

Ontwikkelingen op het gebied van e-assurance

M.A.J. de Haas RA en drs. J.J. van Beek RE RA

In de Compact die ingaat op de rol van de ICT-audit in het kader van de accountantscontrole, mag een artikel over de ontwikkelingen op het gebied van e-assurance niet ontbreken. Gezien hun opleiding en deskundigheid is zowel de accountant als de ICT-auditor uitstekend toegerust om in de komende jaren nieuwe diensten op dit gebied te ontwikkelen. In het artikel wordt op een aantal actuele ontwikkelingen ingegaan.

Inleiding

Het World Wide Web heeft momenteel in verhoogde mate de aandacht van bedrijven en particuliere gebruikers. Geen week gaat voorbij of nieuwe verwachtingen worden gepubliceerd over de snelle groei van het aantal en type transacties over de elektronische snelweg. Tegelijkertijd worden door gebruikers en bedrijven terecht vragen gesteld over de integriteit van transacties, de betrouwbaarheid van gegevens in de Internet-omgeving, etc. Juist in de grotendeels anonieme omgeving van Internet en e-commerce is er behoefte aan assurance in enige vorm, waarbij een onafhankelijke derde partij naar alle waarschijnlijkheid een belangrijke rol kan spelen. Gezien de traditionele positie die de accountant en de ICT-auditor hebben op dit gebied in het zakelijk verkeer is het noodzakelijk dat zij ook tijdig hun rol bepalen op het gebied van e-assurance.

In dit artikel zal na het definiëren van enkele begrippen worden ingegaan op een aantal actuele ontwikkelingen op het gebied van e-assurance die op het raakvlak liggen van de deskundigheid van de accountant en de ICT-auditor en waar zij vaak in samenwerking zullen optreden. In andere artikelen is reeds ingegaan op de wijze waarop deze samenwerking vorm kan krijgen. Relatief veel aandacht zal worden besteed aan het toevoegen van vertrouwen bij e-commercetransacties door middel van WebTrust. Daarnaast zullen kort enkele nieuwere vormen van e-assurance worden beschreven. Dit zijn het toevoegen van zekerheid bij een opgave van het aantal bezoekers van een website (verder te noemen aantal 'hits') en het beoordelen van risico's en beheersmaatregelen van organisaties die volledig gebruikmaken van de Internet-technologie voor hun business.

Wat is e-business?

Zakendoen via Internet wordt vaak met e-commerce aangeduid. Er bestaat geen breed aanvaarde definitie van het begrip e-commerce. Een veelgebruikte is: *'Elektronisch zakendoen zijn alle vormen van transacties die gerelateerd zijn aan commerciële activiteiten, waarbij zowel organisaties als individuen betrokken zijn en die zijn gebaseerd op het verwerken en verzenden van gedigitaliseerde data'*.

Indien organisaties voor het automatiseren van hun processen in de breedte gebruik gaan maken van Internet-technologie, dan wordt dit aangeduid met e-business. Deze werkwijze biedt een groot aantal voordelen: door koppeling van systemen met leveranciers kan inkoop plaatsvinden zodra er iets verkocht is (Just in Time), applicaties kunnen worden geoutsourced en via Internet benaderbaar gemaakt (webbased applicaties via Application Service Providers), en er kan geopereerd worden tegen de laagst mogelijke kosten. Verder kan een organisatie die op deze wijze de Internet-technologie gebruikt, snel voldoen aan de veranderende marktvraag (flexibiliteit) en heeft zij de beschikking over bruikbare klantinformatie. E-commerce is gericht op de commerciële processen en is daarmee een onderdeel van e-business.

De volgende definities zullen worden gehanteerd voor e-commerce en e-business:

- * *e-commerce*: het elektronisch zakendoen via Internet in al zijn verschijningsvormen;
- * *e-business*: het optimaliseren van bedrijfsprocessen door gebruik te maken van Internet-technologie;
- * *e-businesses*: als in dit artikel wordt gesproken over e-businesses, Internet-organisaties of Internet-bedrijven, worden hiermee organisaties bedoeld die Internet gebruiken als primair verkoopkanaal (e-commerce). Alhoewel de grens moeilijk te trekken is, vallen toeleveranciers zoals Cisco of technische access providers zoals World Online hier niet onder.

