5 De marktwerking van beveiliging & betaling op elektronische marktplaatsen

Arthur van der Wees

5.1 Inleiding

5.1.1 Marktwerking

Marktwerking is een bekende term die geheel van toepassing is op een marktplaats en derhalve de elektronische marktplaats[1]. Teneinde vraag en aanbod op een succesvolle wijze bij elkaar te brengen en te houden alsmede de handel zo optimaal als mogelijk c.q. gewenst te krijgen, dienen beide zijden van de markt adequaat gefaciliteerd te worden. Anders gezegd: zowel de aanbieder als de vrager dienen zich op hun gemak te voelen.
Op een elektronische marktplaats zijn adequate, parate informatie en het gebruik ervan vitale elementen. In de binaire wereld van een dergelijk marktplein is die kennis één van de succesfactoren. Die informatie zal centraal staan en (in aangepaste of gecombineerde vorm) van waarde worden of reeds zijn.
Om een waardevolle, winstgevende althans kostendekkende dienst te kunnen verlenen, stemt een B2B-initiatief de aanwezige mogelijkheden af op de behoeften van de markt en reduceert men de risico's en bedreigingen. Ervan uitgaande dat voor de moderne boer het adagium 'wat de boer niet kent, eet hij niet' niet geldt, biedt een B2B-marktplein voor zijn branche goede mogelijkheden.

5.1.2 Vertrouwen in beveiliging & betaling

Eén van de cruciale aspecten voor het welslagen van een elektronische marktplaats is het vertrouwen van alle participanten ervan. Werkelijk succes van een levendige handel volgt slechts nadat alle betrokken partijen voldoende vertrouwen hebben in de partijen waarmee en de locatie waarop zij handelen. Veiligheid en dus beveiliging zijn daarbij sleutelbegrippen. Behalve indien de participant niet avers is van het nemen van ongecalculeerde risico's zal hij niet tot handelen en het doen van transacties overgaan, indien het vertrouwen daarbij ontbreekt. Het genereren van vertrouwen zal niet eenvoudig zijn; vertrouwen speelt bij de

[1] Voorbeelden van diverse soorten B2B-marktpleinen zijn te vinden in Hoofdstuk 1 van dit boek, alsmede op http://www.forbes.com/bow/b2b/main.jhtml.

boer (en anderen) in de fysieke wereld – op de 'gewone' markt – eveneens een grote rol.

Gesteld kan worden dat het vertrouwen in beveiliging van een coöperatieve en besloten elektronische marktplaats hoger zal zijn dan op een commerciële en openbare, publieke marktplaats. Immers, de relatieve kleinschaligheid van eerstgenoemde marktplaats genereert en behoudt meer vertrouwen; de vertrouwensrelatie zal daar in beginsel minder onpersoonlijk en meer transparant zijn. Bij het definiëren, structureren, opbouwen, uitbalanceren en instandhouden van een B2B-marktplein moet continue gekeken worden naar de beveiliging en de betaling op dat marktplein. Vertrouwen is een sleutelbegrip voor het succes van het B2B-marktplein, hetgeen onder meer inhoudt dat transacties niet onderschept en gewijzigd zullen mogen worden, de identiteit van de vrager en aanbieder buiten kijf zal moeten staan, een betaling van de vrager aan de aanbieder adequate kwijting moet bieden en de digitale informatie als wettig bewijsmiddel moet kunnen dienen. Beveiliging en betaling gaan grotendeels hand in hand; men zou immers kunnen stellen dat beveiliging in de meeste gevallen een conditio sine qua non is voor handel en dus betaling.

5.1.3 Behandeling

Gegeven het thema van deze NVvIR-publicatie alsmede de ruimte van deze bijdrage, beperkt deze bijdrage zich tot het signaleren van juridische en aanverwante elementen van beveiliging en betaling op elektronische elektronische marktplaatsen. Deze bijdrage betreft een momentopname in de steeds veranderende maatschappij van e-commerce & elektronische marktplaatsen. Met de voetnoten wordt getracht verwijzingen aan te bieden naar meer gedetailleerde en actuele informatie op internetsites en/of in literatuur verband houdende met de hier behandelde en aanverwante onderwerpen.
In paragrafen 5.2 en 5.3 worden de belangrijkste mogelijkheden, bedreigingen en uitgangspunten van de elektronische marktplaats behandeld. Voor het adviseren (of procederen) over juridische kwesties is voldoende kennis over de werking en doelstellingen van de branche en haar bedrijfsprocessen essentieel; uitsluitend juridische kennis is zoals altijd niet voldoende. In paragraaf 5.4 wordt stilgestaan bij de beschikbare juridische basis en hulpmiddelen om bij te dragen in het succes van de elektronische marktplaats. In de daarop volgende paragrafen worden de mogelijkheden van beveiliging (5.6), betaling als ook facturering (5.7) kort nader behandeld. Deze bijdrage wordt in paragraaf 5.8 met enkele afsluitende opmerkingen afgerond.

5.2 B2B-business case

5.2.1 Feiten, voorwaarden & beeldvorming

Wat is nodig of gewenst om een elektronische marktplaats te kunnen aanvangen, succesvol te worden en te blijven? Dat is een vraag die gesteld en beantwoord dient te worden voorafgaand aan de inschatting wat ter zake juridisch (alsmede organisatorisch en technisch) nodig is.
Voor een juiste balans tussen (i) vertrouwen en werkbaarheid ter zake de elektronische marktplaats (en daarmee het genereren en instandhouden van marktwerking) en (ii) een faciliterend bestanddeel als de beveiliging van die marktplaats, zijn als sleutelbegrippen te noemen: adequate afstemming en coördinatie van de B2B-markt(plein)structuur en haar organisatie op de behoeften van de markt. Een andere sleutelbegrip dat genoemd kan worden, is overigens de compatibiliteit tussen het voor de elektronische marktplaats gebruikte systeem en het bedrijfssysteem van de participant zelf.[2]
Er zijn vele typen elektronische marktplaatsen mogelijk: besloten, semi-publiek, publiek (eenzijdig of wederkerig) of gemengde elektronische marktplaatsen.[3] Het besluit welk type het B2B-initiatief gaat worden, is vanzelfsprekend de basis voor de te nemen (juridische en andere) maatregelen en is verder van belang om te kunnen bepalen welke partijen er zullen bestaan: zelfstandige of consortia marktpartijen, een separate beheerder, andere faciliterende dienstverleners, aandeelhouders et cetera. Dit zal van invloed zijn op de te nemen maatregelen.

Voor een elektronische marktplaats zijn – onder meer – apparatuur en programmatuur voor communicatie, verwerking en opslag nodig, maar ook infrastructuur, bedrijfsruimte en deskundige personen. Dit boeket aan elementen (dat hierna gezamenlijk 'faciliterende informatiesysteem' wordt genoemd) dient gestructureerd, georganiseerd en gestuurd c.q. beheerd te worden ter facilitering van de elektronische marktplaats en de daarop gewisselde en beschikbare informatie.
Bij een B2B-initiatief zal onder meer het juiste niveau van gebruik, en de scheidingslijn tussen gebruik en misbruik van zowel de informatie als het faciliterende informatiesysteem dienen te worden gedefinieerd en vervolgens continue worden gecontroleerd, geactualiseerd en gehandhaafd.

---

2 R. op het Veld, E-markten komen moeilijk op gang, *Het Financieele Dagblad* d.d. 7 mei 2001.
3 Verwezen wordt naar Hoofdstuk 1 van dit boek.

5.2.2 *Handhaving*

Het valt misschien al op dat de handhaving, beheer, controle en instandhouding terugkomende begrippen zijn in deze bijdrage. De reden hiervan is om extra aandacht te vestigen op het feit dat in de praktijk de neiging bestaat om voornoemde niveau's en scheidslijnen wel redelijk te definiëren maar daarna niet meer te controleren en te handhaven. Overigens is die praktijk helaas universeel; hoe vaak gebeurt het immers niet dat een zorgvuldig afgewogen en schriftelijk vastgelegde overeenkomst, procedure of regelgeving na ondertekening c.q. activering ervan in een archiefkast verdwijnt, en partijen tijdens de uitvoering ervan vervallen in oude (en soms ongewenste) gewoonten, gedoogbeleid of zelfs onwetendheid. In een mogelijke geschillensituatie of (gerechtelijke) procedures levert dat onnodige complicaties op.

