolen bedrijfsinformatie. *Smart Bussiness Strategies* , p. 15.

Wokke, A. (2009, 11 13). *Dell gaat Android smartphone ook vanuit China verkopen.* Opgeroepen op 11 14, 2009, van Tweakers.net: http://tweakers.net/nieuws/63720/dell-gaat-android-smartphone-ook-buiten-china-verkopen.html

Wood, C. (1995). Writing infosec policies. *Computers & Security* , 667-674.

Geraadpleegde whitepapers

Acosta, A. (2008). *Stanford on Itunes U.* Opgeroepen op februari 4, 2010, van Apple.com: http://images.apple.com/education/docs/it/Apple-Stanford011509.pdf

Alladin. (2009). *Attack Intelligence™ Research Center Annual Threat Report 2008 Overview and 2009 Reports.* Belcamp: AIRC.

Brown, J. (2009). *Exploring Mobile Learning: Part one of the mLearning Series.* Opgeroepen op februari 4, 2010, van Blackberry.com: http://na.blackberry.com/eng/solutions/industry/education/WP_JudyBrown_Part1Long_HighRes_MobileLearning.pdf

F-Secure. (2007). *Résumé des menaces Mobiles pour 2007.* F-Secure.

Motahari-Nezad, H. R., Stephenson, B., & Singhal, S. (2009). *Ousourcing Business to Cloud Computing Service: Opportunities and Challenges.* HP Laboratories.

Oracle. (2010, april). *Overcoming the Management Challenges of Portal, SOA, and Java EE Applications.* Opgeroepen op mei 16, 2010, van Oracle.com: http://www.oracle.com/technology/products/oem/pdf/wp_overcome_mgmt_challenges.pdf

Research In Motion. (2010). *Blackberry Enterprise Server, version 4.1, Policy Reference Guide.* Opgeroepen op maart 13, 2010, van Research In Motion: http://docs.blackberry.com/en/admin/deliverables/3801/Policy_Reference_Guide.pdf

Research In Motion. (2010). *Blackberry Internet Service 3.1.* Opgeroepen op mei 28, 2010, van Blackberry.com: http://www.blackberry.com

Research in motion. (2010, mei 25). *About memory cleaning*. Opgeroepen op mei 28, 2010, van Blackberry.com: http://docs.blackberry.com/en/smartphone_users/deliverables/1487/About_memory_cleaning_65063_11.jsp

Research In Motion. (2010). *Blackberry Enterprise Server*. Opgeroepen op maart 3, 2010, van Blackberry.com: http://na.blackberry.com/eng/services/business/

Research In Motion. (2010). *Blackberry Security Features*. Opgeroepen op mei 11, 2010, van Blackerberry.com: http://uk.blackberry.com/ataglance/security/features.jsp#tab_tab_stored_data

Research In Motion. (2009). *CIO's Guide To Mobile Security.* Blackberry.

Research In Motion. (2010). *Feature and Technical Overview - BlackBerry Enterprise Server for Microsoft Exchange*. Opgeroepen op maart 13, 2010, van

Research In Motion: http://docs.blackberry.com/en/admin/deliverables/12056/BlackBerry_Enterprise_Solution_security_834422_11.jsp

Research In Motion. (2009). *Going mobile: developing an effective corporate mobile policy.* Blackberry.

Research In Motion. (2010, april 21). *Knowledge base blackberry*. Opgeroepen op april 21, 2010, van Blackberry.com: http://na.blackberry.com/eng/ataglance/security/knowledgebase.jsp#faq8

Research In Motion. (2009). *Network Transports*. Opgeroepen op februari 6, 2010, van Blackberry.com: http://www.blackberry.com/DevMediaLibrary/view.do?name=network

Research In Motion. (2010). *Security Features Blackberry Enterprise Server*. Opgeroepen op april 7, 2010, van uk.blackberry.com: http://uk.blackberry.com/ataglance/security/features.jsp

Research In Motion. (2009, april 30). *The CIO's Guide to Mobile Security.* Opgeroepen op februari 12, 2010, van Blackberry.com: http://www.blackberry.com/solutions/resources/CIOs_Guide_to_Mobile_Security_100606_online.pdf

Geraadpleegde websites

Apple. (2010). *Mobile Learning and Itunes U: Now download directly to iPhoneand iPod touch*. Opgeroepen op februari 4, 2010, van Apple.com: http://www.apple.com/education/mobile-learning/