Risico's van Internet

Bij alle vormen van Internet-gebruik is er sprake van een vorm van communicatie. Continu worden berichten (in de vorm van 'pakketjes') verstuurd tussen de gebruiker en de computers ('servers') waarop de informatie staat. Of er nu gevoelige informatie wordt verstuurd of niet, men dient zich te realiseren dat dit niet zonder risico is. Informatie die via Internet wordt verstuurd, kan door derden worden gelezen of verminkt en ontvangst ervan is niet eenvoudig vast te stellen. Men zal zich dus bewust moeten zijn van het feit dat Internet als communicatiemedium per definitie niet betrouwbaar is. Dit wordt veroorzaakt door de volgende factoren:

- * De beschikbaarheid van de Internet-verbinding is niet zonder meer gewaarborgd.
- * De betrouwbaarheid van het berichtenverkeer is zonder aanvullende maatregelen niet gewaarborgd.
- * Het is niet eenvoudig aantoonbaar dat een bericht afkomstig is van de vermelde afzender noch dat een bericht is ontvangen door geadresseerde.



Als het uitwisselen van informatie via Internet zoveel risico's met zich meebrengt kan de vraag worden gesteld of Internet in feite wel geschikt is als medium voor zakelijk gebruik. Dat dit medium hier de laatste jaren toch op grote schaal voor wordt gebruikt, komt doordat het Internet Protocol (TCP/IP) zich als de-factostandaard voor open netwerken heeft ontwikkeld, en doordat het medium goedkoop is en geweldige mogelijkheden biedt om rechtstreeks met klanten te communiceren. Gezien de hierboven beschreven risico's zullen echter wel aanvullende beheersmaatregelen moeten worden getroffen.

Internet is als communicatiemedium
per definitie niet betrouwbaar.

Assurance bij transacties: WebTrust

Het aantal Nederlanders dat 'on line' is, loopt tegen de vijf miljoen¹. Deze grote groep consumenten *lijkt* minder terughoudend geworden om bestellingen te plaatsen via het net. Toch valt het aantal geslaagde transacties dat door deze groep is geplaatst, tegen. Uit verschillende onderzoeken² is gebleken dat onzekerheden bij consumenten een belangrijke drempel vormen voor de groei van e-commerce. Deze onzekerheid wordt veroorzaakt doordat er grote verschillen zitten tussen on line en op een traditionele manier iets kopen. Omdat meestal geen gebruik kan worden gemaakt van het 'gelijk oversteken'-principe (goederen voor geld), zit de consument met de volgende vragen:

- * Krijg ik wel wat ik heb besteld?
- * Wanneer krijg ik wat ik heb besteld?
- * Kan ik veilig betalen?
- * Waar kan ik terecht met mijn vragen of klachten?
- * Kan ik de geleverde spullen terugsturen?
- * Wat doet men met mijn (privacygevoelige) gegevens?

Een speciaal hierop gericht onderzoek³ heeft uitgewezen dat onzekerheid kan worden weggenomen door het geven van adequate informatie aan de twijfelende consument en het toevoegen van zekerheid over deze informatie door een onafhankelijke partij.

De Amerikaanse en Canadese beroepsinstellingen van accountants⁴ hebben medio 1996 het gebrek aan vertrouwen in e-commerceomgevingen gesignaleerd en hierop ingespeeld door de introductie van het WebTrust-programma. Het doel van dit programma is door het afgeven van een digitaal certificaat (verder te noemen het 'WebTrust-zegel') door de accountant, de consumenten het vertrouwen te geven dat er sprake is van een degelijk bedrijf, dat transacties correct zullen worden afgehandeld en dat betrouwbaar met de verstrekte gegevens zal worden omgegaan. Een dergelijke onafhankelijke verificatie door accountants en IT-auditors, uitmondend in het WebTrust-zegel op de website, verleent consumenten een grote mate van vertrouwen in de achterliggende organisatie.

Ook het Koninklijk NIVRA ontplooit momenteel diverse activiteiten op het gebied van WebTrust. Naar verwachting zal binnenkort een licentie met het AICPA worden getekend waarna ook accountantskantoren zonder een internationale licentie WebTrust kunnen aanbieden.