5.2.3 *Wat is adequaat?*

Ter zake het B2B-initiatief, het faciliterende informatiesysteem en de informatie daarop, rijst vervolgens de vraag wat nu de 'noodzakelijke', 'afdoende', 'adequate' en/of 'wenselijke' balans is tussen ondernemen en handel enerzijds en beveiligen anderzijds. Dat is lastig te bepalen. In ieder geval staat vast dat honderd procent veiligheid een onbereikbaar en zelfs onwenselijk ideaal is. Op dit moment bestaat het dan ook niet.[4] Honderd procent veiligheid is onbereikbaar vanwege de tand des tijds en nieuwe mogelijkheden om die beveiliging te omzeilen of te doorbreken, en onwenselijk vanwege de torenhoge kosten die gepaard gaan met omvangrijke beveiligingsmaatregelen.
Het actueel houden van het faciliterende informatiesysteem, de bescherming tegen steeds ingenieus opererende computervirussen, en het maken van backups van het systeem en de informatie kosten veel geld. Een kosten-baten afweging zal (naast afwegingen van andersoortige belangen zoals het belang van de te beveiligen informatie) een redelijk indicatie kunnen geven wat 'adequaat' is. Dat adequate beveiliging als onontbeerlijk wordt gezien, blijkt wel uit het feit dat – in geval van de op dit moment regulier voorkomende, kostenreducerende maatregelen – het budget voor beveiliging meestal pas als allerlaatste wordt geschrapt. Men is er over eens dat proactief en preventief handelen verstandiger is dan achteraf (trachten te) repareren en herstellen.

---

[4] *Hacker-bestendig internet nog jaren weg* d.d. 14 februari 2002, http://www.automatiseringgids.nl/news/default.asp?nwsId=15986, *Fraud Continues to Haunt Online Retail* d.d. 4 maart 2002, http://cyberatlas internet.com/markets/retailing/article/0,,6061_984441,00.html, *Online Transaction Fraud and Prevention Get More Sophisticated*, 17 January 2002, http://www.gartnerg2.com/site/default.asp.

De toegevoegde waarde van een B2B-marktplein is het aantrekken, samenbrengen en behouden van vragers en aanbieders alsmede het optimaliseren van de interacties tussen die vragers en aanbieders. Daarvoor is geen honderd procent waterdichte beveiliging nodig. Aan ondernemen zijn risico's verbonden. Evenwel dient een B2B-marktplein zich op zodanige wijze preventief te beschermen tegen ongeautoriseerde toegang, misbruik van informatie, schending van geheimen en verstoring van communicatie, dat de marktwerking zoveel als mogelijk ongestoord blijft. Wederom is (gerechtvaardigd) vertrouwen de rode lijn voor een goede start en continuïteit van de onderneming.
Om te weten welke beveiligingsmaatregelen nodig en zinvol zijn, is ten eerste inzicht vereist in de mogelijke risico's die een ongestoorde marktwerking bedreigen. Wat kan er gebeuren, welke schade kunnen de participanten en derden ondervinden en hoe groot is de kans daarop? En is de schade verzekerbaar? Eerst zal een onderzoek naar en inventarisatie van de mogelijkheden, risico's en (frequentie van) bedreigingen (of anders gezegd: de SWOT) noodzakelijk zijn.[5] Als bedreigingen zijn bijvoorbeeld te noemen: menselijke fouten, opzet (zoals 'mollen' (tijdelijk personeel), ex-werknemers, concurrenten, recreatie hackers, hackivisten, terroristen c.a.), technische storingen en externe oorzaken (zoals storingen in de infrastructuurketen, natuurrampen c.a.).

5.2.4 Welke maatregelen moeten genomen worden?

Voornoemde inventarisatie zal gevolgd moeten worden met een onderzoek naar en inventarisatie van de te nemen (i) fysieke (locatie), (ii) technische, (iii) organisatorische, (iv) procedurele en (v) andere juridische maatregelen en/of middelen. Daarbij moet in ogenschouw worden genomen of die maatregelen en/of middelen (a) preventief, (b) detectief, (c) repressief en/of (d) correctief moeten worden ingezet. Na afweging van de risico's en potentiële schade versus de maatregelen tot beveiliging van de belangen van de vragers, aanbieders en andere betrokkenen op de elektronische marktplaats zullen de voorgenomen beveiligingsmaatregelen moeten worden vastgelegd, gehandhaafd, continue geactualiseerd en periodiek heroverwogen.

---

2 De afkorting SWOT staat voor 'Strengths, Weaknesses, Opportunities & Threats'.

5.3 Enkele basisbegrippen ter bevordering van B2B-vertrouwen

5.3.1 Basis

Enkele begrippen ter bevordering van het vertrouwen ten aanzien van een elektronische marktplaats zijn:
- identiteit en autorisatie;
- beschikbaarheid;
- authenticiteit en integriteit;
- vertrouwelijkheid, en;
- onweerlegbaarheid.

Identiteit & autorisatie
Op een virtueel marktplein moet men – voor het gevoel van de participanten nog beter dan op een fysieke markt – zeker weten wie de andere partij is waarmee men handelt en wie (zowel voor als achter de schermen) de andere aanwezigen zijn op dat marktplein. Het woord marktplaats impliceert een groot aantal partijen: de beheerder van het marktplein, faciliterende dienstverleners, vragers en aanbieders. Het is dus van belang om die partijen adequaat te kunnen identificeren. Daarnaast kan een ieder zijn eigen (beperkte) toegangsrechten krijgen, waardoor men geautoriseerd wordt om kennis te nemen van bepaalde, voor die partij geselecteerde informatie op de elektronische marktplaats of die te gebruiken. De veelal, inzake bepaalde B2C kwesties besproken anonimiteit lijkt geen optie voor het B2B-marktplein. De boer, andere participanten en de beheerder van de elektronische marktplaats zelf, zullen een betrouwbare identiteit noodzakelijk vinden, al was het maar omdat men moet weten waar de zaken en/of diensten moeten worden afgeleverd en wie moet en gaat betalen.

Beschikbaarheid
Dit betreft de toegankelijkheid van de elektronische marktplaats. Zijn de informatie daarop en faciliterende informatiesysteem ervan ook daadwerkelijk en altijd te gebruiken als men ze nodig heeft?

Authenticiteit & integriteit
Als de betreffende informatie dan beschikbaar is gesteld door een te identificeren entiteit, dan dient die informatie wel correct, compleet en dus betrouwbaar te zijn, de oorspronkelijke inhoud te hebben en tijdig beschikbaar te zijn.

Vertrouwelijkheid
De vertrouwelijkheid van de (waardevolle) informatie dient gegarandeerd te zijn, zodat die beschermd is tegen inzage en/of gebruik door ongeautoriseerden en andere onbevoegden. Daarbij kan gedacht worden aan bepaalde exclusiviteit en strikte geheimhouding.

Onweerlegbaarheid
De handel, transacties en aanverwante informatie moeten vastgelegd kunnen worden voor controle- en bewijsdoeleinden.

