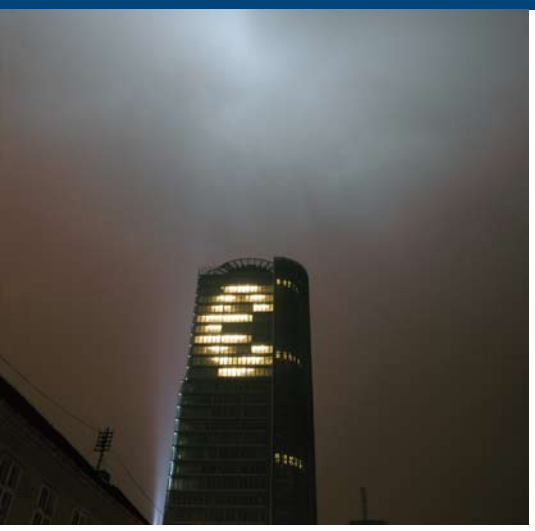


Risico's in het betaalproces en betaalpakketten

Drs. ing. L. Benjaminse
werkt als IT-auditor bij KPMG Advisory Financial Services. Hij heeft voor zijn referaat aan de Universiteit van Amsterdam onderzoek gedaan naar betaalpakketten en risico's en beheersingsmaatregelen in het betaalproces. Daarnaast heeft hij ruime ervaring met het uitvoeren van data-analyses binnen bijvoorbeeld het betaalproces in het kader van jaarrekeningcontroles.

benjaminse.lodewijk@kpmg.nl

Drs. H.G.Th. van Gils RE RA
is senior manager bij KPMG Advisory en vooral werkzaam in de Financiële dienstverlening. Daarnaast is hij docent aan de Universiteit van Amsterdam, zowel bij de accountantsopleiding als de IT-auditorsopleiding.

vangils.herman@kpmg.nl

Drs. ing. Lodewijk Benjaminse en drs. Herman van Gils RE RA

Dit artikel is deels gebaseerd op het referaat van Lodewijk Benjaminse dat hij onlangs in het kader van de opleiding EMITA aan de Universiteit van Amsterdam heeft geschreven. Het referaat is gebaseerd op een onderzoek naar het betaalproces en de betaalpakketten van de banken die daarbij worden ingezet. De inrichting van het betaalproces wordt behandeld aan de hand van een korte procesanalyse en een beschrijving van de zeer beperkte wet- en regelgeving op het gebied van het betaalproces. Data-analyse kan een bijdrage leveren aan het inzichtelijk maken van het betaalproces inclusief de momenten in dat proces waarop uitval en/of handmatig ingrijpen in het proces heeft plaatsgevonden.

Inleiding

Het betaalproces kent diverse risico's waarvan velen zich te weinig bewust zijn. Mede daardoor zijn situaties bekend waarin men onvoldoende preventieve beheersingsmaatregelen treft. In gesprekken met medewerkers van organisaties en ook wel van auditors hoort men reacties als 'het zal zo'n vaart niet lopen', 'we controleren om het betaalpakket heen' of 'de crediteur belt vanzelf wel een keer'.

In dit artikel beschrijven wij de inzet van betaalpakketten van banken, zowel de versie waarbij gebruik wordt gemaakt van de onlinefunctionaliteit op de website van de bank als de versie waarbij een betaalpakket lokaal bij de organisatie (niet de bank) is geïnstalleerd. Aan de hand van de belangrijkste verschillen in de functionaliteiten van betaalpakketten lichten wij de risico's toe. Met een voorbeeld gaan we in op de mogelijkheden om op eenvoudige wijze een CLIEOP03-bestand te bewerken.

In het kader van de jaarrekeningcontrole bespreken we wet- en regelgeving, richtlijnen en raamwerken die impact hebben op de AO/IC, algemene IT-beheersingsmaatregelen, het betaalpakket en het betaalproces. Als onderdeel daarvan lichten we de 'bucket-approach' toe, waarmee door middel van data-analyse inzicht wordt verkregen in de betaalstromen en de omvang en aard van eventuele uitval in het betaalproces.