De managementverklaring en de WebTrust-principes

Het WebTrust-zegel is op bepaalde punten vergelijkbaar met de accountantsverklaring. Om deze analogie verder uit te diepen: de accountantsverklaring zegt iets over het getrouwe beeld van de getoonde informatie, het WebTrust-zegel zegt iets over de betrouwbaarheid van de e-commerceaanbieder. Meer specifiek: over het getrouwe beeld van de managementverklaring.

Verklaring van het management van XYZ

Onderneming XYZ verklaart op haar website (www.XYZ.nl) het volgende:

Wij hebben onze leveringsvoorwaarden inzake e-commercetransacties op deze Internet-site openbaar gemaakt. Alle opdrachten die langs deze elektronische weg tot stand komen zullen conform deze voorwaarden worden uitgevoerd.

Wij hebben effectieve maatregelen getroffen om redelijkerwijs te kunnen garanderen dat bestellingen die door middel van e-commerce worden geplaatst, op de daarover overeengekomen wijze worden gefactureerd en uitgevoerd.

Wij hebben effectieve maatregelen getroffen om redelijkerwijs te kunnen garanderen dat klantgegevens verkregen door middel van e-commerce niet voor gebruik buiten ons bedrijf worden aangewend.

Geldend voor de periode van 1 februari 2000 tot 31 maart 2000 conform de AICPA/CICA WebTrust-criteria.

Kader 1. Voorbeeld van een managementverklaring.

Op een prominente plaats op de website publiceert het management een verklaring waarin zij verklaart dat de organisatie de drie WebTrust-principes onderschrijft. De drie WebTrust-principes behandelen drie van de fundamenten van e-commerce:

* *Openheid van zaken (business practice disclosure)*. Is op de website alle relevante informatie opgenomen omtrent de achterliggende organisatie, hoe wordt omgegaan met privacygevoelige gegevens en klachten en heeft het management maatregelen getroffen om te waarborgen dat transacties volgens de op de website gepubliceerde wijze worden uitgevoerd?

* *Integriteit (transaction integrity)*. Zijn er voldoende effectieve beheersmaatregelen geïmplementeerd die met een redelijke mate van zekerheid zorg dragen dat transacties juist en volledig worden afgewerkt en dat artikelen/diensten voor de juiste prijzen in rekening worden gebracht?

* *Beveiliging (information protection)*. Zijn er voldoende maatregelen getroffen om met een redelijke mate van zekerheid ervoor te zorgen dat privacygevoelige gegevens van consumenten zijn beveiligd tegen raadpleging en gebruik door derden en wordt de consument een keus geboden indien gegevens worden gebruikt voor andere dan puur interne doeleinden?

Deze WebTrust-principes sluiten in het algemeen naadloos aan op de eisen die een bedrijf zichzelf stelt om een betrouwbare organisatie op te zetten zowel in de traditionele als in de digitale wereld. De gehanteerde normen wijken ook niet wezenlijk af van andere zegels, zoals WebTrader van de Consumentenbond. Een groot verschil tussen beide zegels zit in de mate van zekerheid. Het WebTrust-zegel gaat vergezeld van een uitgebreid verificatieonderzoek door een derde partij (de accountant/ICT-auditor), bij een WebTrader-zegel ontbreekt dit element.

Een organisatie die geïnteresseerd is in een WebTrust-audit en -zegel krijgt van haar accountant een WebTrust-self-assessment vragenlijst waarmee zij kan toetsen in hoeverre de inrichting en opzet van haar website, de e-commerceactiviteiten en de back-office voldoen aan WebTrust-principes. Indien het management tot een positief oordeel komt kan men aan de accountant vragen een WebTrust-audit te verrichten.

De WebTrust-audit

De WebTrust-audit wordt uitgevoerd door een multidisciplinair team van IT-auditors (technische Internet-specialisten), accountants en eventueel aangevuld met e-businessconsultants. Het onderzoek is globaal als volgt gefaseerd:

1. *Verkrijgen van inzicht in de bedrijfsactiviteiten en in de opzet van de website.*

