De ICT-auditor en e-Business Security

Ir. P. Kornelisse RE

In dit artikel wordt stilgestaan bij de ondersteuning die door ICT-auditors kan worden geleverd in de verschillende fasen van een e-businessproject, evenals bij de beoordeling door de ICT-auditor van de aandachtsgebieden die van belang worden geacht bij een e-Business Service. Hierbij komen ook webzegels aan de orde, zoals die van WebTrust en ZekeRE Business.

Inleiding

De cliënt verwacht steeds meer toegevoegde waarde van een ICT-auditor. Steeds vaker blijkt het niet voldoende te zijn om pas bij de oplevering van een systeem een oordeel af te geven. De cliënt wil binnen een project zo snel mogelijk weten of aan alle te onderkennen risicogebieden voldoende aandacht wordt geschonken. Vlak voor de oplevering van een project wordt vervolgens gevraagd om een 'groene vlag' van de ICT-auditor. Het oordeel van de ICT-auditor dient dan een 'groene vlag', een positive assurance te geven. Dit geldt in het bijzonder in de snelle wereld van de e-business.

Juist bij de realisatie van veilige e-Business Services wordt van de ICT-auditor een hoog tempo van werken en opleveren gevraagd. Niet voor niets wordt wel eens gezegd dat een internetjaar veel korter is dan een mensenjaar.
Door dit hoge tempo van werken veranderen de verwachtingen ten aanzien van het functioneren van ICT-auditors. Een nadere overweging is gewenst aangaande de rol van de ICT-auditor bij een e-businessproject.

Ontwikkelfasen bij e-Business Security

In een tijd dat voor elk begrip een 'e' lijkt te worden geplakt, is het niet eenvoudig de betekenis van de e-Business Security duidelijk te krijgen.
In dit artikel wordt voor de eenvoud bij e-Business Services uitgegaan van services die niet zozeer worden toegepast door gebruikers binnen een organisatie zelf, maar juist on line beschikbaar zijn gesteld aan afnemers (consumenten en bedrijven). Het betreft dus zowel B2C (Business to Consumer) als B2B (Business to Business). Daarmee richt e-Business Security zich op de beveiliging van alle applicaties die on line beschikbaar worden gesteld aan de afnemers van de organisatie.

Organisaties ontwikkelen de eigen e-Business Services veelal volgens een vast stramien, van presence naar interactie, transacties en transformatie. Bij de overgang naar volgende fasen van ontwikkeling van e-Business Services dienen ook de te treffen beveiligingsmaatregelen te worden versterkt, want bij elke ontwikkelfase treden additionele risico's op en zijn bijgevolg additionele beveiligingsmaatregelen vereist.

In tabel 1 zijn per ontwikkelfase ter indicatie risico's en te treffen beveiligingsmaatregelen geformuleerd.

E-businessfase	Risico's	Voorbeelden van beveiligingsmaatregelen	Toelichting
* Presence	* Imagoschade	* Bescherming webserver met firewall en veilige configuratie van platforms * Geen authenticatie	* De aanwezigheid op internet betreft informatieve diensten
* Interactie	* Schending privacy	* Beveiliging op applicatieniveau (web- en databaseserver) * Authenticatie op basis van kennis	* Een gebruiker kan eigen informatie vastleggen
* Transactie	* Onjuiste transacties * Onjuiste goederen- of geldstromen	* Zware voorzieningen betreffende detectie van mogelijke inbraken * Authenticatie op basis van kennis en bezit	* Initieel als additioneel transactiekanaal naast conventionele kanalen
* Transformatie	* Omzetderving	* Redundante inrichting ten behoeve van hoge mate van beschikbaarheid * Authenticatie op basis van kennis en bezit, voor zowel gebruikers als bijvoorbeeld webservers	* Gebruik van internet-kanaal als primair kanaal, gegeven het aan klanten toegezegde serviceniveau * Communicatie B2B kan plaatsvinden tussen servers

Tabel 1. Risico's en beveiligingsmaatregelen per e-businessfase.

Ontwikkelproces e-Business Services

Tijdens het ontwikkelproces waarbinnen e-Business Services worden gerealiseerd, zijn er verscheidene fasen waarbij beveiliging in het bijzonder de aandacht verdient.