Hieronder staat het artikel 'Het banksaldo aangevuld'[1] uit *Accountant* ([Grooo8]) dat illustreert hoe (relatief) eenvoudig het in de praktijk is om fraude te plegen bij uitgaande betalingen. In dit voorbeeld wordt aangegeven hoe door het muteren van bankrekeningnummers in betaalvoorstellijsten en het bijwerken van tussenrekeningen werd gefraudeerd.

Een onderneming maakt bij het verrichten van betalingen gebruik van een betaalpakket. Het betaalproces is als volgt ingericht. Een medewerker van de administratie stelt vanuit de crediteurenadministratie een zogenaamde betaalvoorstellijst op. De medewerker geeft dit overzicht aan de directeur, inclusief de onderliggende facturen. De directeur controleert het overzicht met de onderliggende bescheiden en keurt de betalingen in het betaalpakket goed. Hierna vindt (geautomatiseerd) de betaling plaats.
Recentelijk is de onderneming gestuit op een aantal vreemde betalingen. Nader onderzoek heeft uitgewezen dat de medewerker verantwoordelijk voor het opstellen van de betaalvoorstellijst voor ruim één miljoen euro heeft gefraudeerd. Hoe? De medewerker wijzigde na aanmaak van de betaalvoorstellijst in het betaalpakket de naam en het bankrekeningnummer van de crediteur in zijn eigen naam en bankrekeningnummer. De directeur kreeg echter het oude ongewijzigde bestand, stelde vast dat het overzicht aansloot met de facturen en keurde de betaling goed. Hij was zich er niet van bewust dat de gegevens in het betaalpakket waren gewijzigd en dat in werkelijkheid de bedragen werden overgemaakt aan de fraudeur. Nadat de betaling was verricht werd het betaaloverzicht door de fraudeur op zodanige wijze gemanipuleerd dat het weer de juiste crediteurengegevens bevatte. Hierna werd de crediteurenadministratie bijgewerkt.
Als facturen niet worden betaald, gaan na verloop van tijd natuurlijk de crediteuren klagen. Dit werd door de fraudeur op eenvoudige wijze voorkomen. De fraudeur liet de facturen nogmaals betalen, maar nu op het juiste bankrekeningnummer. De directeur had dit toch niet door. Er werden dagelijks zoveel betalingen verricht dat hij een dubbele betaling niet op zou merken. Daar de crediteur al was afgeboekt, werden de betalingen op een tussenrekening geboekt. Nu zou je natuurlijk verwachten dat de accountant dit bij zijn controle wel zou ontdekken. Een tussenrekening met een hoog saldo valt natuurlijk op. Maar ook dit was snel opgelost. Op het moment dat de accountant zijn controle aankondigde, schoonde de fraudeur de tussenrekeningen en boekte de bedragen over naar diverse kostenrekeningen. Hij gebruikte hiervoor kostenrekeningen waarvan de realisatie ruim onder het budget en de realisatie van vorig jaar lag, zodat een en ander bij een cijferbeoordeling door de accountant niet op zou vallen. De medewerker kon op deze wijze jarenlang zijn banksaldo aanvullen, zonder dat hij tegen de lamp liep.
Fraude in het betaalproces komt in de praktijk zeer veel voor. Dit is ook logisch, aangezien hier het geld de onderneming verlaat. Toch blijkt de accountant deze vorm van fraude in de praktijk maar zelden te ontdekken, terwijl het in veel gevallen om omvangrijke (materiële) bedragen gaat. Uit oogpunt van fraude is het betaalproces dan ook een proces dat de nodige aandacht van de accountant verdient.

1 Het artikel is iets aangepast. Enkele begrippen zoals 'electronic banking', 'betalingssysteem', 'electronic bankingsysteem', 'betalingsvoorstellijst' en 'betalingsproces' zijn aangepast aan de terminologie zoals die elders in dit artikel wordt gehanteerd. Deze begrippen zijn vervangen door 'betaalpakket', 'betaalvoorstellijst' c.q. 'betaalproces'.