Apple. (2010). *Understanding Credentials and User Access for Advanced Access.* Opgeroepen op februari 4, 2010, van Apple.com: http://deimos.apple.com/rsrc/doc/iTunesUAdministrationGuide/CustomizingYouriTunesUSite/chapter_8_section_7.html#//apple_ref/doc/uid/AdminGuide-CH6-SW2

BSIgroup. (2009). *About BSI*. Opgeroepen op maart 26, 2009, van Order BSI Standards Online: http://www.standardsuk.com/about.php

Nessus. (2009, september 26). *Nessus*. Opgeroepen op september 26, 2009, van Tenable Network Security: http://www.nessus.org/nessus/

PGP. (2010). *PGP Corporation*. Opgeroepen op maart 13, 2010, van PGP Mobile: http://www.pgp.com/products/mobile/index.html

Proximus. (2010). *Proximus mobiel internet*. Opgeroepen op maart 29, 2010, van Proximus.be:

http://customer.proximus.be/nl/Introduction/Internet.html?WT.ac=CBU_TopNav_HP_Internet_nl_click

Telenet Mechelen. (2010). *Telenet mobile*. Opgeroepen op maart 29, 2010, van Telenet.be: http://telenet.be/1905/0/1/nl/thuis/mobile/abonnement-gsm.html

Vmware. (2010). *ESX Server*. Opgeroepen op april 3, 2010, van Vmware.com: http://www.vmware.com/products/esx/

VMware. (2009). *VMware ESX, a bare metal hypervisor*. Opgeroepen op september 22, 2009, van VMware vSphere: http://www.vmware.com/products/esx/index.html

Interviews

Van den Driessche, N. (2009, november 6). Head of Information Risk Management. (T. Princen, Interviewer)

Vanderheyden, P. (2010, april 29). Medewerker IT afdeling. (T. Princen, Interviewer)

Bijlagen

Bijlage 1: Security Policy, een voorbeeld

State of Illinois
Department of Central Management Services

MOBILE DEVICE SECURITY POLICY

Effective: October 01, 2009

State of Illinois

Department of Central Management Services
Bureau of Communication and Computer Services

MOBILE DEVICE SECURITY POLICY

Effective October 01, 2009

Version 1.0

APPROVAL SHEET

State CIO	Greg Wass	Date: 9/30/09
CMS Director:	James P. Sledge	Date: 9-9-09
CMS/BCCS Deputy Director:	Doug Kasamis	Date: 9/08/09
CMS/BCCS Deputy General Counsel:	Dominic Saebeler	Date: 9/3/09
CMS/BCCS Chief Information Security Officer:	Rafael Diaz	Date: 9/02/09

Please Return to: **CMS/BCCS**
Chief Information Security Office
120 W. Jefferson
Springfield, IL 62702
Thank You.

TABLE OF CONTENTS

POLICY STATEMENT

The Illinois Department of Central Management Services, Bureau of Communication and Computer services (CMS/BCCS) seeks to protect State of Illinois (State) mobile devices from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal.

PURPOSE

This document describes the minimum security policy for State of Illinois mobile devices. Mobile devices must be appropriately secured to prevent sensitive or confidential data from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the State of Illinois' computing and information infrastructure.

SCOPE

This security policy (Mobile Device Security Policy) applies to the user of any State mobile device which connects to the CMS/BCCS managed network / resource.

DEFINITIONS

Definitions for terms used in this policy can be found in the *BCCS Terminology Glossary* located at http://bccs.illinois.gov . The terms and definitions listed below are meaningful for this policy. In the event of conflict between the definition in the *BCCS Terminology Glossary* and the definition contained in this policy, the definition below shall control for this Policy.

1. **Mobile Devices:** These include, but are not limited to, Portable Digital Assistants (PDAs), notebook computers, Tablet PCs, Palm Pilots, Microsoft Pocket PCs, RIM Blackberrys, MP3 players, text pagers, smart phones, compact discs, DVD discs, memory sticks, USB drives, floppy discs and other similar devices.
2. **User** - Anyone with authorized access to State business information systems, including permanent and temporary employees or third-party personnel such as temporaries, contractors, consultants, and other parties with valid State access accounts.
3. **Screen Lock** - Mechanism to hide data on a visual display while the computer continues to operate. A screen lock requires authentication to access the data. Screen locks can be activated manually or in response to rules.
4. **Screen Timeout** - Mechanism to turn off a device or end a session when the device has not been used for a specified time period.