Business case

Bij aanvang van een ontwikkelproces, als de haalbaarheid van een e-project wordt onderzocht, is het van belang een *business case* op te stellen. Met behulp van een business case kan een organisatie onderzoeken of een bedrijfsmatige onderbouwing bestaat voor het realiseren van de beoogde e-Business Services. Bij het vaststellen van de business case is het raadzaam relevante kostenposten en/of vereiste beveiligingsmaatregelen vast te stellen, die van invloed zijn op de besluitvorming aangaande de ontwikkeling van e-Business Services. Denk hierbij aan kostbare beveiligingsmaatregelen zoals PKI en kosten voor het dagelijks beheer van de e-Business Services. Een eerste risicoanalyse voorafgaande aan een project is gewenst, waarbij beveiligings- en beschikbaarheidsrisico's worden meegenomen. Een eventuele outsourcing van het beheer van een e-service dient tijdig te worden geadresseerd.

Projectinrichting

Een project vereist, zoals bij elk project, een adequate *projectinrichting*. In de wereld van e-business is een projectplan onontbeerlijk, zeker als we denken aan veelvoorkomende factoren die projecten in het recente verleden hebben doen vertragen of zelfs falen. Dit betreft bijvoorbeeld onduidelijke mijlpaalproducten, het ontbreken van gebruikersvertegenwoordiging (gebruikers vormen geen onderdeel van de eigen onderneming), te late integratie van applicatieve en infrastructurele ontwikkelactiviteiten en slecht change management.
Ook wordt er vaak van uitgegaan dat de scope van een project alleen *die* facetten van de organisatie betreft, die nieuw worden gerealiseerd ten behoeve van het ontsluiten van het internetkanaal. Niets is minder waar; de bestaande IT-infrastructuur en de bestaande IT-controls dienen mede op orde te zijn of te komen als het gaat om e-Business Services, gegeven het verhoogde risicoprofiel. De klant (consument en/of bedrijf) benadert immers vanaf de eigen werkplek veelal interne systemen van de betreffende organisatie, waardoor alle systemen on line en real-time benaderbaar dienen te zijn. Als één van de systemen faalt, dan wordt dit voor de gebruiker zichtbaar.
In een projectplan dienen dan ook onderwerpen aan de orde te komen zoals de productspecificatie, op te leveren mijlpaalproducten (inclusief documentatie), vereiste projectleden (inclusief verantwoordelijken voor ICT-audit en ICT-beveiliging) en uiteraard een overzicht van onderkende risico's.

Ontwerp

Op basis van de projectuitgangspunten wordt een *ontwerp* opgesteld betreffende de IT-infrastructuur, het beheer en het gebruik. Vaak wordt dan naast het functioneel en het technisch ontwerp gesproken over een beveiligingsontwerp. Dit kan echter leiden tot misverstanden. Beveiliging is immers impliciet onderdeel van zowel het functioneel als het technisch ontwerp.

> Beveiliging is impliciet onderdeel van zowel het functioneel als het technisch ontwerp.

Tijdens de ontwerpfase is het gewenst een risicoanalyse op te stellen en te onderhouden aangaande de binnen het project te realiseren producten. Hierbij komen aandachtsgebieden aan de orde zoals beveiliging, performance en gebruikersacceptatie.

Implementatie

Als het ontwerp op hoofdlijnen stabiel is, dan is het raadzaam een eerste (deel)*implementatie* te realiseren van de gewenste e-Business Services, waarbij de voornaamste functionaliteiten kunnen worden getest. Hiermee wordt zeker gesteld dat in een vroeg stadium nog ontwerpaanpassingen kunnen worden gemaakt, op basis van eerste operationele ervaringen met tijdens het ontwerp onderkende risico's.
Na deze eerste implementatie zal veelal nog een aantal iteraties volgen, voordat de applicatie voldoet aan de gestelde eisen. Het beëindigen van iteratieslagen dient mede te worden gebaseerd op de resultaten van testactiviteiten.
Als voordeel van deze werkwijze van implementeren kan ook worden gezien, dat de IT-infrastructuur, de test- en de productieomgeving reeds in een vroeg stadium in redelijke mate worden ingericht. Uit de praktijk blijkt namelijk dat de complete formele inrichting van de IT-infrastructuur en de bijbehorende IT-controls een relatief lange doorlooptijd vereist.