0mschrijving van het betaalproces en betaalpakketten

Hoog inherent risico

Op diverse momenten in het betaalproces worden bestanden gebruikt: als overdrachtsmedium tussen de financiële administratie dat opdrachten genereert en het betaalpakket, bij het versturen van de betaalopdrachten, maar ook afschriften en verwerkingsinformatie zijn veelal in bestanden opgeslagen. Hierin ligt een inherent hoog risico op bewuste manipulatie of onbewuste fouten. Bewuste manipulatie is voor de hand liggend aangezien via het betaalproces het meest direct geld aan de organisatie kan worden onttrokken. Ook het maken van onbewuste fouten is niet onwaarschijnlijk als er in het betaalproces veel momenten zijn dat bestanden worden overgedragen en regelmatig (handmatige) correcties plaatsvinden.

Als compensatie zou daarom een goed stelsel van beheersingsmaatregelen essentieel zijn. Echter, beheersingsmaatregelen rondom deze bestanden zijn dat niet altijd. Veelal wordt slechts gesteund op de controle van het totale bedrag in het betaalbestand en wordt de juistheid van individuele betaalopdrachten niet altijd vastgesteld.

Betaalproces en betaalpakket

Het betaalproces kent op hoofdlijnen de volgende stappen:

Subproces aanmaken (in financiële administratie):
a. betaalvoorstellijst aanmaken
b. betaalbestand aanmaken
c. betaalbestand exporteren

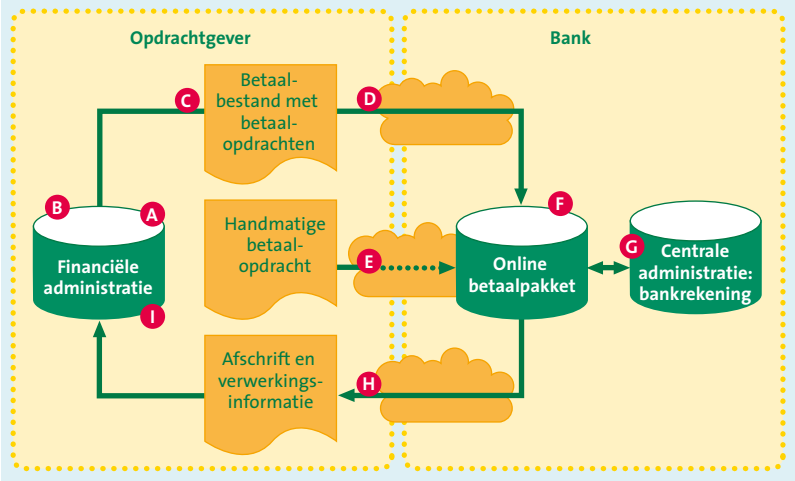
Subproces betalen (in betaalpakket):
d. betaalbestand importeren
e. betaalopdracht handmatig invoeren
f. betaalopdrachten versturen

Subproces bankverwerking (in centrale administratie van de bank):
g. betaalopdrachten uitvoeren

Subproces verwerkingsinformatie (in betaalpakket):
h. afschriften en verwerkingsinformatie downloaden

Subproces boeken van betaling (in financiële administratie):
i. afletteren betalingen

De letters a tot en met i zijn ook opgenomen in de figuren 1 en 2. In deze twee figuren zijn in het kort de stappen weergegeven die worden doorlopen bij versturen van betaalopdrachten via een betaalpakket.