ENFORCEMENT

Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including discharge, may involve civil or criminal litigation, and may involve restitution, fines, and/or penalties.

RESPONSIBILITY

1. Each user of a State mobile device is responsible for following this policy and any related policy or procedure promulgated by their Agency head.

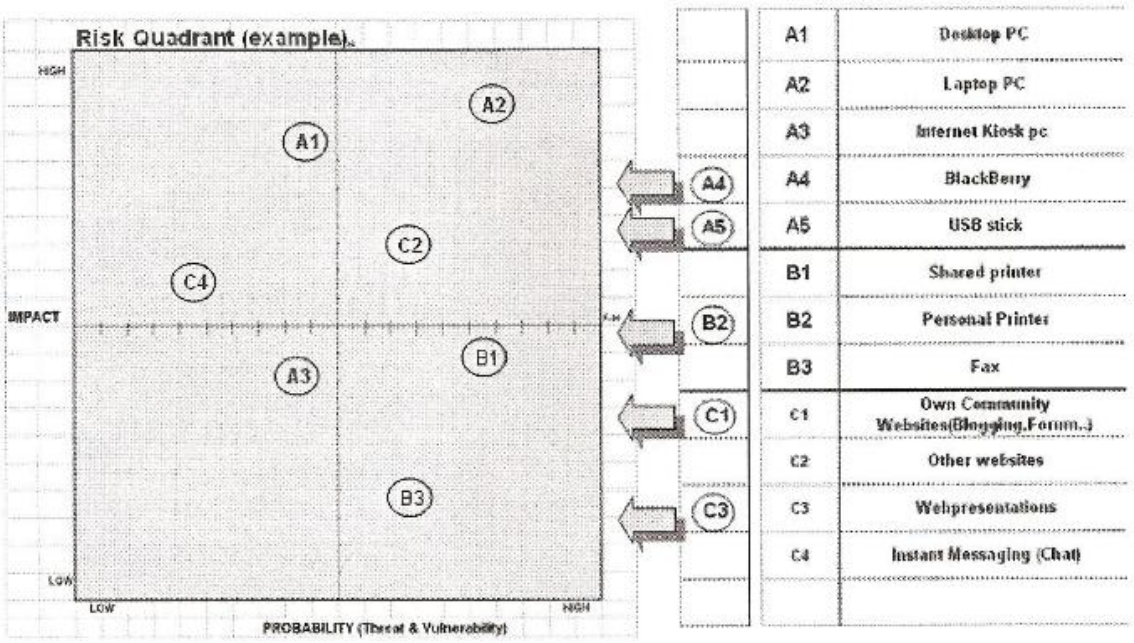
2. Each Agency may also establish policies and procedures and assign responsibility to specific agency personnel to achieve compliance with this policy.
3. Anyone observing what appears to be a breach of security, violation of this policy, violation of state or federal law, theft, damage, or any action placing State resources at risk must report the incident to an appropriate level supervisor, manager, or security officer within their organization. Those reporting alleged incidents will be protected from retaliation by existing whistleblower protection laws.
4. Managers and supervisors are responsible for ensuring that users are aware of and understand this policy and all related procedures.