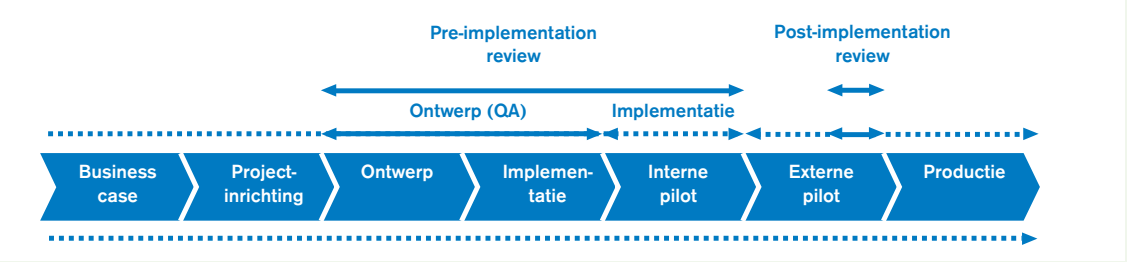
Interne pilot

Na de acceptatie van alle infrastructurele en applicatieve mijlpaalproducten komt de volgende fase van ontwikkeling in zicht: de *interne pilot*. Bij de interne pilot worden alle functionaliteiten aan interne gebruikers beschikbaar gesteld. Risico's betreffende bijvoorbeeld imagoschade en omzetderving worden op deze wijze tegengegaan.

Externe pilot

Als eenmaal is vastgesteld dat de interne pilot met goed gevolg is volbracht, kan een *externe pilot* worden gestart. Bij de externe pilot is het van belang een geschikte omvang van de externe gebruikersgroep vast te stellen.

Figuur 1. Generiek ontwikkelproces.



Figuur 2. Fasegewijze beoordeling van e-Business Services.

Enerzijds is het gewenst deze omvang dusdanig beperkt te houden dat bijvoorbeeld transacties nog met de hand kunnen worden gevolgd. Anderzijds is het nodig een voldoende realistisch transactievolume te genereren, opdat niet alleen de IT-infrastructuur maar ook de administratieve organisatie van de back-office in voldoende mate kan worden getest.

Productie
Als de externe pilot is voltooid, kan na een laatste go/no go-beslissing de e-Business Service volkomen operationeel worden gemaakt.

Rol van de ICT-auditor

Aan de ICT-auditor wordt nogal eens gevraagd een oordeel af te geven betreffende de kwaliteit van e-Business Services. Vaak betreft dit e-Business Services die nog in ontwikkeling zijn. De vraagstelling betreft dan in veel gevallen de effectiviteit van de getroffen maatregelen (bijvoorbeeld betreffende beveiliging, beheersing en beschikbaarheid), aangaande voor de cliënt relevante kwaliteitsaspecten.

In het verleden werd in een dergelijke situatie aan de ICT-auditor nogal eens gevraagd een momentopname te maken van de effectiviteit van de getroffen beveiligingsmaatregelen, met als op te leveren product een rapportage van de verkregen bevindingen en de gedane aanbevelingen. Juist bij een ontwikkelproces is een dergelijk eindproduct van de ICT-auditor onvoldoende. Een op te leveren definitieve rapportage komt te laat en is reeds achterhaald, of een formele rapportage is niet gewenst.

Veelal is de behoefte van de cliënt het verkrijgen van een rapportage in de vorm van positive assurance met als resultaat een groene vlag in de eindfase van het ontwikkelproject. Deze groene vlag dient uiteraard wel te zijn gebaseerd op compliance aan gestelde normen. Daarnaast wordt negative assurance gevraagd tijdens het ontwikkeltraject, in de vorm van groene, gele en rode vlaggen. In het bijzonder bij beoordelingen die worden uitgevoerd met als doel het informeren van toezichthoudende instanties (zoals STE en DNB) en het certificeren van e-Business Services is positive assurance gewenst. Als echter de ICT-auditor pas in de eindfase van een project zou worden ingeschakeld, dan wordt in de praktijk helaas vaak vastgesteld dat diverse aandachtsgebieden tijdens het project onvoldoende belicht zijn geweest, waardoor uiteindelijk geen gunstige beoordeling betreffende de effectiviteit van de getroffen maatregelen kan worden afgegeven.