Voornoemde basisbegrippen leveren een grote doch niet uitputtende bijdrage voor het benodigde vertrouwen. Uiteraard zijn andere factoren, zoals efficiëntie, gebruiksvriendelijkheid en transparantie eveneens van belang. Eenvoudige en duidelijke aanmelding- en transactieprocessen en transactieafhandeling zijn vitaal. Zo is het verzorgen van adequate faciliteiten voor goede klantenservice essentieel gebleken. Immers zal een participant in andere gevallen er weinig voor voelen om de elektronische marktplaats opnieuw en regelmatig te bezoeken. Vertrouwen betreft een grotendeels psychologisch verschijnsel. Het is dan ook bekend dat elektronische marktplaatsen (maar ook andere elektronische handelsinitiatieven) psychologen inschakelen om te beoordelen en adviseren over de 'look and feel' ervan. Zal de klant c.q. participant zich voldoende naar zijn zin hebben en wekt de elektronische marktplaats op die wijze ook vertrouwen?
Voornoemde basiselementen zijn eveneens van toepassing op het betalingsverkeer op de elektronische marktplaats. De mogelijkheid om veilig en betrouwbaar (elektronisch) te betalen is een ander belangrijk element voor het benodigde vertrouwen. Samengevat zijn gebreken ter zake beveiliging, betalingsmogelijkheden, transparantie en gebruiksvriendelijkheid de belangrijkste obstakels op de weg naar vertrouwen en rooskleurige vooruitzichten in de branche van de B2B-markten.[6]

5.3.2 Faciliterende rol

De te nemen beveiligingsmaatregelen zijn er slechts om de belemmeringen tot handelen zoveel als mogelijk weg te nemen en zelfs om handel te stimuleren; van wantrouwen naar vertrouwen in de elektronische marktplaats. Deze puur faciliterende rol mag niet uit het oog worden verloren bij het opstellen en

[6] Zo vindt (volgens onderzoek van Evan Data Corp.) 45% van de 400 ondervraagde technologie managers de beveiliging het grootste obstakel voor ecommere projecten. The web at your service, *Business Week* d.d. 18 maart 2002.

implementeren van beveiligingsplannen, -procedures en ter zake doende overeenkomsten. De maatregelen moeten effectief, efficiënt en werkbaar zijn. Dit betekent onder meer dat die maatregelen de markt niet mogen hinderen of het gehele systeem vertragen.

5.4 Juridisch kader

5.4.1 Wet- en regelgeving & zelfregulering

Het Nederlandse civiele recht en beveiliging van een B2B-omgeving zijn eigenlijk bijzonder goed op elkaar ingespeeld.[7] De waarborging van adequate beveiliging van een elektronische marktplaats (maar ook andere e-commerce initiatieven) en daarmee de bedrijfsvoering van de elektronische marktplaats kan immers alleen geschieden indien vooraf (en vervolgens continue) wordt onderzocht en onderkend wat de beveiligingsrisico's zijn, naar aanleiding waarvan preventieve en andersoortige maatregelen worden genomen, vastgelegd en gehandhaafd om die risico's weg te nemen althans zoveel als nodig te beperken. Die (i) respectievelijke analyse, structurering en besluitvorming over de mate van zekerheid die gewenst is, (ii) de afweging ter zake de kosten en inspanningen die daarvoor nodig zijn, alsmede (iii) het beheer en de handhaving ervan, zullen steeds op maat moeten worden uitgevoerd. Het Nederlandse recht sluit daar goed bij aan, nu het– mede gezien het vele regelend recht en het feit dat bij een elektronische marktplaats de consument en haar rechten praktisch geen rol spelen – zelfregulering lijkt te promoten.[8] Adequate beveiliging is bij uitstek interdisciplinair en grotendeels gebaseerd op consensus tussen partijen. Een ondernemer (in casu de participanten op de B2B-markt) is zelf verantwoordelijk om zijn zaken correct te regelen. Naast de juridische noodzaak en promotie van zelfregulering van beveiliging van een elektronische marktplaats, zijn er ook andere belangrijke argumenten zoals de commerciële belangen om vertrouwen en daarmee marktwerking te genereren en behouden. Dit geldt overigens mutatis mutandis voor de betaling op de elektronische marktplaats.

De onderwerpen beveiliging en betaling zullen op maat geregeld moeten worden als resultante van actuele kennis over die onderwerpen en de contractsvrijheid van partijen, een en ander rekening houdend met de Nederlandse wet-

---

[7] De argumentatie gaat niet op voor het Nederlandse strafrecht, nu daar vanzelfsprekend geen sprake is van de bevordering van zelfregulering en contractsvrijheid.

[8] Hoewel in casu (de B2B-(boeren)marktplaats) deels relevant, wordt in deze bijdrage niet ingegaan op de regeling voor algemene voorwaarden (artikel 6:231 BW e.v.) en aanverwante onderwerpen, zoals de invloed van de open norm van artikel 6:233 sub a BW op (rechts)personen die een vergelijkbare (zwakke) positie innemen als een consument.

en regelgeving. Die wet- en regelgeving fungeert (zoals vaker bij kwesties tussen ondernemingen) daarbij 'slechts' als basis en vangnet, in de gevallen dat die niet door partijen geregeld zijn en/of geregeld kunnen worden vanwege toepasselijke dwingendrechtelijke bepalingen.
Adequate beveiliging van een elektronische marktplaats zal moeten bestaan uit een samenhangende structuur van technische, organisatorische en juridische beveiligingsmaatregelen en –middelen. De technische en organisatorische maatregelen zullen in paragraaf 5.6 nader worden behandeld.
De wettelijke basis van de rechten en plichten ter zake onderhavige beveiliging staat (expliciet of meer impliciet) verspreid in diverse wet- en regelgeving, zoals het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht, het Wetboek van Strafvordering, de Telecommunicatiewet, de Wet bescherming persoonsgegevens, de Auteurswet 1912 en de Databankenwet.[9] Net als de technische en organisatorische maatregelen en middelen is die wettelijke basis – vanwege de aard van beveiliging – grotendeels preventief. Hoewel de relevante bepalingen in het Wetboek van Strafrecht[10], het Wetboek van Strafvordering ook deels als preventief zijn bedoeld, staan die beter bekend als reactief.[11] In de praktijk is het natuurlijk niet verstandig om het op een (reactief) beroep op strafbepalingen aan te laten komen.

Strafrecht
In deze bijdrage zal ik het strafrecht niet nader behandelen. Daarbij komt dat het merendeel van bedreigingen op onderhavige faciliterende informatiesystemen en de informatie daarop veroorzaakt wordt door menselijke fouten. Slechts een relatief beperkt deel van de risico's wordt veroorzaakt door opzettelijke aanvallen van buitenaf. Voor het regelen en sanctioneren van de meeste fouten (welke dus meestal niet opzettelijk zijn gemaakt) is geen toepassing van strafrecht vereist. Als laatst mogelijke (en meest drastische) sanctiemiddel blijft het strafrecht echter noodzakelijk.

Burgerlijk Wetboek
Verspreid in het Burgerlijk Wetboek (BW) staan diverse bepalingen die impliciet of expliciet gerelateerd zijn aan (de zorgplichten ter zake) beveiliging en betaling. Zo moet de boekhouding van een rechtspersoon krachtens artikel 2:10

[9] Voor nadere informatie ter zake wordt hier kortheidshalve verwezen naar literatuur c.q. artikelen als: H. Franken c.a., *Recht en Computer*, Kluwer, Deventer 2001 en J.E.J. Prins & S.J.H. Gijrath, *Privaatrechtelijke aspecten van elektronische handel*, Deventer, Tjeenk Willink 2000.
[10] Aandacht in het Wetboek van Strafrecht verdienen bijvoorbeeld (i) ter zake de integriteit en beschikbaarheid van faciliterende informatiesystemen en gegevens de artikelen 138 a (hacken), 161 sexies-septies (computersabotage) en 350 a-b (gegevensbeschadiging & virussen) en (ii) ter zake de vertrouwelijkheid van faciliterende informatiesystemen en gegevens de artikelen 139 a-e (afluisteren en aftappen) en artikel 273 (bedrijfsgeheimen).
[11] Y. Buruma, internet en strafrecht, in: *Preadviezen over het onderwerp Recht en internet*, Deventer, Tjeenk Willink 1998.

lid 3 BW gedurende zeven jaar bewaard blijven en dient die boekhouding conform artikel 2:10 lid 4 BW aan de eisen van integriteit en beschikbaarheid te voldoen indien die op 'papierloze' wijze wordt gevoerd. Krachtens artikel 3:15 a lid 2 BW gelden die bepalingen ook voor zelfstandigen.
Onder meer in boek 6 van het Burgerlijk Wetboek zijn meer impliciete bepalingen en algemene leerstukken als toerekenbare tekortkoming (artikel 6:81 BW e.v.) en onrechtmatige daad (artikel 6:162 BW e.v.) opgenomen welke onderdeel zijn van de essentiële, wettelijke basis inzake beveiliging en betaling. Naast contractuele verplichtingen en de mogelijkheid om ter zake toerekenbaar tekort te schieten, kan in andere gevallen wellicht een beroep worden gedaan op een onrechtmatige daad, zijnde 'een inbreuk op een recht en een doen en nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond'.[12] Daarbij valt te denken aan het schenden van evidente zorgplichten en andere beginselen van behoorlijk IT-gebruik of geheimhoudingplichten, hoewel rekening moet worden gehouden met een lastige weg om een vordering ook daadwerkelijk gehonoreerd te krijgen.