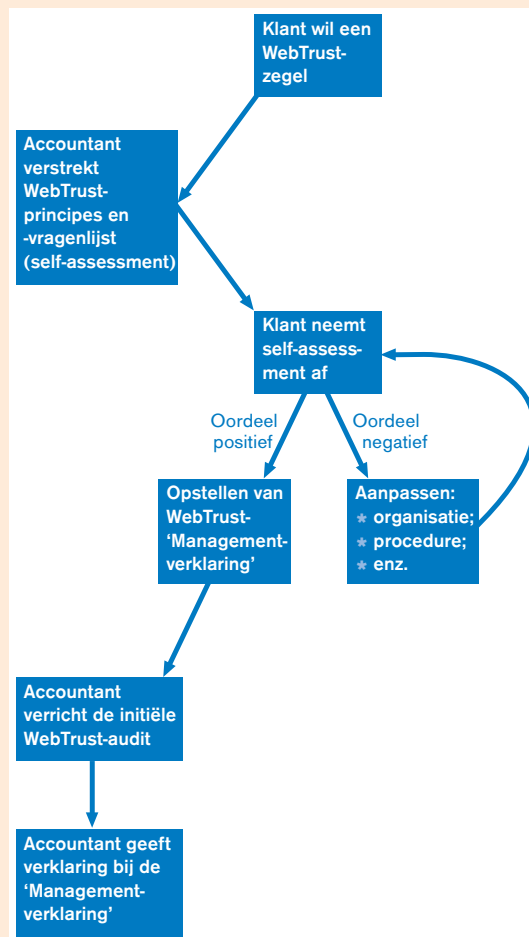
In deze fase wordt inzicht verkregen in de bedrijfsdoelstellingen, de kritieke succesfactoren en de beheersstructuur. Risico's die de realisatie van de e-commerce doelstellingen bedreigen, worden in deze fase globaal in kaart gebracht.

2. *Vaststellen in hoeverre wordt voldaan aan de WebTrust-principes (business disclosure, transaction integrity en information protection) en eventueel rapporteren indien wijzigingen noodzakelijk zijn.*

In deze fase zal specifiek aandacht worden besteed aan de inhoud en opzet van de website en de e-commerceactiviteiten. Op basis van de kennis van de bedrijfsactiviteiten, de bedrijfsdoelstellingen en de gesignaleerde risico's wordt een raamwerk van eisen van interne controle opgesteld, gebaseerd op de WebTrust-principes.

3. *Vaststellen in hoeverre de getroffen maatregelen van interne controle (in opzet en bestaan) voldoende effectief zijn om met een redelijke mate van zekerheid te waarborgen dat orders juist en volledig worden afgewerkt en dat artikelen/diensten voor de juiste prijzen in rekening worden gebracht.*

De getroffen maatregelen van interne controle worden geïnventariseerd. Voorts wordt geëvalueerd in hoeverre



Figuur 1. Naar de WebTrust-mededeling⁵.

dit stelsel van maatregelen in opzet voldoet aan de gestelde eisen van interne controle.

4. *Vaststellen of de informatiebeveiliging toereikend is.* In deze fase wordt aandacht besteed aan de technische infrastructuur en de getroffen beveiligingsmaatregelen rondom de privacygevoelige informatie.

5. *Rapporteren en (indien alle eventueel geconstateerde tekortkomingen zijn opgelost) het uitgeven van het WebTrust-zegel.*

De bevindingen worden gerapporteerd. Het rapport zal naast de conclusie tevens de belangrijkste bevindingen en aanbevelingen ter verbetering bevatten.

Het 'zegelproces'

Het verkrijgen van een zegel

Nadat het WebTrust-onderzoek is afgerond en is vastgesteld dat de organisatie over een bepaalde periode (meestal tussen de twee en drie maanden, te weten de doorlooptijd van het onderzoek) aan de eisen heeft voldaan, wordt een verklaring verstrekt op basis waarvan het zegel kan worden verkregen.

Het behouden van het WebTrust-zegel

Om het zegel te behouden dienen de bovengenoemde werkzaamheden in grote lijnen eens in de drie maanden

5) Artikel M. de Haas: 'Vertrouwen in e-Commerce', De Accountant, november 1999.



Figuur 2. Het WebTrust-zegel.



te worden herhaald. De frequentie en diepgang van een dergelijk onderzoek is afhankelijk van onder andere:

- * de aard en complexiteit van de activiteiten van de onderneming;
- * de frequentie waarmee belangrijke veranderingen op de site worden aangebracht;
- * de effectiviteit van de beheersingssystemen van de onderneming (inclusief change management) die waarborgen dat de WebTrust-criteria worden nageleefd, en
- * het vakkundig oordeel van de accountant.