In de praktijk is dan ook geen momentopname van de ICT-auditor gewenst, maar een vroegtijdige betrokkenheid bij het project in de rol van quality assurance. Op deze wijze kunnen relevante aandachtsgebieden tijdig onder de aandacht van de projectdeelnemers worden gebracht, kunnen tussentijdse beoordelingen op hoofdlijnen plaatsvinden en kan uiteindelijk bij de afronding van het ontwikkelproject tijdig een rapportage met positive assurance worden verstrekt.

Bij het beoordelen van e-Business Services als eindproduct kunnen dan ook verschillende reviews worden onderkend, waarbij de effectiviteit van de getroffen maatregelen wordt onderzocht. Hierbij is het van belang reeds in een vroeg stadium een normenstelsel op te bouwen voor de te beoordelen e-service.

Pre-implementation review
- *Beoordelen van de opzet van te treffen maatregelen*

Door het uitvoeren van een nulmeting (eerste beoordeling) gevolgd door een quality assurance-traject (vervolgbeoordelingen op basis van beperkte documentreviews en periodieke afstemmingen) verstrekt de ICT-auditor in een relatief hoog tempo tussenrapportages aangaande de status van te treffen maatregelen.
- *Beoordelen van het bestaan van getroffen maatregelen*

Voor alle bij de opzetbeoordeling onderkende maatregelen wordt het bestaan van deze maatregelen vastgesteld. Hiertoe worden ten aanzien van de IT-infrastructuur de beveiligingsparameters van toegepaste componenten onderzocht en vindt een penetratietest plaats. De IT-controls worden met name beoordeeld op basis van beschikbare operationele en managementrapportages, en van vastleggingen van het uitvoeren van beheerprocedures.

Post-implementation review (als aanvulling op de pre-implementation review)
- *Beoordeling van wijzigingen in de opzet van te treffen maatregelen*

Bij de post-implementation review is het van belang een beoordeling uit te voeren op alle wijzigingen van de getroffen maatregelen, onder andere naar aanleiding van aanbevelingen uit de pre-implementation review. De beoordeling van de wijzigingen kan bijvoorbeeld plaatsvinden op basis van een workshop.
- *Beoordeling van het bestaan en mogelijk de werking van getroffen maatregelen*

Als de e-Business Services gedurende enige tijd hebben gefunctioneerd, kan een hogere mate van zekerheid worden gegeven omtrent de kwaliteit van de getroffen maatregelen. Op basis van een voldoende aantal van deelwaarnemingen kan zelfs een oordeel worden gevormd aangaande de werking van de getroffen maatregelen.

Na het toetsen van de werking van getroffen maatregelen is het mogelijk de e-Business Services te certificeren, waarbij een zegel op de website wordt geplaatst. Voor het verkrijgen van zegels, bijvoorbeeld ZekeRE Business (NOREA) en WebTrust, zijn specifieke normen opgesteld.

Het is afhankelijk van de ontwikkelfase van de e-Business Services, welke beoordelingen voor een cliënt relevant zijn. Bij het bepalen van de vorm van ondersteuning door een ICT-auditor dient de effectiviteit van de ICT-auditondersteuning te worden bezien ten opzichte van de projectmatig te behalen voordelen en met name de eventuele auditverplichtingen, in het bijzonder bij financiële instellingen.

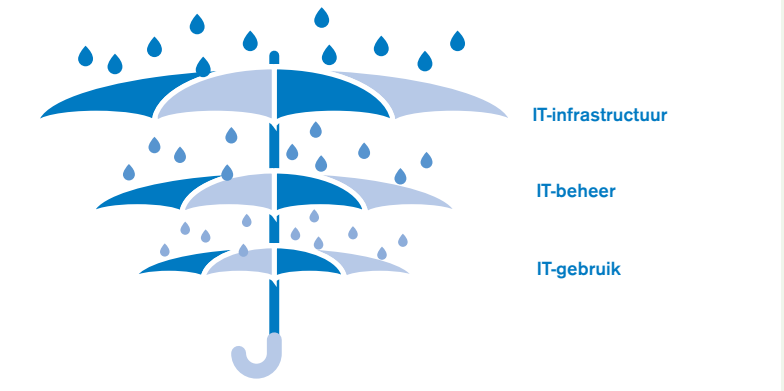
In de praktijk is gebleken dat via een tijdige beoordeling van de opzet van getroffen maatregelen een project kon worden bijgestuurd op gebieden waar het restrisico te hoog bleek te zijn, waardoor de doorlooptijd en de vereiste inspanning niet hoefden te worden gewijzigd. In gevallen waarbij een beoordeling van de opzet en het bestaan van de getroffen maatregelen pas plaatsvond vlak voor de feitelijke inproductiename, bleek dat het elimineren of beperken van geconstateerde restrisico's een wezenlijke uitbreiding van de doorlooptijd vergde, en resulteerde in extra kosten.