Telecommunicatiewet
De voor de elektronische marktplaats relevante artikelen 11 Telecommunicatiewet (Tw) en 13 Tw (bevoegd aftappen) zijn echter ook van toepassing op internet faciliteiten als e-mail en internetsites, nu dergelijke faciliterende diensten onder de definitie 'openbare telecommunicatiedienst' als beschreven in artikel 1.1 Tw vallen.[13]

Auteurswet & Databankenwet
Naast het feit dat zowel de Auteurswet 1912 (Aw) als de Databankenwet op hun eigen wijze intellectuele eigendomsrechten beschermen, dragen zij tevens bij aan de beveiliging van de (waardevolle) informatie op een elektronische marktplaats.[14] Dergelijke informatie zal – binnen het bepaalde gebruiksrecht daarop – slechts beperkt bruikbaar zijn. Misbruik van beschermde informatie wordt op die wettelijke basis zowel privaatrechtelijk als strafrechtelijk gesanctioneerd door de Auteurswerende Databankenwet.[15]

---

[12] Zie artikel 6:162 lid 2 BW.
[13] Zo bepaalt artikel 11.2 Tw dat aanbieders van openbare telecommunicatienetwerk en/of –diensten zorg dienen te dragen voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer van hun abonnees en gebruikers van hun netwerk en diensten, en bepaalt artikel 11.3 Tw dat die aanbieders onder meer verplicht zijn om passende technische en organisatorische maatregelen te treffen ter beveiliging van de door hen aangeboden netwerken en diensten.
[14] De Auteurswet en Databankenwet worden nader behandeld in Hoofdstuk 6 (van Ted Hermans) van dit boek.
[15] Zie bijvoorbeeld de artikelen 27a, 28 en 31 Aw e.v.

Wet bescherming persoonsgegevens
Naast voornoemde wettelijke bescherming van (onderdelen van een) B2B-marktplein, hangt een deel van het essentiële vertrouwen samen met de wettelijke bescherming van de persoonlijke levenssfeer. De Wet bescherming persoonsgegevens (Wbp) draagt daar een belangrijke steen aan bij. De Wbp is op 1 september 2002 in werking getreden en heeft onder meer gevolgen voor de inrichting van de faciliterende informatiesystemen van een elektronische marktplaats. Zo zal de verantwoordelijke voor het verwerken van persoonsgegevens ervoor moeten zorgdragen dat conform die wet wordt gehandeld; de verantwoordelijke kan aansprakelijk gesteld worden voor een onrechtmatige verwerking.[16] Een entiteit die in opdracht van de verantwoordelijke persoonsgegevens verwerkt (de bewerker) is daarnaast zelfstandig aansprakelijk voor gebreken binnen zijn eigen organisatie. Ten behoeve van de elektronische marktplaats is verder goed te weten dat het samenhangend geheel van informatie- en communicatietechnologieën die worden ingezet ter waarborging van privacy en de bescherming van persoonsgegevens 'Privacy-Enhancing Technologies' (PET) worden genoemd.[17]
Het College bescherming persoonsgegevens (Cbp) is het onafhankelijk bestuursorgaan dat toezicht houdt op de naleving van de wetten die het gebruik van persoonsgegevens regelen. Verder adviseert het Cbp de regering over de bescherming van persoonsgegevens en behandelt vragen en klachten.[18] Ook stimuleert het Cbp mogelijkheden van zelfregulering door organisaties die persoonsgegevens verwerken.[19]

Volgens artikel 1a Wbp zijn persoongegevens kort gezegd, gegevens die informatie bevatten over een natuurlijk persoon welke natuurlijke persoon identificeerbaar is. Als er in de gegevensbestanden van de elektronische marktplaats uitsluitend gegevens van ondernemingen voorkomen, dan zijn de betreffende gegevens dus geen persoonsgegevens. Echter, indien er in die bestanden bijvoorbeeld ook gegevens van medewerkers (zijnde identificeerbare personen) van die ondernemingen in de bestanden staan, dan zijn die weldegelijk als persoonsgegevens aan te merken. Dat laatste zal praktisch altijd het geval zijn.
De verplichtingen als beschreven in de Wbp waren overigens per saldo grotendeels al beschreven in de voorganger van de Wbp, de Wet persoonsregistraties.

[16] Zo moet de verantwoordelijke als bedoeld in de Wbp (i) nagaan of de gegevensverwerking rechtmatig is (ii) nagaan of die verwerking behoorlijk, zorgvuldig en in overeenstemming is met de Wbp en andere relevante wetten, (iii) nagaan of die verwerking moet worden gemeld aan het Cbp, (iv) de persoonsgegevens niet langer bewaren dan noodzakelijk is, (v) informatie verstrekken aan de betrokkene (degene waarop de persoonsgegevens betrekking hebben), (vi) inzage geven op verzoek van de betrokkene, (vii) gegevens corrigeren op verzoek van de betrokkene en (viii) de verwerking beëindigen als de betrokkene zich daartegen verzet.
[17] De verplichting tot het gebruik van technische (PET) en organisatorische maatregelene is opgenomen in artikel 13 Wbp. Zie verder J.J.Borking, Ch.Raab, Laws, *PETs and Other Technologies for Privacy Protection* in: JILT February 2001.
[18] De Cpb – de voormalige registratiekamer – heeft een uitgebreide internetsite, http://www.cbpweb.nl/.
[19] Over de mogelijkheden van zelfregulering wordt in paragraaf 5.4.2 nader ingegaan.

De Wbp is aan te merken als een 'verbeterde versie', met een aantal geheel nieuwe bepalingen (zoals boeteregelingen en bepalingen over direct marketing).[20]

Europese en andere internationale wet- en regelgeving
Ook de Europese Commissie (die 'electronic commerce' ook wel 'information society services' noemt) is reeds jaren actief om e-commerce te stimuleren, structureren en deels te reguleren, een en ander binnen de doelstellingen van de EU.[21] Inzake het handelsverkeer op een elektronische marktplaats mag bijvoorbeeld de op 19 juli 2001 van kracht geworden Europese richtlijn inzake de elektronische handtekening niet ongenoemd blijven.[22] Vanzelfsprekend hebben deze (en andere internationale) activiteiten invloed op die wettelijke basis in Nederland.

5.4.2 *Zelfregulering met contracten & verklaringen*

Zelfregulering & handhaving
Ter vermijding van ongewenste situaties – bijvoorbeeld dat informatie van (het gedrag van) participanten van de elektronische marktplaats ongewild openbaar wordt – dient niet alleen rekening gehouden te worden met de, in de vorige paragraaf genoemde wettelijke (deels dwingendrechtelijke) basis, maar eveneens met de commerciële implicaties van dergelijke situaties. De elektronische marktplaats leidt in die situaties gezichtsverlies en zal het verloren vertrouwen van de participant wellicht moeilijk of niet weten terug te vinden. Verder ontvangen de concurrenten van de marktplaats daardoor interessante en voor hen waardevolle informatie. Kortom, het is noodzaak om vanuit alle mogelijke invalshoeken naar de elektronische marktplaats te kijken. Het adagium 'voorkomen is beter dan genezen' geldt tenslotte ook in de wereld van het risicomanagement.
Zoals reeds opgemerkt, zal een adequate beveiliging van de elektronische marktplaats alleen kunnen worden gewaarborgd door analyse, structurering, besluitvorming, beheer en handhaving van de preventieve en andersoortige maatregelen. Nu beveiliging als bedrijfskritisch dient te worden aangemerkt, zal het be-

---

[20] Gezien de overvloed aan literatuur en internetsites over privacy en de Wbp wordt hier volstaan met de navolgende verwijzingen. De internetsites van het Ministerie van Justitie: www.minjust.nl en het Cpb: www.cpbweb.nl, op welke site tevens de digitale versies te vinden zijn van L.B. Sauwerwein & J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens*, Ministerie van Justitie, Den Haag 2001, en M. Artz, *Klant in het web, privacywaarborgen voor internettoegang*, Registratiekamer, Den Haag 2000.