Figuur 1. **Onlinebetaalpakket op website van bank.**

Betaalpakketten

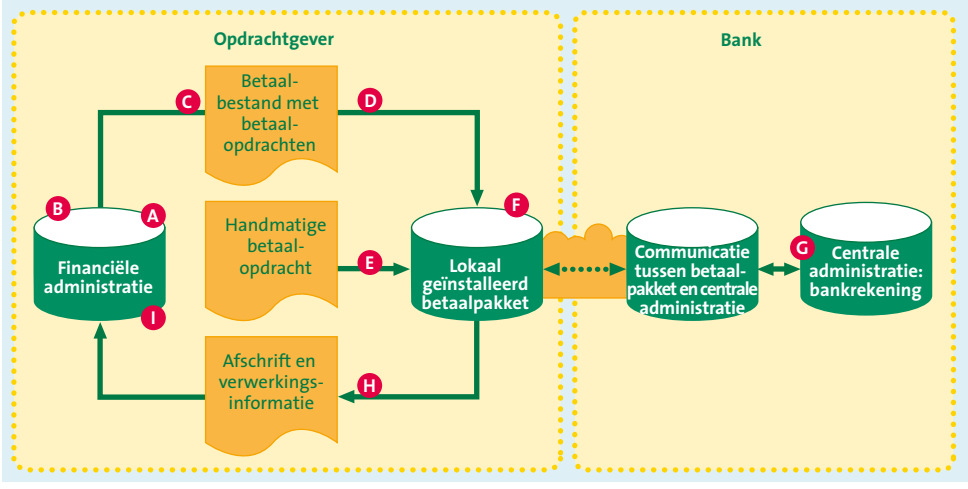
In figuur 1 is het proces weergegeven dat ondersteund wordt door een onlinebetaalpakket en in figuur 2 betreft het een lokaal geïnstalleerd betaalpakket. In beide figuren is links door middel van de stippellijnen de organisatie weergegeven die de betaalopdrachten verstuurt. De bank zelf is in beide figuren eveneens door middel van stippellijnen aan de rechterkant weergegeven. Communicatie tussen beide partijen vindt veelal via internet plaats.

Figuur 1 geeft de situatie weer waarbij het onlinebetaalpakket via een website van de bank (rechts) wordt benaderd. De betaalopdrachten worden vanuit de financiële administratie gegenereerd en geïmporteerd in het onlinebetaalpakket of direct handmatig in het betaalpakket ingevoerd. In de figuur is duidelijk zichtbaar dat het betaalpakket zich op een webserver binnen de infrastructuur van de bank bevindt. Vanaf de webserver wordt met de centrale administratie van de bankrekeningen (transacties en saldi) gecommuniceerd. Het onlinebetaalpakket wordt door middel van een browser via internet benaderd voor zowel het invoeren van betaalopdrachten als het downloaden van de afschriften en de verwerkingsinformatie.

In figuur 2 wordt een betaalpakket gebruikt dat lokaal bij de opdrachtgever is geïnstalleerd. Het lokaal geïnstalleerde betaalpakket ontvangt betaalopdrachten uit de financiële administratie of deze worden rechtstreeks ingevoerd. Daarvandaan worden betaalopdrachten (veelal op een later moment) naar de bank verstuurd. Deze zal de betaalopdrachten in haar centrale administratie van bankrekeningen verwerken. De verwerkingsinformatie wordt vervolgens door de bank beschikbaar gesteld in het lokaal geïnstalleerde betaalpakket.

Risico's

Het is niet de doelstelling van dit artikel alle risico's hier uitputtend te behandelen. Belangrijk verschil tussen beide hiervoor beschreven varianten is dat bestanden met betaal- en/of verantwoordingsinformatie gedurende enige tijd of bij de bank of bij de organisatie zelf staan. In het laatste geval is het risico op manipulatie (bewust) of bijvoorbeeld overschrijving (onbewust) aanmerkelijk groter.



Figuur 2. **Betaalpakket lokaal geïnstalleerd bij de opdrachtgever.**

Enkele andere voorbeelden van risico's in het proces van uitgaande betalingen en inkomende verwerkingsinformatie zijn:
- Betaalopdrachten worden ten onrechte gemuteerd.
- Betaalopdrachten worden niet gefiatteerd.
- Functiescheiding in het betaalproces ontbreekt.
- Afschriften en verwerkinginformatie van de bank worden gemuteerd.
- Door middel van slepen wordt geld aan de organisatie onttrokken.
- Details van betaalopdrachten zijn achteraf niet meer te herleiden (audit trail).