In geen geval mag de periode tussen twee onderzoeken langer dan drie maanden zijn. In de tussentijdse periode dient de onderneming de accountant te informeren omtrent belangrijke veranderingen in algemene voorwaarden, processen en beheersingsmaatregelen indien dergelijke veranderingen het naleven van de WebTrust-criteria mogelijk beïnvloeden. Dergelijke veranderingen leiden mogelijk tot versneld onderzoek of zelfs tot verwijdering van het zegel totdat een nieuw onderzoek heeft plaatsgevonden.

Vereiste deskundigheid

Alhoewel de accountant bij een WebTrust-audit de eindverantwoordelijkheid draagt vereist de aard van de WebTrust-audit een veelheid aan deskundigheid. Bij de uitvoering van een WebTrust-audit heeft de auditor te maken met:

- * de organisatie die transacties verwerkt, haar beleid en de getroffen internecontrolemaatregelen;
- * de processen en systemen die de elektronische transacties ondersteunen;
- * de relevante wetgeving (privacy, leveringsvoorwaarden, etc.);
- * de netwerk- en ICT-platformen inclusief de getroffen beveiligingsmaatregelen.

Om de risico's die samenhangen met het gebruik van Internet als primair verkoopkanaal goed te kunnen inschatten, evenals het vertalen van enkele algemene WebTrust-normen (denk bijvoorbeeld aan de 'business practice disclosure'-principes) naar een specifieke organisatie, zal een beroep worden gedaan op een e-business-deskundige. Dit kan een e-businessconsultant zijn of een op dit gebied geschoolde IT-auditor.

Voor het beoordelen en controleren (opzet, bestaan en werking) van de back-officeprocessen is de accountant de deskundige bij uitstek. De informatiebeveiliging zal over het algemeen dienen te worden beoordeeld door een IT-auditor.

Verdere ontwikkeling van WebTrust

Ondanks het feit dat een WebTrust-zegel onzekerheden wegneemt van consumenten op Internet en de audit het management inzicht verschaft in tekortkomingen, neemt het aantal afgegeven zegels slechts mondjesmaat toe. Schrikt de relatief zware audit e-commerceorganisaties af of is er iets anders aan de hand?

De praktijk leert dat hiervoor twee oorzaken zijn te onderkennen. Ten eerste is het voor een gemiddelde (jonge) Internet-organisatie een zware audit waarvoor

men niet eenvoudig 'slaagt'. Deze Internet-startups zijn nog niet erg stabiel en de markt is nog volop in ontwikkeling. Ten tweede hebben deze organisaties veel processen geoutsourced en het blijkt dat het samenbrengen van deze processen geen eenvoudige zaak is. Slechts een fractie van de Nederlandse on-linebedrijven heeft haar Internet-zaken echt voldoende geregeld als de WebTrust-norm wordt gehanteerd.

Veel van deze vaak jonge bedrijven zijn vol goede bedoelingen van start gegaan maar de consumenten lopen risico's. Denk hierbij bijvoorbeeld aan een onvoldoende beveiliging van privacygevoelige gegevens. Vrijwel dagelijks komen er incidenten in de pers waarbij hackers informatie van klanten lezen of openbaar hebben gemaakt en wat de pers haalt is slechts het topje van de ijsberg.

Een andere constatering is dat het WebTrust-zegel zich richt op de zogenaamde business-to-consumer (B2C)-markt waarin de accountant en de IT-auditor relatieve onbekenden zijn. De vraag is of zij zich in deze markt een duidelijke positie kunnen verwerven⁶. De meer traditionele markt voor accountants en IT-auditors is de business-to-business (B2B)-markt, waarin overigens de komende jaren de grootste groei wordt verwacht. Ook daar is (Web)Trust een noodzaak. Wij verwachten dat WebTrust zich de komende tijd verder zal ontwikkelen richting de B2B-markt.

In ieder geval is WebTrust een belangrijke bron van ervaring om te leren over e-business, wat de impact hiervan is op organisaties en welke bijdrage de accountant/ICT-auditor op dit nieuwe aandachtsgebied kan leveren.