POLICY

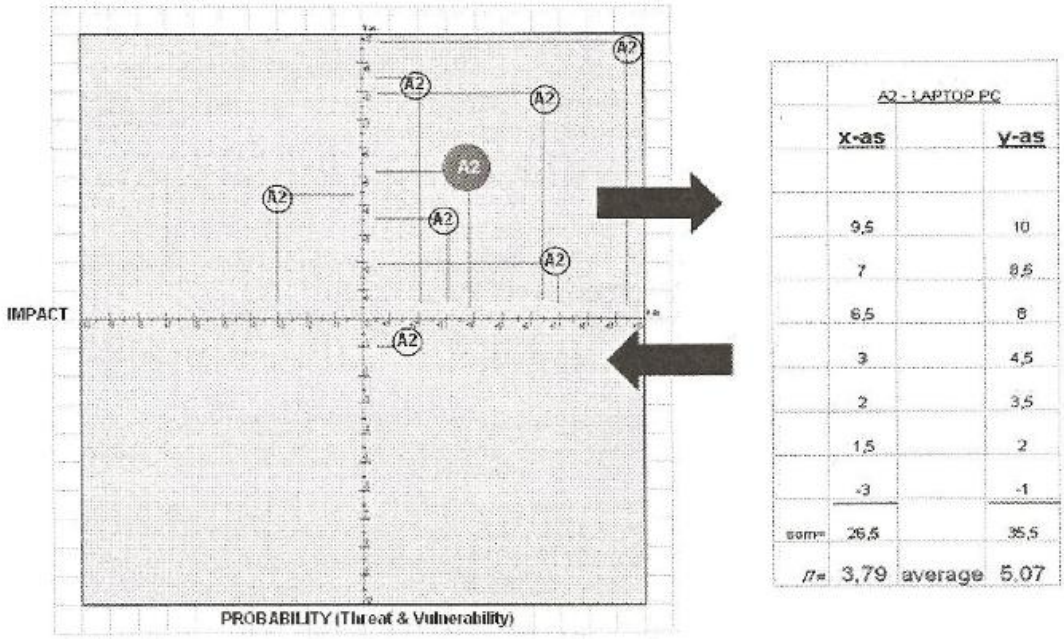
1. Whenever possible, all mobile devices must be password protected. Choose and implement a strong password – at least eight (8) characters in length.
2. The physical security of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight.
3. If a mobile device is lost or stolen, promptly report the incident to the CMS/BCCS Help Desk and proper authorities. Also, be sure to document the serial number of your device now, for reporting purposes, in the event that it is lost or stolen.
4. Sensitive or confidential documents, if stored on the device, should be encrypted if possible.
5. Mobile device options and applications that are not in use should be disabled.
6. Sensitive and confidential information should be removed from the mobile device before it is returned, exchanged or disposed.
7. Whenever possible all mobile devices should enable screen locking and screen timeout functions.
8. No personal information (as defined by the personal information protection act – 815 ILCS 530) shall be stored on mobile devices unless it is encrypted and permission is granted from the data owner.
9. Before a mobile device is connected to State IT systems, it shall be scanned for viruses (the user risks having files on the device deleted if any viruses are detected). If media mobile device is used for transitional storage (for example copying data between systems), the data shall be securely deleted from the mobile device immediately upon completion.

- End of Mobile Device Security Policy -

Bijlage 2: Risk assessment deel 1

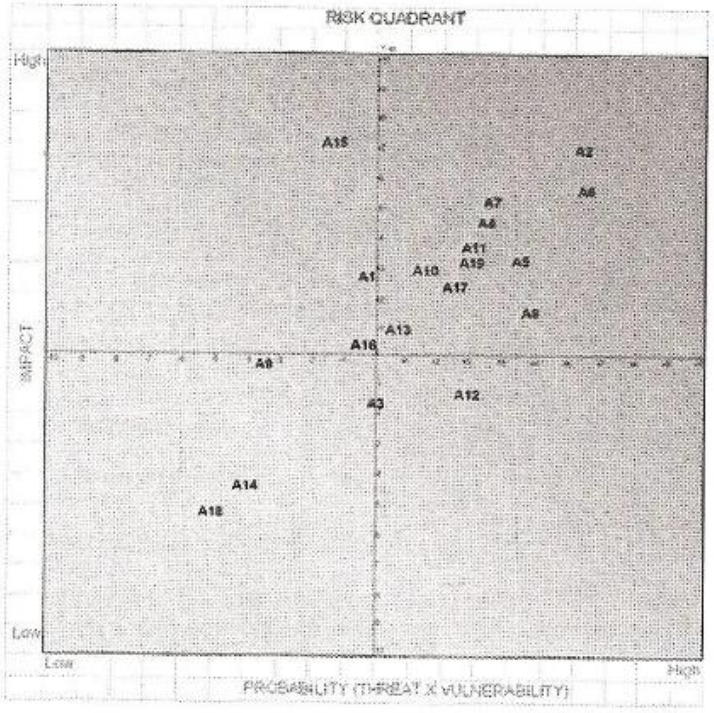


Figuur 33: Plaatsing van de toestellen in het grid door executives - stap 1 (Van den Driessche, When data goes up and out: Data Leakage Prevention in a Financial Organisation, 2009)