Er heerst vaak een groot vertrouwen in collega's: passen worden bij de pincodes bewaard en pincodes worden gedeeld met collega's.

De bestanden waarin de betaalopdrachten (CLIEOP03) en afschriften of verwerkingsinformatie (MT940) zijn opgeslagen, zijn relatief eenvoudig in een simpele tekstverwerker aan te passen. Doordat veelal ten onrechte wordt gesteund op de controle van het totale bedrag, worden mutaties in het bestand lang niet altijd ontdekt aangezien het mogelijk is het bestand aan te passen, zoals in het voorbeeld dat in de inleiding wordt aangehaald. Er worden minimale controles op de juistheid van de betaalopdrachten uitgevoerd en vastlegging van deze controles vindt nauwelijks plaats. In sommige gevallen worden slechts de bedragen van een paar facturen gecontroleerd of wordt alleen het controletotaal beoordeeld.

Hieronder is ter illustratie een voorbeeld opgenomen om aan te tonen dat deze controles onvoldoende zijn. In figuur 3 is een deel van een CLIEOP03-bestand weergegeven. In blauw is het bedrag in centen weergegeven. Rood en groen geven de bankrekeningnummers weer van respectievelijk de opdrachtgever en de ontvanger. Het betreft een declaratie van 209,75 euro voor De Vries naar bankrekeningnummer 248592831 en de betaling van het salaris van Boer à 3.533,93 euro naar bankrekeningnummer 938492837.

Het is relatief eenvoudig dit CLIEOP03-bestand te bewerken zonder dat dit wordt ontdekt wanneer het bestand alleen aan de hand van het totaalbedrag wordt gecontroleerd. De bedragen

```
...
0100A00050000000020975058394788302485928 31
0160ADeclaratie 39239
0170BG. de Vries
0173BAMSTERDAM
0100A00050000003533930583947883093849283 7
0160ASalaris juni2010
0170BV. M. Boer
0173BZWOLLE
...
```

Figuur 3. **Deel van originele CLIEOP03-bestand.**

kunnen immers binnen het bestand worden verplaatst omdat dit opgeteld nog altijd hetzelfde totaalbedrag oplevert.

In figuur 4 is te zien dat een deel van het bedrag van de declaratie bij de betaling van het salaris is opgeteld. Dit heeft geen invloed op het totaalbedrag omdat de 200 euro die bij de betaling van het salaris is opgeteld, van de betaling van de declaratie is afgetrokken.

```
...
0100A00050000000009750583947883024859283 1
0160ADeclaratie 392390
170BG. de Vries
0173BAMSTERDAM
0100A00050000003733930583947883093849283 7
0160ASalaris juni 2010
0170BV. M. Boer
0173BZWOLLE
...
```

Figuur 4. **Deel van bewerkte CLIEOP03-bestand.**

Verschillen in functionaliteiten van betaalpakketten

Wij treffen de volgende belangrijkste verschillen aan in de functionaliteiten bij betaalpakketten:

Autorisatie

De mate waarin gedetailleerd autorisaties kunnen worden ingericht, verschilt sterk tussen de pakketten. Dit varieert van betaalpakketten waarin alle gebruikers dezelfde rechten hebben tot betaalpakketten waarin autorisaties minutieus kunnen worden toegekend door middel van profielen. Om risico's te beperken is het aan te bevelen een betaalpakket te gebruiken waarin de rechten per gebruiker gedetailleerd kunnen worden toegekend door middel van profielen.

Authenticatie

Voor veel activiteiten in de betaalpakketten geldt dat authenticatie en autorisatie van de gebruiker moeten plaatsvinden. Dit kan op de volgende manieren geschieden:
- door middel van iets wat men *weet:* bijvoorbeeld een gebruikersnaam, het wachtwoord of een pincode;
- met iets wat men *heeft:* bijvoorbeeld een token, een bankpas of een digitaal certificaat;
- met behulp van iets wat men *is:* bijvoorbeeld een vingerafdruk, stemherkenning, iriscopie of gezichtsherkenning.