[21] Het deel *Media in the Information Society* op de site van de DG Interne markt geeft een goed overzicht.http://europa.eu.int/comm/internal_market/en/media/index.htm

[22] Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *PbEG* 2000 L 13/12. In Hoofdstuk 4 (van Serge Gijrath) wordt die richtlijn kort nader besproken.

stuur van de onderneming ter zake actief moeten handelen. Het bestuur legt de besluiten en uitwerkingen daarvan vast, handhaaft de besluiten en draagt zorg voor afdoende communicatie met de overige personen in de organisatie (zijnde personeel en andere betrokkenen bij de organisatie). Nadat is vastgesteld welke partijen er betrokken (zullen) zijn bij de elektronische marktplaats dient hun identiteit en autorisatie, de (rechts)verhoudingen tussen hen, en de rechten en verplichtingen tijdens het handelsproces te worden geregeld. Daarmee kunnen de rechtszekerheid en het vertrouwen aanzienlijk worden verhoogd, zeker als de regelingen transparant blijven.

Eenzijdig & wederzijds
Bij wederzijdse overeenkomsten die bepalingen zullen (moeten) bevatten over de beveiliging- en betaling op de elektronische marktplaats valt – naast de overeenkomsten die in de hoofdstukken 2 (van Heleen Hoogeveen), 3 (van Merijn Seelt) en 4 (van Serge Gijrath) zijn besproken – te denken aan arbeidsovereenkomsten, detacheringovereenkomsten, beheer- en andere faciliterende overeenkomsten van betrokken dienstverleners (als internetdienstverleners en telecommunicatiebedrijven), geheimhoudingovereenkomsten, gebruikersovereenkomsten voor digitale certificaten alsmede bewijsovereenkomsten. Bij eenzijdige verklaringen kan men denken aan een 'privacy statement, 'security policy', 'best practise principles' en andere informatieve verklaringen.
Als extra doch noodzakelijk vangnet moeten de verzekeringovereenkomsten niet vergeten worden; in principe zijn alle met informatie- en communicatietechnologie samenhangende risico's te verzekeren.

Standaardisatie
Er bestaan diverse (zelfregulerende) initiatieven voor standaardisatie en harmonisatie van voorwaarden ten behoeve van elektronisch handelen. Die zijn in ieder geval prima geschikt om als basis c.q. ondergrens van het beveiligingsniveau aan te houden. Twee voorbeelden van de vele 'standaarden' met dergelijke basisbeveiligingsniveaus zijn de Code voor informatiebeveiliging (bedoeld voor ondernemingen) en het Besluit Voorschrift Informatiebeveiliging Rijksdienst 1994 (VIR) (weliswaar bedoeld voor de overheid, doch naar analogie goed te gebruiken voor het bepalen van de ondergrens van de beveiliging van de elektronische marktplaats).[23] Voorbeelden van in de Code voor Informatiebeveiliging genoemde basisbeveiligingsmaatregelen zijn: (i) zorgdragen voor een duidelijke structuur van verantwoordelijkheden, (ii) zorgdragen voor training en opleiding aan de participanten, (iii) zorgen voor een duidelijk beleidsdocument,

[23] Besluit van 22 juli 1994, nr. 94/M004882 is te vinden op http://www.rijksarchiefinspectie.nl/wetgeving/overige_VIR1994.html alsmede in Staatscourant 173, 1994.

controlemechanisme en een rapportagesysteem voor beveiligingsincidenten alsmede (iv) beschermen van bedrijfs- en persoonsgegevens.

Een harmoniserend initiatief in de Europese Unie op het gebied van Electronic Data Interchange (EDI) is die van de Europese Commissie uit 1994. Teneinde directe uitwisseling tussen gestructureerde en genormeerde gegevens tussen informatiesystemen (EDI) te regelen en binnen de Europese Unie te harmoniseren, heeft de Europese Commissie een Europees model EDI-overeenkomst vastgelegd.[24] De stichting Electronic Commerce Platform Nederland (ECP.nl) heeft daarvan een Nederlandse versie gemaakt.[25] Met name de artikelen 4 (bewijs), 5 (verwerking en bevestiging van EDI-berichten), 6 (beveiliging van EDI-berichten), 7 (Vertrouwelijkheid en bescherming van persoonsgegevens), 8 (opslag van EDI-berichten) en 10 (Technische specificaties en eisen) zijn van belang voor het onderwerp van deze bijdrage.

Juridische documenten op maat

Zoals Merijn Seelt in Hoofdstuk 3 van dit boekwerk ook reeds betoogt, valt het op dat vele onderhoud- of beheerovereenkomsten, de daarbij behorende Service Level overeenkomsten (SLA's) alsmede andersoortige overeenkomsten als participatie-, arbeids-, detacherings- en geheimhoudingovereenkomsten eigenlijk verbazend weinig bepalen over voor een elektronische marktplaats (of andere e-commerce initiatieven) bedrijfskritische – en dus zeer waardevolle – faciliteiten als beschikbaarheid en beveiliging van die marktplaats. Om betere en meer specifieke overeenkomsten en andere relevante documenten op maat te maken, is ruime kennis over de werking en doelstellingen van de elektronische marktplaats alsmede haar branche en bedrijfsprocessen essentieel.
Omdat er relatief weinig specifieke wet- en regelgeving bestaat op het gebied van B2B e-commerce, is het handig om te leren van aanverwante wet- en regelgeving en die zo mogelijk – weloverwogen en met mate – naar analogie te gebruiken bij het op maat opstellen van de overeenkomsten en verklaringen.[26] Zo staat in de richtlijn inzake de bescherming van de consument bij op afstand gesloten overeenkomsten een aantal (en inzake de relatie met consumenten dwingendrechtelijke) minimumregels op punten als informatie- en gegevensverstrekking, transparantie, herroepingrecht, nakoming en betaling.[27]

---

[24] De EDI-modelovereenkomst is gepubliceerd als: *Aanbeveling van de Commissie betreffende de juridische aspecten van de elektronische uitwisseling van gegevens*, PbEG L 338/98 van 28 december 1994.

[25] De modelovereenkomst en aanverwante informatie is te vinden op www.ecp.nl, alsmede beschreven en becommentarieerd door R.E. van Esch, *Electronic Data Interchange overeenkomst* in: *Automatiseringscontracten*, Kluwer, Deventer 2001.

[26] Hier wordt verwezen naar de diverse nuttige bepalingen in de Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, Aanpassing van Boek 7 van het Burgerlijk Wetboek aan richtlijn nr. 97/7/EG van het Europees Parlement en de Raad van de Europese Unie van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten, *PbEG L 144* en andere in de Hoofdstukken 1 en 4 van dit boek aangehaalde wet- en regelgeving.

[27] Zie de hierboven staande **noot 28**.

Een onderwerp dat typisch op summiere wijze wordt geregeld in overeenkomsten is de geheimhouding.[28] De beperktheid ervan is veelal reeds op te maken uit het hoge abstractieniveau van de tekst van de bepaling. De jurist of ander persoon die een dergelijk bepaling opstelt, gaat er – wellicht ten onrechte – vanuit dat kan worden volstaan met een raamwerk dat partijen vervolgens zelf moeten invullen. In de meeste gevallen zullen partijen dat echter nalaten, omdat zij op hun beurt ervan uitgaan dat het reeds goed geregeld is in die bepaling. Ook ter zake de elektronische marktplaats zou een dergelijke vacuüm niet mogen bestaan. Het moge verder duidelijk zijn dat de geheimhoudingsbepalingen ten behoeve van een B2B-initiatief bij voorkeur wederzijds moeten zijn; alle partijen hebben immers (om verschillende redenen) behoefte aan vertrouwelijkheid. Verder zullen partijen hun personeel en betrokken derden moeten verplichten (zo nodig op straffe van ontmoedigende boetes en onverminderd het recht om de volledige schade te verhalen) gelijkwaardige geheimhoudingsbepalingen na te leven.
In het kader van de benodigde informatieverstrekking door, de gewenste transparantie van (en vertrouwen op) de elektronische marktplaats is het van belang om de participanten inzichtelijk te informeren over de handelwijze van en op de marktplaats. Het lijkt gebruikelijk te worden om die handelwijze in verklaringen en/of beleidscriteria vast te leggen en op de site openbaar te maken, hoewel de verstrekte informatie aldaar vaak nog (te) summier te noemen is.