Naast beoordelingen van het eindproduct, de feitelijke e-service, kunnen uiteraard diverse andere reviews plaatsvinden, onder andere betreffende project risk management en privacy.

Aandachtsgebieden

Het bepalen van de scope van een beoordeling is niet altijd eenvoudig. De IT-infrastructuur is veelal complex, zowel door de diversiteit als door de veelheid van de toegepaste componenten, en verschillende partijen zijn betrokken (hostingpartij, ontwikkelaars, gebruikers e.d.). Daarnaast is het de vraag welke applicaties binnen de scope van de beoordeling vallen. Denk bijvoorbeeld aan de pc van de gebruiker: in welke mate dient deze mede te worden beoordeeld? Welke risico's zijn aanwezig in de pc-omgeving, een omgeving die niet wordt beheerd door de organisatie zelf.

Het is voor een organisatie effectief te beschikken over een internetbeveiligingsbeleid, juist omdat op basis van een internetbeveiligingsbeleid reeds bij de projectinrichting duidelijke uitgangspunten en randvoorwaarden kunnen worden gehanteerd.
Per project is een risicoanalyse gewenst, op basis waarvan kan worden bepaald welk beveiligingsniveau vereist is. Denk bijvoorbeeld aan authenticatie en netwerkbeveiliging. Bij authenticatie dient te worden overwogen of kennis voldoende is als kenmerk, of dat juist een bezitskenmerk vereist is. Bij netwerkbeveiliging kan een firewall afdoende zijn, maar het kan ook vereist zijn een sterk IDS (Intrusion Detection System) toe te passen. Met een IDS kunnen (ongewenste) gebeurtenissen worden gedetecteerd, waardoor beheerders in staat zijn de beveiliging, beschikbaarheid en beheersing van de infrastructuur en de applicatie optimaal te houden.



Figuur 3. Aandachtsgebieden voor beveiliging.

Met de introductie van e-Business Services ontstaat 'plotseling' de situatie dat klanten directe toegang hebben tot de IT-infrastructuur van de organisatie. De organisatie kan dus eventuele technische problemen niet meer verbergen. Dit vereist een verscheidenheid van maatregelen. In figuur 3 zijn de voornaamste aandachtsgebieden afgebeeld waarbinnen beveiligingsmaatregelen moeten worden getroffen. In de figuur wordt ervan uitgegaan dat de IT-infrastructuur de eerste beveiligingslinie vormt tegen bedreigingen. Met behulp van IT-beheer dienen deze infrastructurele maatregelen te worden versterkt en gehandhaafd. Het samenstel van maatregelen betreffende de IT-infrastructuur en het IT-beheer is echter niet voldoende. Ook het IT-gebruik kan niet zonder maatregelen. Denk hierbij aan het geheim houden van passwords.

Kader 1. Aandachtsgebieden e-Business Security.

IT-infrastructuur
- Topologie:
  - redundantie betreffende beveiliging en beschikbaarheid.
- Verkeersplan:
  - voor alle gebruikersgroepen: klanten, interne gebruikers en beheerders;
  - per verkeersroute: authenticatie-, sessie- en transactiebeveiliging.
- Event handling (doe niets, log gebeurtenis, alarm, noodstop).
- Beheerhulpmiddelen voor netwerk- en serverbeheer.
- Componentbeveiliging:
  - security baselines;
  - compliance aan security baselines.
- Applicaties:
  - bedrijfsspecifieke applicaties (geprogrammeerde controles);
  - standaardapplicaties:
    - webservices;
    - mailservices (filters, antivirusprogrammatuur e.d.).