Andere vormen van e-assurance

Naast de vraag naar assurance over transacties zijn er andere actuele vragen op het gebied van e-commerce waar een onafhankelijke derde vertrouwen kan toevoegen.

Een voorbeeld hiervan betreft de factoren die de waarde van een e-business bepalen. De afgelopen tijd zijn diverse Internet-organisaties voor aanzienlijke bedragen naar de beurs gebracht. Waardering van deze ondernemingen blijkt erg moeilijk en is soms voornamelijk gebaseerd op een onduidelijk bepaalde omzet, de kwaliteit van het management, de strategie en het aantal bezoekers of het aantal abonnees van de website. Verder blijkt het lastig te bepalen wat wel en wat niet tot de omzet van een e-business moet worden gerekend. Momenteel worden over deze onderwerpen veel vragen gesteld aan de accountant/ICT-auditor. Welke zekerheid kan hij op dit gebied verschaffen?

Om inzicht te krijgen in de kwaliteit van een e-business op basis van risico's en de aanwezige beheersmaatregelen hanteert KPMG momenteel twee methodieken met allebei een eigen invalshoek, te weten de 'E-Business Review' (EBR) en de 'Web Risk Management Benchmark' (WRMB). Bij de EBR ligt de nadruk op de organisatorische aspecten beredeneerd vanuit de business-

6) Prof. dr. P. Wallage RA, *De ontwikkeling van e-handel: een kwestie van vertrouwen*, Management & Informatie, 7e jaargang, 1999, p. 51-58.

risico's, bij de WRMB ligt de nadruk meer op de technische aspecten en de risico's die daaruit voortvloeien. Beide methodieken maken gebruik van standaardvragenlijsten en de resultaten kunnen worden gebenchmarkt ten opzichte van de brancheleden.

De omzet die moet worden toegerekend aan een Internet-organisatie en het toevoegen van zekerheid hieromtrent wordt bij uitstek tot het kennisdomein van de accountant gerekend. Maar omzet is niet altijd eenvoudig te bepalen en er kunnen discussies ontstaan over wat tot de omzet moet worden gerekend. Een paar voorbeelden ontleend aan een discussienota van de Amerikaanse SEC⁷:

- * Veel organisaties treden op als tussenpersoon en geven elkaar provisies (bijvoorbeeld 15% Amazon) en reclameruimte; wat is hiervan de waarde, wie loopt het debiteurenrisico, etc.
- * Wat te doen met kosten van weggevertjes om klanten te binden (als kosten nemen, activeren, aftrekken van omzet?).
- * Hoe krijgen we zekerheid over de omzet als voor een belangrijk deel wordt afgerekend op basis van 'clicks', 'hits' en 'views'?

Vragen hieromtrent zijn actueel bij overnames maar eveneens bij een jaarrekeningcontrole. In technische omgevingen zoals Internet is de inbreng van een IT-auditor echter essentieel. Binnen KPMG wordt hiervoor de internationale aanpak 'revenue-assurance' gebruikt. Aan de hand van een gedetailleerde procesbeoordeling op basis van de BPA-methodiek, aangevuld met een technische beoordeling van de gebruikte programmatuur, instellingen en dergelijke, kan een uitspraak worden gedaan over de juistheid, volledigheid of tijdigheid van de gerapporteerde omzet.

In het vervolg van dit artikel zal worden ingegaan op de problematiek rondom het aantal hits en de zelfstandige waarde die hier door (risico-)investeerders aan wordt toegekend.

Waarde gebaseerd op het aantal hits?

Een opgave van het aantal hits wordt relevant als de marktwaarde van een Internet-bedrijf moet worden bepaald en betere factoren voor een dergelijke bepaling ontbreken. Hierbij moet worden gedacht aan de volgende elementen: directe omzet uit verkoop van producten, omzet uit reclameopbrengsten, provisieomzet, het aantal geregistreerde leden/gebruikers of het aantal bezoekers van de website. Een kopende partij zal geïnteresseerd zijn in de juistheid van het aantal hits op een website. Maar wat zegt een hit? Er hoeft niets gekocht te zijn, de site hoeft niet eens daadwerkelijk te zijn bekeken, alleen al het simpele feit dat de webpagina is opgevraagd zegt al iets over de commerciële potentie van de website. Een potentiële klantenkring van 300.000 per maand is bijvoorbeeld veel meer waard dan een van 50.000.