Privacy statement & audit
Voor de bij wet verplichte informatieverstrekking over het privacybeleid (als uitvoering van de Wbp) wordt vaak gebruik gemaakt van een 'privacy statement' of – op dit moment nog in beperkte mate – een certificaat en/of verklaring van een onafhankelijke, deskundige partij die het privacybeleid heeft geverifieerd. Als het bij een privacyverklaring blijft en de daadwerkelijke handelwijze en handhaving niet in lijn zijn met de wet en die verklaring, blijft het een puur commerciële (en hooguit als marketingtool gebruikte) verklaring; de vraag of daadwerkelijk wordt voldaan aan de gestelde eisen als bijvoorbeeld vervat in de Wbp blijft voor de betrokkene onbeantwoord. Een onafhankelijk onderzoek kan (naast een professionele indruk) een waardevolle bijdrage aan het benodigde vertrouwen geven. Nu ook het Cbp zelfregulering stimuleert, heeft zij in een samenwerkingsverband met auditors en andere adviesorganisaties een aantal vragenlijsten c.q. procedures ontwikkeld, zoals de Quickscan[29], de Wbp Zelfevaluatie & het Raamwerk Privacy Audit. Via die vragen c.q. procedures kan

[28] Over geheimhouding c.a.: Ch. Gielen, *Bescherming van bedrijfsgeheimen*, Deventer, Tjeenk Willink 1999.
[29] Informatie over de Cbp Quickscan is vinden op de internetpagina http://www.cbpweb.nl/bis/top-1-13.html.

de elektronische marktplaats zelf al enigszins nagaan of voldaan wordt aan de (minimum)vereisten van bescherming van persoonsgegevens.

Bewijs

Ter vergroting van de rechtszekerheid van alle bij de elektronische marktplaats betrokken partijen en de waardering van de faciliterende informatiesystemen en de informatie daarop, kunnen partijen besluiten een bewijsovereenkomst opstellen.[30] Maar ook in het geval van een rechtsgeldig totstandgekomen bewijsovereenkomst geldt de regel: 'de waardering van het bewijs is, voor zover de wet niet anders bepaalt, aan het oordeel des rechters overgelaten'.[31] Die (onzekerheid genererende) vrijheid geldt dus ook voor de (inhoud van de) bewijsovereenkomst. Daarbij moet artikel 180 Rv (ter zake de beperkte toelaatbaarheid van de bewijsovereenkomst) in ogenschouw worden genomen. Evenwel is het inzake een B2B-initiatief (waar min of meer zal worden gewerkt aan een bestendige relatie met de participanten of wellicht zelfs sprake is van een gesloten systeem) verstandig om de bewijskracht van de handelingen en bewijslastverdeling van de partijen op de elektronische marktplaats te regelen. Daarbij noodzaakt het partijen om vooraf eens goed na te denken over deze materie, hetgeen de transparantie en rechtszekerheid weer ten goede zal komen.

Permanente handhaving

Nu de Nederlander onder meer bekend staat om zijn behoefte om te preken, wordt hier herhaald dat de zorgvuldig opgestelde en rechtsgeldig ondertekende overeenkomsten en verklaringen vervolgens niet in het archief zouden moeten belanden en dat zorggedragen zou moeten worden voor adequate controle, handhaving en actualisering ervan, zodat die juridisch documenten hun waarde behouden.

5.5 Casus

Ten aanzien van de elektronische marktplaats voor en door boeren zoals beschreven in Hoofdstuk 1 zijn de uitgangspunten en mogelijkheden ter zake beveiliging en betaling gelijk aan andere B2B-markplaatsen.[32] Deze hangen evenwel af van het type (boeren)marktplaatsmodel (of combinatie van meerdere modellen) dat wordt gebruikt. Maatregelen ter zake

[30] Voor een artikel met de actuele stand van zaken over bewijsovereenkomsten: B.T.M. van der Wiel, *De Bewijsovereenkomst*, WPNR 6480 d.d. 9 maart 2002.

[31] Artikel 179 lid 2 Rv.

[32] Diverse voorbeelden van B2B-boerenmarktpleinen zijn te vinden op http://www.forbes.com/bow/b2b/industry.jhmtl?id=2.

beveiliging en betaling kunnen immers alleen worden geregeld indien de diverse verantwoordelijkheden van de betrokken partijen vast staan.
Hoewel de ideale beveiliging ten behoeve van een elektronische marktplaats niet bestaat, kan men stellen dat het zou moeten gaan om een adequate beveiliging die ongewenste elementen weert, de participanten op het marktplein zo min mogelijk belemmert in hun handelen en daarenboven (extra) vertrouwen wekt bij die (en potentiële) participanten.
Bij het nemen van adequate beveiligingsmaatregelen dient men zich ervan bewust te zijn dat het nemen van technische maatregelen niet zaligmakend en genoeg zijn. De menselijke factor van beveiligen blijft van belang. Niettemin doen de aanbieders van technische beveiligingsmaatregelen op dit moment goede zaken[33], gezien die menselijke factor enerzijds en de (melding van een) toenemend aantal beveiligingsproblemen anderzijds, blijft de vraag of de markt van beveiligingapparatuur en –programmatuur alsmede de gerelateerde diensten nu 'hot' is of een 'hype'.[34] Wat daar ook van zij, beveiliging wordt in het algemeen niet langer meer slechts als overhead beschouwd, maar als voorwaarde voor zakelijk welzijn en succes.
Ter zake de B2B-(boeren)marktplaats zal men willen beoordelen met welke beveiligingsrisico's rekening moet worden gehouden en wie welke verantwoordelijkheden ter zake de beveiliging gaat dragen. Het gaat daarbij niet alleen om de elektronische marktplaats en de informatiestromen daarop, maar ook om de faciliterende informatiesystemen van die marktplaats. Vervolgens zal de uitkomst daarvan leiden tot het nemen, regelen en vastleggen van maatregelen en/of middelen op (i) fysiek (locatie), (ii) technisch, (iii) organisatorisch, (iv) procedureel en (v) juridisch gebied. Voor deze doeleinden zou men onder meer de navolgende aandachtspunten de revue kunnen laten passeren en ter zake de in dit hoofdstuk (reeds) genoemde maatregelen nemen.

[33] Het is algemeen bekend dat de uitgaven door ondernemingen ter zake beveiliging de laatste jaren sterk is toegenomen en de komende jaren verder zullen stijgen. Diverse bedrijven hebben zich gericht op de markt van de elektronische beveiliging, zoals bijvoorbeeld SecurityFocus (www.securityfocus.com), @stake (www.@stake.com), Checkpoint (www.checkpoint.com), RSA Security (http://www.rsasecurity.com), Symantec (www.symantec.com) en VeriSign (www.verisign.com). Zie ook de site www.security.nl (een Nederlandse portal voor computerbeveiligingstaken) en de site van de Brancheverenigingen van Nederlandse internet Providers (NLIP), www.nlip.nl/index.html).

[34] Bijna dagelijks zijn er in de media berichten te lezen over internet, beveiliging, virussen et cetera, bijvoorbeeld '2002 wordt rampjaar voor computerbeveiliging' d.d 23 februari 2002, http://www.webwereld.nl/nieuws/10343.html.

5.6 Aandachtspunten bij beveiliging

5.6.1 Bedrijfsruimte

De elektronisch marktplaats zal – ondanks haar non-fysieke karakter – per saldo ergens in een bedrijfsruimte op een computersysteem met randapparatuur staan, welke verbonden zullen zijn met netwerkcomponenten. Hoe en tegen welke risico's is die ruimte beveiligd? Wie heeft toegang tot die ruimte, hoe wordt de ruimte beheerd en wie is ervoor verantwoordelijk? En welke maatregelen dienen te worden genomen om de continuïteit en constante bereikbaarheid van de B2B-markt te garanderen?

5.6.2 Apparatuur en programmatuur voor communicatie, verwerking en opslag

Deze apparatuur en programmatuur dient men te onderhouden en beheren.[35] Daarnaast zal ze vanzelfsprekend – bij voorkeur op meerdere niveau's – moeten worden beveiligd.[36] Wie verleent die diensten en wat zijn hun verantwoordelijkheden? Is de apparatuur redundant, worden er (werkende) reservekopieën gemaakt van de programmatuur, installatie-instructies en andere documentatie, waar worden die back-ups bewaard en wie heeft daar toegang toe? Hoe kan inbraak van buitenaf worden voorkomen, hoe is de toegang geregeld en hoe is de programmatuur beveiligd tegen computervirussen en andere ongewenste elementen?