IT-beheer
- Organisatie:
  - betrokken partijen;
  - verantwoordelijkheden, taken en bevoegdheden;
  - communicatiestructuren (inclusief managementrapportages).
- Managementprocessen:
  - security management;
  - incident en problem management;
  - change management;
  - operations management;
  - availability management;
  - performance en capacity management.

IT-gebruik
- Administratieve organisatie en interne controle.
- Wet- en regelgeving.
- Gebruikersovereenkomsten.

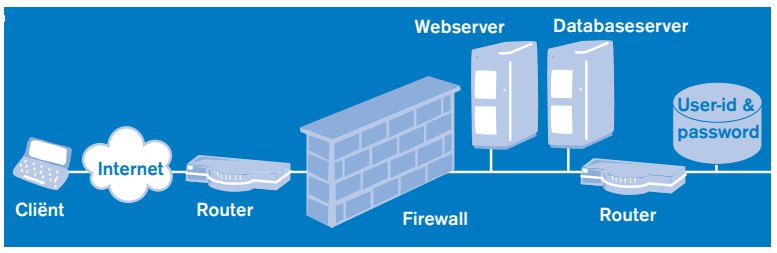
In kader 1 zijn de onderkende aandachtsgebieden nader uitgewerkt. Deze uitwerking is overigens niet volledig, per situatie dienen de te onderkennen aandachtsgebieden te worden aangepast. Voor deze aandachtsgebieden dienen normen te worden opgesteld waarmee een beoordeling kan plaatsvinden.

IT-infrastructuur

Veel van de internetsites die worden gehackt, blijken in de praktijk zwakten te hebben in de IT-infrastructuur. Denk hierbij aan in het verleden onderkende zwakke implementaties van DNS (Domain Name Services) en webservices. Uiteraard komen deze zwakten mede voort uit onvoldoende sterke beheerprocedures betreffende security management.

Binnen de IT-infrastructuur dienen diverse beveiligingsmaatregelen te worden getroffen, om veilige e-Business Services te realiseren. En dan nog ..., dan nog kan niet worden gegarandeerd dat een e-Business Service honderd procent veilig is. Wel kan met een hoge mate van zekerheid worden aangegeven dat een eventuele inbraak(poging) wordt gedetecteerd. Juist daarom is het zo belangrijk de preventieve en detectieve beveiligingsmaatregelen binnen de IT-infrastructuur in samenhang te bezien.

Bij de beoordeling van e-Business Services is veelal de afbeelding van de netwerktopologie een efficiënt en effectief startpunt. Aan de hand van een netwerktopologie kan eerst de functie van elk van de toegepaste componenten worden besproken, gevolgd door onderlinge positionering van de toegepaste netwerkcomponenten en -servers. In figuur 4 is een eenvoudig voorbeeld gepresenteerd van de netwerktopologie van een e-Business Service.



Figuur 4.
De netwerktopologie van een e-Business Service.

Op basis van deze figuur kan direct een aantal vragen worden gesteld. Op welke wijze communiceren beheerders met elk van de toegepaste componenten? Waar wordt logging bewaard? Wat is de relatie tussen toegepaste filterregels in de firewall en de routers? Welke uitgangspunten worden gehanteerd bij de beveiliging van de servers? Zijn eisen gesteld aan de beveiliging van de besturingssystemen en applicaties?

De functionaliteit van elke component binnen de netwerktopologie moet worden gespecificeerd. Het is immers pas mogelijk goed te beveiligen, als duidelijk is welke services daadwerkelijk nodig zijn, en welke services kunnen worden geblokkeerd.

Vervolgens wordt vastgesteld welke gebruikersgroepen zijn te onderkennen. Per gebruikersgroep wordt vaak een afzonderlijke verkeersstroom toegepast. Een klant zal bijvoorbeeld toegang tot de webserver van de organisatie nodig hebben. De netwerkbeheerder heeft toegang nodig tot de netwerkcomponenten (bijvoorbeeld de routers en de firewall), beheerders benaderen vaak elk van de componenten via een eigen beheernetwerk. Interne medewerkers hebben doorgaans toegang via het interne netwerk. Het is echter de vraag of daarmee alle gebruikersgroepen zijn onderkend. Zijn er derden die beheer op afstand verzorgen? Hoe vindt databasebeheer plaats? Hoe is de koppeling gerealiseerd tussen de front- en de back-office?