Er bestaat geen eenduidige definitie van wat een hit precies is. Gebruikte definities zijn:

- * het opvragen van een enkele pagina (inclusief alle op deze pagina aanwezige frames) op een website door een gebruiker;

- * het openen van meerdere pagina's. Een hit is dan gelijk aan de sessie.

De meest voorzichtige is de laatste: een hit is gelijk aan een bezoek aan de website. Voor dit artikel zal dan ook impliciet deze laatste worden gehanteerd.

Ervan uitgaande dat een derde partij zekerheid wil over het door de verkopende partij opgegeven aantal hits, zal deze partij met name geïnteresseerd zijn in de juistheid hiervan. Hiermee lijkt de controle van het aantal hits op een website op het eerste gezicht qua problematiek vergelijkbaar met een oplageverklaring. Toch is er een groot aantal complicerende factoren die deze vergelijking mank laten gaan. Het grote verschil zit 'm in het ontbreken van een fysieke goederenstroom, waardoor het leggen van controleverbanden onmogelijk is; verder is het object van de controle een database met hierin de statistische informatie betrekking hebbend op het aantal hits.

Voorwaarden

Het aantal hits moet vergeleken worden met het aantal bezoekers die een winkel binnen zijn gelopen. In plaats van een meetapparaatje met een teller op de winkeldeur wordt elke pagina voorzien van een virtueel label. Een statistiekprogramma houdt bij wanneer de pagina (en dus het label) wordt opgevraagd. Uiteraard telt het statistiekprogramma precies op de wijze waarop dit geconfigureerd is. Het is bijvoorbeeld heel eenvoudig enkele van de meest populaire pagina's tijdelijk van meerdere labels te voorzien. Omdat het ontdekken van dergelijke fouten de kennis van de gemiddelde accountant te boven gaat, zal de accountant voor de controle van het aantal hits in belangrijke mate steunen op het werk van een IT-auditor.

Het is feitelijk niet mogelijk om met enige mate van zekerheid een uitspraak te doen omtrent de in het verleden gegenereerde hits op de website.

Als de vraag naar controle op de juistheid van het aantal hits achteraf komt, zal de accountant zijn klant waarschijnlijk moeten teleurstellen. Het is feitelijk niet mogelijk om met enige mate van zekerheid een uitspraak te doen omtrent de in het verleden gegenereerde hits op de website. Daarvoor zijn er te veel complicerende factoren:

- * Hoe stel je vast dat een statistiekpakket de hele periode juist heeft gewerkt en dat de configuratie niet ten nadele is veranderd?
- * Hoe voorkom je dubbelstellingen en hoe kom je erachter dat hits niet door de organisatie zelf worden gegenereerd?
- * Wat is de invloed van acties die gebruikers tijdens een korte periode naar een bepaalde website hebben gelokt?

Deze situatie is overigens vergelijkbaar met de jaarrekeningcontrole. Als de accountant achteraf wordt gevraagd

7) Accounting Issues Related to Internet Operations for EITF Consideration, SEC oktober, 1999.



M.A.J. de Haas RA is werkzaam bij KPMG Information Risk Management bij de business unit Electronic Commerce te Amstelveen. Na het afronden van zijn RA-studie in 1997 is hij werkzaam als IT-auditor. Zijn primaire aandachtsgebied betreft assurance in Internet-omgevingen en in die hoedanigheid is hij betrokken bij internationale productontwikkeling van KPMG op het gebied van e-business en assurance.

Drs. J.J. van Beek RE RA is als directeur werkzaam bij KPMG Information Risk Management. Hij heeft een jarenlange ervaring in alle aspecten van het IT-auditvakgebied, met een zwaartepunt in het beoordelen van en adviseren over de geautomatiseerde informatievoorziening bij financiële instellingen. Hij is lid van de Commissie Organisatie van de Informatie Voorziening van het Koninklijk NIVRA, waar nieuwe e-assurance-diensten momenteel veel aandacht krijgen. Zijn bijdrage aan dit artikel is op persoonlijke titel.

een controle over een afgesloten boekjaar te verrichten zal hij (op z'n best) niet verder kunnen komen dan een zelfstandig balansonderzoek; hij kan de werking van bepaalde processen niet achteraf vaststellen.