5.6.3 Dienstverleners en personeel

De beheerders van de faciliterende informatiesystemen en andere betrokken personen en dienstverleners moeten weten wat hun rechten, verplichtingen en verantwoordelijkheden zijn. Zo dient de autorisatie bij voorkeur per persoon en op maat geregeld te worden. In het algemeen krijgen personen (waaronder tijdelijk personeel) immers teveel toegangrechten. Diverse onderdelen van de elektronische marktplaats zullen niet toegankelijk hoeven en mogen zijn voor iedere betrokkene.[37] Hiermee dient rekening gehouden te worden bij het opstellen van onderhoud-, beheer-, detacherings- en andere dienstenovereenkomsten. Denk daarbij ook aan de beveiligingsdeskundige zelf.

---

[35] Hier wordt verwezen naar Hoofdstuk 3 van Merijn Seelt ter zake IT-infrastructuur.

[36] Veelal is een systeem en/of netwerk beveiligd met een enkele firewall. Dit is echter maar één linie van beveiliging. Het gehele systeem en/of netwerk loopt gevaar als de firewall doorbroken wordt. Een meer gelaagde beveiligingstructuur is derhalve gewenst.

[37] Hierbij valt bijvoorbeeld te denken aan het gedeelte van de elektronische marktplaats waar persoonsgegevens zijn opgeslagen.

De betrokkenen – waaronder het personeel – dienen zich ervan bewust te zijn hoe bedrijfskritisch de constante, adequate beveiliging is voor de elektronische marktplaats. Een onderdeel van dat permanente bewustzijn en het behouden van de nodige kennis, zal het volgen van cursussen en trainingen betreffen. Verder dienen zij op de hoogte gehouden te worden van het actuele beveiligingsbeleid van de elektronische marktplaats en schriftelijk te verklaren dat zij zich aan de gestelde eisen van beveiliging en geheimhouding zullen houden.

5.6.4 Toegang tot, en informatie op de marktplaats

Net als de andere betrokkenen dienen de participanten zich op controleerbare wijze te registreren, identificeerbaar te zijn en op maat geautoriseerd te worden. Daarnaast dient de toegang van de geautoriseerde participanten te worden bewaakt, geactualiseerd en zonodig stopgezet. Daarbij kan gebruik worden gemaakt van (i) controlemogelijkheden in bijvoorbeeld de registers van de Kamers van Koophandel, (ii) registratie en verzending van die (en alle andere) informatie op de elektronische marktplaats met behulp van encryptie (bijvoorbeeld door gebruikmaking van een adequaat 'Secure Socket Layer' protocol of een 'Secure Electronic Transaction' protocol) en (iii) een combinatie van identificatiegegevens en (niet voor de handliggende) wachtwoorden met (bijvoorbeeld) een chipkaart met digitale handtekening.[38] Het is verder aan te bevelen om de verleende autorisatie periodiek te heroverwegen, in te trekken of op te schorten indien de geautoriseerde participant een bepaalde periode geen gebruik heeft gemaakt van de marktplaats.

5.6.5 Verantwoordelijkheid voor beveiliging op de elektronische marktplaats

Wie beheert en onderhoudt de beveiliging en wat zijn de verplichtingen ter zake van de participanten? Wie beslist over de doelstellingen en gewenste niveaus van die beveiliging? Wat zijn de maatregelen en sancties indien er onverhoopt problemen voordoen? De antwoorden op deze vragen en aanverwante onderwerpen zullen zorgvuldig gedocumenteerd moeten worden. Deels kunnen zij worden opgenomen in de onderhoud- en beheerovereenkomsten die de diverse

---

[38] Een Secure Socket Layer protocol (SSL) is een bepaalde cryptografisch protocol dat het veilig versturen van gegevens via het internet regelt en mogelijk maakt. Let wel, SSL is niet 100% veilig; met veel moeite is het in principe te kraken. Het Secure Electronic Transaction protocol (SET) is veiliger dan SSL, maar voor SET dient wel speciale software geïnstalleerd te worden. Overigens bestaan voor beide beveiligde verbindingen (SSL en SET) verschillende standaarden. De internetsite van de organisatie die SET beheert is: www.setco.org. Overigens wordt er continue gewerkt aan een betere standaard ter bevordering van de veiligheid en daarmee de activiteiten op internet, zoals onder meer te lezen in *World Wide Web Consortium Issues XML Signature as a W3C Recommendation*, 14 februari 2002, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/.

niveaus ervan regelen. In diverse ondernemingen bestaat tegenwoordig de managementfunctie van 'chief information officer ' (CIO) of 'chief security officer' (CSO), dit om het bestuur en die bestuurder een bewuste en duidelijk verdeling van de verantwoordelijkheden te laten realiseren. Men zal tevens frequent dienen vast te stellen of het beveiligingsbeleid voldoet aan de wettelijke wet- en regelgeving en contractuele verplichtingen.

5.6.6 Informatie over mogelijke beveiligingsproblemen

Partijen kunnen afspraken maken over wederzijdse verplichtingen om elkaar onmiddellijk te informeren indien de beveiliging problemen vertoont of indien men denkt dat de beveiliging onvoldoende is en/of doorbroken gaat worden. De elektronische marktplaats zal daarvoor faciliteiten moeten aanbieden.

5.6.7 Informatie en afspraken over escalatie mogelijkheden

Voor gevallen dat een van de partijen van mening is dat de ander onvoldoende doet om een adequate beveiliging te waarborgen of in geval van andere klachten, zijn oplossingsgerichte escalatieregelingen en procedures wenselijk, waaronder mogelijkheden om geschillen op te laten lossen door externe deskundigen.[39]

5.7 Betaling en facturering

Voor participanten op een nieuwe markt als het elektronisch marktplein is het van belang te weten hoe er gefactureerd en betaald mag en/of moet worden.

5.7.1 Facturering

Iedere ondernemer die zaken of diensten levert aan een andere ondernemer (B2B) is verplicht een factuur te sturen, dit met name in verband met de administratie- en bewaarplicht en de te betalen B.T.W. en andere belastingheffingen. Dat geldt ook voor deelbetalingen en vooruitbetalingen. De factuur op papier is bekend, maar mag de factuur ook elektronisch worden verzonden? Vooruitlopend op de richtlijn ter zake[40] heeft de staatssecretaris van het Ministerie van

[39] Zo zijn er een tweetal ISO-normen (15408 en 17799) die bepaalde minimum beveiliging normeren, zijn er normen voor EDP audit onderzoek (bijvoorbeeld zoals beschreven op www.netcentrum.nl/ea/norm.htm) en kunnen ook andere externe deskundigen de beveiliging van de elektronische marktplaats controleren en certificeren (bijvoorbeeld zoals beschreven op www.tscheme.org).

[40] Op 4 december 2001 heeft de Europese Commissie het voorstel om de factuurvereisten (waaronder bepalingen voor elektronisch factureren) voor de B.T.W. in de Europese Unie te harmoniseren aangenomen, zodat vanaf 1 januari 2004 dezelfde voorwaarden gelden binnen de gehele Europese Unie dezelfde voorwaarden. Het betreft de richtlijn tot wijziging van Richtlijn 77/388 met het oog op de vereenvoudiging, modernisering en harmonisering van de terzake van de facturering geldende voorwaarden op het gebied van de B.T.W.