Figuur 34: Bepaling van het risico, impact en de gemiddelden (Van den Driessche, When data goes up and out: Data Leakage Prevention in a Financial Organisation, 2009)

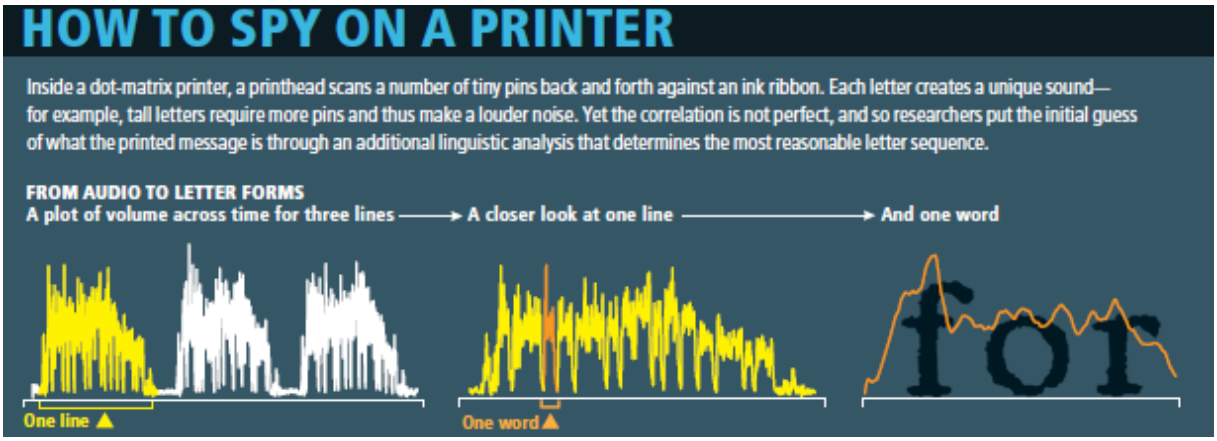
Bijlage 2: Risk assessment deel 2



	End User	Function
A1	Desktop PC	Storage of information either electronically or in paper form from end user perspective (client components)
A2	Laptop PC	
A3	Internet Kiosk pc	
A4	Agent's computer	
A5	Smart phone/PDA	
A6	USB stick	
A7	External Disk	
A8	Storage on Paper	
A9	Microfilm/Microfische	
A10	Optical Magnetic device writer	
A11	Memory cards	
A12	Mobile Phone	
A13	Private Home PC	
A14	Whiteboard	
A15	Server	
A16	Disposals	
A17	External Webstorage	
A18	I-Pen (Electronic Pen)	
A19	Non company devices	

Figuur 35: Uiteindelijke risico na de uitmiddeling van de verkregen waarden door de bevraging (Van den Driessche, When data goes up and out: Data Leakage Prevention in a Financial Organisation, 2009)