Zekerheid over het aantal hits

Op grond van wat hiervoor globaal is besproken zou een mogelijke aanpak er als volgt uit kunnen zien:

1. Verkrijgen van inzicht in de activiteiten, risicoanalyse en aanpak hierop afstemmen.

Afbakenen van een periode waarover het aantal hits betrekking heeft, de definitie van een hit vaststellen en het 'bevrozen' van de database. Hiervan dient een kopie (bijvoorbeeld op tape) aan de accountant te worden overhandigd, zodat hij diverse cijferbeoordelingen kan verrichten op de informatie.

2. Zekerheid verkrijgen omtrent de gebruikte techniek.

In deze fase wordt aandacht besteed aan de afgeschermdes logbestanden en de netwerkconfiguratie (geeft een indruk van de capaciteit en hierbij een maximumpositie), maar ook aan zaken als de configuratie van de firewall en de betrouwbaarheid van de gebruikte applicaties voor het genereren van statistische informatie omtrent het bezoek van de website.

3. Beoordeling opzet, bestaan en werking van de IT-organisatie.

Denk hierbij aan de procedures rondom change management en omtrent functiescheiding in de IT-organisatie om enige zekerheid omtrent de stabiliteit van de configuratie en de betrouwbaarheid van de database te verkrijgen.

4. Detailcontroles op de database.

In deze fase wordt de database onderworpen aan diverse 'cijferbeoordelingen'. Aandachtspunten hierbij zijn:

- * trends (algemene ontwikkeling);
- * vreemde pieken;
- * seizoensinvloeden (over de onderzoeksperiode).

Bepaalde acties of andere 'vreemde' pieken met een materiële invloed op het resultaat (het aantal hits) zullen mogelijk moeten worden geëlimineerd.

5. Overige detailtests.

Tijdens een bepaalde periode kan de accountant het bezoek van een website meten en deze gegevens afzetten tegen de in fase 4 ontdekte trends.

Ten slotte

In dit artikel is ingegaan op de ontwikkeling van het zakelijk gebruik van Internet en de rol van de accountant en de IT-auditor hierin. Door veel particuliere en zakelijke gebruikers wordt aangegeven dat de risico's die het gebruik van Internet voor zakelijke transacties met zich meebrengt, nog steeds een belangrijke belemmering vormen om op grote schaal aankopen te doen. Een belangrijke constatering is dat ook in de nieuwe economie een grote behoefte bestaat aan assurediensten. Accountants en IT-auditors zullen hier in samenwerking op dienen in te spelen. In dit artikel is een aantal ontwikkelingen op het gebied van e-assurance beschreven waarbij met name aandacht is besteed aan WebTrust en assurance op het gebied van transacties. WebTrust mag zich verheugen op een grote belangstelling in de markt en momenteel worden over de hele wereld door accountants/IT-auditors de eerste WebTrust-audits verricht. Daarnaast is kort stilgestaan bij assurance over een aantal andere onderwerpen in de e-commercewereld. Ook voor deze e-assurediensten bestaat veel belangstelling, maar met de uitvoering van onderzoek hebben nog weinig accountants/IT-auditors ervaring en verdere uitwerking is dan ook noodzakelijk. De ontwikkelingen op dit gebied zijn nog volop gaande en de uiteindelijke vorm waarin de accountant/IT-auditor zijn bijdrage zal gaan leveren, is nog niet definitief bepaald. Als de voortekenen ons echter niet bedriegen, wordt e-assurance een vast onderdeel van het werkgebied van de accountant/IT-auditor.

Literatuur

Mw. mr. drs. M.J. Dontje, *No trade without trust*, Compact 1999/6.

Mw. drs. M.J.A. Koedijk RA, *Business Process Analysis en de jaarrekeningcontrole; een praktijkcasus*, Compact 2000/2.

R. de Korte en J.J. van Beek (eindredactie), *Accountant en Internet; Op weg naar de E-accountant!*, artikel van de COIV, te publiceren in de Accountant, juni 2000.

Prof. dr. P. Wallage RA, *De ontwikkeling van e-handel: een kwestie van vertrouwen*, Management & Informatie, 7e jaargang, 1999, p. 51-58.