Financiën bij besluit met de ingangsdatum van 1 mei 2001 die vraag bevestigend beantwoord en daarbij enkele aanwijzingen gegeven voor het gebruik van elektronische facturen.[41] Naast de vereisten voor de opmaak van en de informatie op iedere (zowel papieren als digitale) factuur staat een tweetal vereisten centraal, te weten de authenticiteit van de herkomst (de factuur moet daadwerkelijk afkomstig zijn van de afzender) en de integriteit van de inhoud (de inhoud moet de complete, oorspronkelijke inhoud hebben en dus betrouwbaar zijn).[42] Hoewel er geen specifieke technologie wordt opgelegd voor het verwezenlijken van die twee vereisten, valt met name te denken aan een elektronische handtekening, een systeem van elektronische gegevensuitwisseling (EDI) of een bepaald, periodiek (papieren) overzicht van de verstuurde elektronische facturen.[43] Voornoemde elektronische handtekening moet minimaal en cumulatief voldoen aan de volgende vier vereisten: (i) de handtekening is op unieke wijze aan de ondertekenaar verbonden, (ii) maakt het mogelijk de ondertekenaar te identificeren, (iii) komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en (iv) is zodanig verbonden aan de gegevens waarop ze betrekking heeft, dat een wijziging van de gegevens achteraf kan worden vastgesteld. Overigens is in de praktijk gebleken dat de Belastingdienst nog altijd niet precies weet hoe zij daadwerkelijk moet omgaan met voornoemde vereisten en het besluit ter zake elektronisch factureren. Het is op dit moment dan ook aan te bevelen om contact op te nemen met de Belastingdienst om problemen achteraf te voorkomen.

5.7.2 Betaling

Betalingsmethoden ten behoeve van een elektronische marktplaats zouden idealiter veilige, gebruiksvriendelijke, snelle en kostenefficiënte elektronische betaling en ontvangst ervan mogelijk moeten maken. Verscheidene (bestaande en nieuwe) banken, creditcardmaatschappijen en andere gespecialiseerde dienstverleners hebben nieuwe varianten van betalingsmethoden ontwikkeld en op de markt gebracht. De diversiteit ervan is groot te noemen.[44] Daarnaast zijn de conventionele betalingsmethoden ook bruikbaar op een elektronische marktplaats.

---

41 Staatssecretaris Bos van het Ministerie van Financiën inzake het gebruik van elektronische facturen, Ministerie van Financiën, 26-4-2001, nr. CCP2001/1104M.

42 Een aantal van de minimale eisen van opmaak en informatie op een factuur is de datum van uitreiking, opvolgende nummering, naam en adresgegevens van de leverancier en de afnemer alsmede de hoeveelheid, aard en datum van de geleverde zaken en/of diensten en het toegepaste BTW-tarief.

43 Uitgebreide informatie over de elektronische handtekening en de andere mogelijkheden van de Public Key Infrastructure (PKI) is onder andere te vinden op, www.pkioverheid.nl/informatie/dehandtekening.htm. Verder wordt hier verwezen naar Hoofdstuk 4 van Serge Gijrath inzake elektronische handtekeningen alsmede naar B. Aalberts & S, van der Hof, 'Digital Signature Blindness', *ITeR-reeks 32*, Kluwer, Deventer 2000.

44 Voor een nader en meer gespecificeerd overzicht van de huidige betalingsmethoden: Electronic Commerce Platform Nederland/Nationaal Chipcard Platform, *Betalen op internet*, Leidschendam, januari 2000 (te lezen/downloaden via www.ecp.nl).

Creditcard

De creditcard is – bij gebrek aan een beter alternatief – de meest gebruikte en meteen minst veilige betaalmethode op internet. Het is in beginsel niet aan te raden om zo maar te betalen met een creditcard. Zelfs via een beveiligde verbinding (door middel van het SSL- of SET protocol) is een creditcard betaling niet volledig veilig te noemen; het zegt immers alleen wat over de verbinding tussen de creditcardhouder (de verzender) en de internetsite van de ontvanger, maar zegt niets over hoe goed het systeem van die ontvanger zelf beveiligd is. Bij gebruik van het SSL protocol is daarbij de identiteit van de verzender niet met zekerheid vast te stellen, met het SET protocol kan dat wel.

Diverse creditcardmaatschappijen trachten de veiligheid van de conventionele creditcard te verbeteren of de garanties anderszins te verhogen voor toepassingen op het internet.[45] Daarnaast bestaan er sinds kort nieuwe en veelbelovende manieren om met de creditcard of bankrekening veilige en snelle betalingen te doen.[46]

Elektronisch geld

Naast bovenstaande bezwaren ter zake het gebruik van een creditcard, leent die zich meestal niet voor relatief kleine aankopen, nu de transactiekosten dan te hoog zijn. Onder meer om die problemen op te lossen, trachten instanties systemen van digitaal geld te ontwikkelen; normale financiële waarde worden dan geconverteerd naar een elektronische waarde op een opslagmedium zoals een harde schijf van een computer of een chipcard. Een digitale portemonnee (of ook wel SET-wallet of E-wallet genoemd) dus. Na betaling wordt die elektronische waarde vervolgens door de betreffende bank omgezet in normale financiële waarde. [47]

Internetbankieren

Andere systemen betreffen bijvoorbeeld combinaties van een normale bankpas (of unieke code) met een fysieke kaartlezer of beveiligingscalculator. Deze laatste systemen worden – op zeer gevarieerde (en eigen)wijze – door de meeste Nederlandse banken gebruikt ter zake internetbankieren.

---

[45] Zo tracht Visa de door haar creditcards te vervangen voor een nieuw ontwikkelde creditcard die gebruikmaakt van de magneetstrip en geeft American Express ter zake sommige van haar creditcards een volledige garantie tegen ongeautoriseerde aankopen op het internet.

[46] Zo werkt het betalingsyteem van Paypal (www.paypal.com) eenvoudig, met de snelheid van een email en (voor zover op dit moment na te gaan) relatief veilig. Zie ook het 'Security Center' van Paypal, om te zien hoe zij de beveiliging, privacy en aanverwante onderwerpen regelt en de participanten informeert ter zake.

[47] Over de mogelijkheden en (juridische) problemen van elektronisch geld c.a., wordt hier verwezen naar E. de Ruiter, Betalingsaspecten, in: *De e-consument*, Elsevier 2000, p.111.

Rembours, acceptgiro & andere conventionele betalingsmethoden
Hoewel het bij een elektronische marktplaats in beginsel de bedoeling is om alle facetten (waaronder de facturering en betaling) van het handelen op elektronische wijze uit te voeren, zal dat meestal niet helemaal lukken, al was het maar omdat de te leveren zaak en/of dienst op een niet- elektronische wijze moet worden geleverd. Los daarvan zijn de meeste traditionele betalingsmethoden, zoals betaling onder rembours, via acceptgiro, per bankrekening of in contanten vertrouwd en in principe goed te combineren met een elektronische marktplaats.

5.7.3 Casus

De elektronische marktplaats voor en door boeren zal naar verwachting geen eigen betalingsmethode gaan ontwikkelen maar kiezen voor een of meerdere betaalmethoden die algemeen gangbaar en werkbaar zijn onder de (potentiële) participanten. Bij een B2B-(boeren)marktplaats lijkt een conventioneel betaalmiddel een mogelijke keuze, onder meer gezien de zaken en/of diensten die men levert of geleverd krijgt. Andere methoden zijn echter niet uitgesloten van (mede)gebruik; zelfs een variant op het model van internetbankieren behoort tot de mogelijkheden. Het is een kwestie van consensus tussen de partijen op het B2B-marktplein.

5.8 Slotopmerkingen

Voor marktwerking op een marktplaats zijn adequate faciliteiten noodzakelijk. Op een elektronische elektronische marktplaats voor en door boeren is dat niet anders. De werking van de huidige elektronische marktplaatsen wordt op dit moment vaak nog als teleurstellend ervaren. Toch wordt het potentieel ervan erkend.
Om een B2B-marktplein te beginnen en de continuïteit ervan te waarborgen, is het beschermen van de belangen van het marktplein en haar participanten van cruciaal belang. Indien de elektronische marktplaats een goede reputatie heeft en houdt ter zake beveiliging en betaling alsmede indien de participanten vertrouwen hebben en houden in de werking van de marktplaats, is in ieder geval één essentieel bestanddeel van marktwerking en een succesvolle marktplaats aanwezig.

Pas als de feitelijk basisvoorwaarden duidelijk zijn, heeft het zin om die en de juridische uitwerking ervan op maat te formuleren en vast te leggen in overeen-

komsten, beleidsregels, protocollen en andere documenten. Met behulp van een interdisciplinair team aan deskundigen zal een B2B-initiatief een goede start kunnen maken en als B2B-markt met levendige handel kunnen voortbestaan.