Op basis van het overzicht van de onderkende gebruikersgroepen worden de geoorloofde verkeersstromen bepaald. Dit zijn alle toegangspaden vanaf verschillende gebruikersgroepen naar de gewenste componenten.

Per verkeersstroom worden daarna de wijzen van identificatie, authenticatie en autorisatie vastgesteld. Hierbij komt vaak versleuteling van berichtenverkeer aan de orde. Zo hanteren gebruikers nogal eens SSL. Beheerders benutten vaak het hulpmiddel ssh om te voorkomen dat een terminalverbinding wordt gemaakt die door anderen is af te tappen.

Voor de applicatie is een systeembeoordeling gewenst. Hierbij dienen de functionaliteiten van de applicatie te worden geïnventariseerd, risico's te worden onderkend en getroffen maatregelen te worden vastgesteld. Hierbij mag de koppeling tussen de front- en de back-office niet worden vergeten.

Bij de beoordeling van de opzet van de te treffen maatregelen kunnen de in kader 1 aangegeven onderwerpen worden besproken.

IT-beheer

In de eerste plaats is het van belang een overzicht te verkrijgen van alle bij de e-Business Services betrokken medewerkers en organisaties. Op basis van dit overzicht kunnen de deelnemers worden bepaald voor een workshop waarin de te treffen maatregelen worden besproken.

Per IT-component dient de functioneel en technisch verantwoordelijke medewerker te worden vastgesteld, juist vanwege de diversiteit en het gedecentraliseerde karakter van IT-componenten in het geval van e-Business Services. Tevens dient per IT-component te worden bepaald welk level van service management wordt toegepast. In de praktijk blijkt nogal eens dat niet alle betrokken partijen bekend zijn, of dat niet met alle betrokken partijen adequate afspraken zijn gemaakt, bijvoorbeeld in de vorm van een service level agreement.

Bij een e-Business Service is veelal een groot aantal partijen betrokken. Bijgevolg is communicatie een belangrijk onderwerp. Elk van de betrokken partijen dient managementrapportages aangaande de geleverde diensten te verschaffen. Partijen dienen tevens voldoende frequent met elkaar in gesprek te zijn om onderlinge afhankelijkheden, knelpunten en verbeterpunten te bespreken.

Bij het optreden van incidenten is duidelijkheid gewenst over de verantwoordelijkheden, taken en bevoegdheden, opdat bij incidenten snel en adequaat kan worden ingegrepen.

Als onderdeel van security management is voor e-Business Security een aantal taken in het bijzonder van belang. Denk bijvoorbeeld aan:
* reageren op alarmmeldingen en analyseren van logging;
* volgen van ontwikkelingen aangaande beveiliging op internet;
* tijdig ontvangen van security patches, evenals het testen en implementeren van deze security patches;
* periodiek uitvoeren van penetratietests;
* adequaat handelen bij beveiligingsincidenten, zowel betreffende de externe communicatie als betreffende de bescherming van de IT-infrastructuur, applicaties en gegevens.

In kader 1 zijn diverse beheerprocessen aangegeven die in detail dienen te worden beoordeeld, om vast te stellen dat e-Business Services in voldoende mate proactief operationeel worden gehouden, met een voldoende hoog service level naar de klanten van de organisatie.

IT-gebruik

Met de introductie van e-Business Services is een nieuw communicatiekanaal voor klanten ontstaan. Deze klanten dienen tijdig en adequaat te worden bediend. Hierop dient de administratieve organisatie te zijn ingericht. De ICT-auditor zal dan ook een beoordeling moeten uitvoeren op de soorten van transacties die via het e-kanaal worden ontvangen, evenals de wijze van verwerking van deze transacties.

Aangaande wet- en regelgeving is het in de eerste plaats van belang vast te stellen welke externe eisen worden gesteld aan de e-Business Services. Er dient te worden vastgesteld of aan die eisen wordt voldaan. Zo zal elke organisatie te maken kunnen hebben met de wetgeving aangaande privacy. De volgende wetgeving is elk geval van belang:
* Wet bescherming persoonsgegevens;
* Wet computercriminaliteit;
* Telecommunicatiewet;
* Auteurswet;
* Europese richtlijn Elektronische Handtekening.