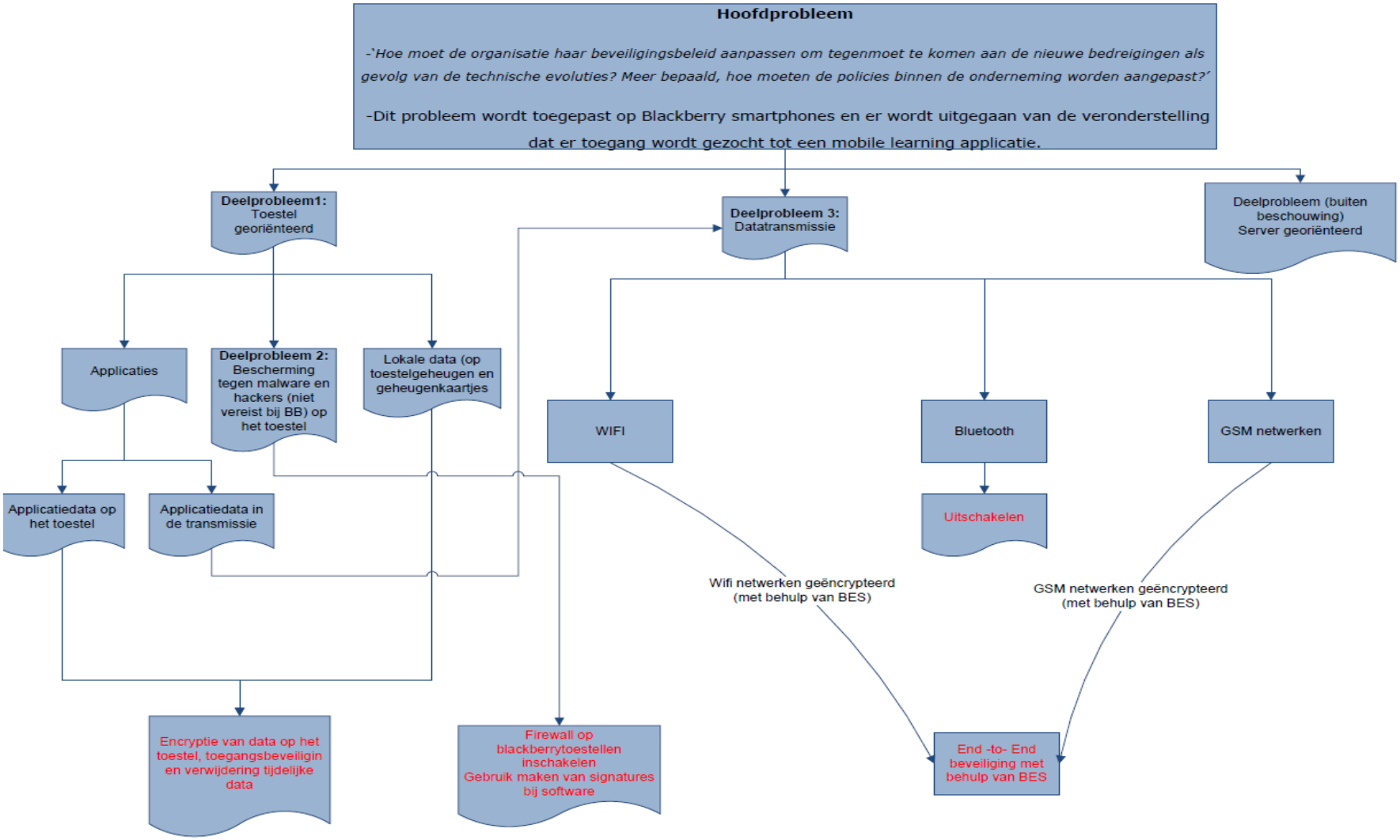
Bijlage 3 : A vulnerable office (Gibbs, 2009)



Figuur 36: Hoe een printer bespioneren? (Gibbs, 2009)

Figuur 37: Anatomie van een kwetsbaar kantoor. (Gibbs, 2009)

Bijlage 4 : Overzicht problematiek



Auteursrechtelijke overeenkomst

Ik/wij verlenen het wereldwijde auteursrecht voor de ingediende eindverhandeling:
IT beveiligingsbeleid aangepast aan nieuwe evoluties van IT. Beveiliging van mobile computing in de onderneming

Richting: **master in de toegepaste economische wetenschappen : handelsingenieur in de beleidsinformatica**
Jaar: **2010**

in alle mogelijke mediaformaten, - bestaande en in de toekomst te ontwikkelen - , aan de Universiteit Hasselt.

Niet tegenstaand deze toekenning van het auteursrecht aan de Universiteit Hasselt behoud ik als auteur het recht om de eindverhandeling, - in zijn geheel of gedeeltelijk -, vrij te reproduceren, (her)publiceren of distribueren zonder de toelating te moeten verkrijgen van de Universiteit Hasselt.

Ik bevestig dat de eindverhandeling mijn origineel werk is, en dat ik het recht heb om de rechten te verlenen die in deze overeenkomst worden beschreven. Ik verklaar tevens dat de eindverhandeling, naar mijn weten, het auteursrecht van anderen niet overtreedt.

Ik verklaar tevens dat ik voor het materiaal in de eindverhandeling dat beschermd wordt door het auteursrecht, de nodige toelatingen heb verkregen zodat ik deze ook aan de Universiteit Hasselt kan overdragen en dat dit duidelijk in de tekst en inhoud van de eindverhandeling werd genotificeerd.

Universiteit Hasselt zal mij als auteur(s) van de eindverhandeling identificeren en zal geen wijzigingen aanbrengen aan de eindverhandeling, uitgezonderd deze toegelaten door deze overeenkomst.

Voor akkoord,

Princen, Tom

Datum: **1/06/2010**