De huidige mechanismen om betaalopdrachten te fiatteren maken geen gebruik van de volledige inhoud van alle betaalopdrachten. Het enige wat door de huidige authenticatiemiddelen wordt bevestigd, is wie men beweert te zijn. Dit zegt dus niets over de feitelijke inhoud van de te fiatteren betaalopdrachten, die kan ondertussen zijn gemuteerd zonder dat de gebruiker dit

bemerkt. Helaas zien we nog erg weinig beweging richting het gebruik van authenticatiemiddelen die gebruikmaken van iets wat men 'is'. Ten slotte komen de meeste fraudes nog voort uit misbruik van zwakke authenticatiemiddelen (zoals het bekend worden van wachtwoorden en pincodes).

Per bank verschilt het sterk hoe gebruikers aan het betaalpakket worden toegevoegd. Het kan zijn dat organisaties geheel zelfstandig gebruikers, authenticatiemiddelen en autorisaties kunnen wijzigen in het betaalpakket of dat dit via de bank dient te verlopen. Dit is van belang voor het triggeren van wijzigingen in bevoegdheden van functionarissen alsmede het periodiek wijzigen van wachtwoorden, etc.

Hashtotalen

Voor gebruikers zijn niet altijd evenveel controlemogelijkheden beschikbaar in de vorm van controletotalen en hashtotalen. Hoe meer mogelijkheden bij het inrichten van controletotalen en hashtotalen de gebruiker tot zijn beschikking heeft, des te beter hij controles kan uitvoeren op de juistheid en volledigheid van het betaalbestand. Hashtotalen zijn een goede aanvulling op controletotalen. Controletotalen zoals die in een CLIEOP03-bestand worden toegepast houden geen rekening met de positie van het bedrag, zoals in figuur 3 is getoond. Het is daarom verstandig ook gebruik te maken van hashtotalen waarbij in de berekeningen wel rekening wordt gehouden met de positie. Hoewel het in theorie mogelijk is een betaalbestand te manipuleren en toch het hashtotaal ongewijzigd te houden, is dat in de praktijk aanzienlijk moeilijker en tijdrovender dan het manipuleren van een betaalbestand dat is voorzien van alleen een totaalbedrag als controletotaal.

Verantwoordingsinformatie

Het verdient de voorkeur om de individuele betaalopdrachten uit een betaalbestand in de verwerkingsinformatie te laten terugkomen, in plaats van alleen het totaalbedrag of de terugmelding dat de betaalopdrachten zijn verwerkt. Niet alle banken bieden een betaalpakket met die mogelijkheid. Eventuele aanpassingen van het oorspronkelijke betaalbestand worden dan niet eenvoudig opgemerkt.

Lokaal versus online

Betaalpakketten worden steeds vaker volgens de onlinevariant aangeboden. De bestanden met daarin de betaalopdrachten worden vanuit de financiële administratie gegenereerd en direct geïmporteerd in het onlinebetaalpakket. Het betaalpakket bevindt zich op een webserver die gekoppeld is met de infrastructuur van de bank. Het onlinebetaalpakket wordt door middel van een browser via internet benaderd voor zowel het invoeren van betaalopdrachten als het downloaden van de afschriften en de verwerkingsinformatie. Anderzijds worden betaalpakketten offline gebruikt waarbij het betaalpakket lokaal bij de opdrachtgever is geïnstalleerd. Het lokaal geïnstalleerde betaalpakket ontvangt betaalopdrachten uit de financiële administratie of deze worden rechtstreeks ingevoerd. Daarvandaan worden betaalopdrachten naar de bank verstuurd. De verwerkingsinformatie wordt vervolgens via diezelfde verbinding door de bank beschikbaar gesteld in het lokaal geïnstalleerde betaalpakket. Wij zien dat betaalpakketten door de banken steeds vaker online worden aangeboden. Het verschil tussen beide mogelijkheden heeft invloed op het risico tot ongewenste aanpassing van de betaalopdrachten. In het algemeen zal het inherente risico op wijziging van het betaalbestand groter zijn wanneer de betaalbestanden eerst intern worden opgeslagen. De eis van beveiliging van de IT bij banken (kans op reputatieschade bij de bank) is dermate hoog, dat verwacht mag worden dat de verwerking van de betaling bij de bank onder hoge beveiliging zal plaatsvinden. Overigens ontvangt de gebruiker van onlinebetaalpakketten geen zekerheid van de bank omtrent de kwaliteit van haar infrastructuur. Hier moeten de gebruikers vertrouwen hebben in de interne en externe toezichthouders.