De regelgeving is veelal zeer branchespecifiek. Zo zijn bij het bank- en effectenwezen van belang:
* richtlijnen STE inzake effectenafhandeling via internet;
* DNB-regeling Organisatie en beheersing.

Niet alleen de organisatie zelf heeft verantwoordelijkheden, taken en bevoegdheden. Ook de klant van de organisatie heeft deze. De klant dient te worden geïnformeerd aangaande de maatregelen die door hem zelf moeten worden getroffen. Hiertoe kan worden gebruikgemaakt van een gebruikerscontract, een eventueel vereiste installatiehandleiding en gebruikersinstructies (on line en op papier).

In kader 1 zijn de onderwerpen nogmaals weergegeven.

Conclusie

De ICT-auditor dient bij de beoordeling van de effectiviteit van maatregelen inzake e-Business Security in overleg met de cliënt een efficiënte en effectieve auditaanpak te kiezen. In de praktijk zal steeds vaker worden gekozen voor een interactieve aanpak, waarbij de ICT-auditor vroegtijdig betrokken wordt in het ontwikkelproces. Bijgevolg is een beoordeling van de opzet van de te treffen maatregelen tijdens het ontwerpproces gewenst, aangevuld met QA-ondersteuning tijdens de verdere ontwikkeling. Aan het einde van het ontwikkelproces kan dan een finale beoordeling van het bestaan van de getroffen maatregelen worden uitgevoerd, zonder dat dit additionele projectrisico's met zich meebrengt.

Bij het certificeren van webservices zullen op periodieke basis post-implementation reviews dienen te worden uitgevoerd.

De ICT-auditor zal voor een effectieve projectondersteuning frequent rapportages moeten kunnen aanbieden, opdat de projectorganisatie op de hoogte blijft van de status van alle relevante aandachtsgebieden.

Ir. P. Kornelisse RE is senior manager bij KPMG Information Risk Management in Amstelveen, alwaar hij verantwoordelijk is voor de groep E-Business Security. Deze groep richt zich op de beveiliging en beheersing van e-businessomgevingen, zowel in de vorm van advies- als auditdiensten. Dit betreft onder andere ethical hacking, QA- en beoordelingsdiensten inzake nieuwe e-businessomgevingen, platformbeveiliging (security baselines) zoals voor Windows 2000 en forensische onderzoeken.

Kader 2. Maatregelen voor een adequate beveiliging.

Een honderd procent sluitende beveiliging tegen ongewenste indringers is zo goed als onmogelijk te realiseren. Bedrijven en organisaties kunnen echter wel diverse maatregelen treffen, waarmee het beveiligingsniveau van hun websites aanzienlijk wordt verhoogd. Deze maatregelen hebben zowel te maken met de IT-infrastructuur als met het beheer en het gebruik.

Hieronder worden tien maatregelen gegeven, gebaseerd op best practices, die een adequate beveiliging mogelijk maken:

e-Business Services-infrastructuur:
1. Installeren van zogeheten 'security patches' (verbeteringen in de beveiligingssoftware) evenals het testen en implementeren van deze 'security patches'. Denk hierbij aan recente beveiligingslekken in Bind (de name services op internet) en IIS (de webserver van Microsoft).
2. Implementeren van netwerkcomponenten op een dusdanige wijze, dat de zogenaamde denial-of-service (DoS)-aanvallen minder kans van slagen hebben.
3. Toepassen van versleutelde verbindingen bij het verzenden van vertrouwelijke informatie, zoals passwords en transactiegegevens.
4. Voorkomen van beheer op afstand van de webinfrastructuur.

e-Business Services-beheer:
5. Reageren op alarmmeldingen en analyseren van 'logging'.
6. Volgen van ontwikkelingen voor wat betreft de beveiliging op internet.
7. Periodiek uitvoeren van penetratietests.
8. Adequaat handelen bij beveiligingsincidenten, zowel wat betreft de externe communicatie als wat betreft de bescherming van de IT-infrastructuur, applicaties en gegevens.

e-Business Services-gebruik:
9. Opstellen van duidelijke gebruikersinstructies, zodat een gebruiker zich bewust is van de risico's bij het installeren van programmatuur via het web en het openen van e-mail met onbekende herkomst.
10. Beschermen van pc's tegen inbraken vanaf internet met behulp van zogenaamde personal firewalls.