De gebruiker ontvangt geen zekerheid van de bank omtrent de kwaliteit van haar infrastructuur

Bovenstaande overwegingen zijn niet alleen van belang voor het beoordelen van de inrichting van het betaalpakket en de bijbehorende beheersingsmaatregelen, maar ook voor het selecteren van een nieuw te implementeren betaalpakket. Het is van belang om aan de hand van de functionele en technische eisen en wensen bovenstaande overwegingen in ogenschouw te nemen.

Regelgeving en richtlijnen

Zoals hierboven eerder is aangegeven, is de organisatie of de auditor zich soms onvoldoende bewust van de risico's, treft men 'bewust' niet voldoende beheersingsmaatregelen of ziet men niet toe op de naleving ervan. Er is ook vrijwel geen wet- en regelgeving op dit punt. Wel zijn er diverse richtlijnen en raamwerken waarin aangegeven staat dat men beheersingsmaatregelen in de kritische processen en informatiesystemen, zoals betaalproces en het betaalpakket, moet aanbrengen.

Risk management principles for electronic banking

De Risk management principles for electronic banking ([Base03]) van het Basel committee on banking supervision van de Bank for international settlements (BIS) zijn opgesteld om banken adviezen ('risk management principles') mee te geven bij het inrichten van e-banking. Hoewel dit document is opge-

steld vanuit het perspectief van de bank zelf, geeft het de gebruiker (als opdrachtgever) genoeg handvatten voor de inrichting van het betaalproces en het betaalpakket.

Hoewel deze veertien adviezen voor de banken zijn uitgegeven om de betrouwbaarheid en continuïteit voor e-banking te waarborgen, zijn ze natuurlijk voor iedereen die betrokken is in het betalingsverkeer van toepassing. De principles betreffen:

A. Board and Management Oversight
1. Effective management oversight of e-banking activities.
2. Establishment of a comprehensive security control process.
3. Comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies.

B. Security Controls
4. Authentication of e-banking customers.
5. Non-repudiation and accountability for e-banking transactions.
6. Appropriate measures to ensure segregation of duties.
7. Proper authorisation controls within e-banking systems, databases and applications.
8. Data integrity of e-banking transactions, records, and information.
9. Establishment of clear audit trails for e-banking transactions.
10. Confidentiality of key bank information.

C. Legal and Reputational Risk Management
11. Appropriate disclosures for e-banking services.
12. Privacy of customer information.
13. Capacity, business continuity and contingency planning to ensure availability of ebanking systems and services.
14. Incident response planning.

Ieder principle wordt in het rapport verder uitgewerkt, waarbij er voor zes principles in een bijlage duidelijke richtlijnen worden geformuleerd:
- security;
- outsourcing;
- authorisation;
- audit trails;
- privacy;
- availability, business continuity en contingency planning.

Voorbeelden van dergelijke richtlijnen zijn:
- *'Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.'*
- *'Specific authorisation and access privileges should be assigned to all individuals, agents or systems, which conduct e-banking activities.'*
- *'E-Banking data and systems should be classified according to their sensitivity and importance and protected accordingly. Appropriate mechanisms, such as encryption, access control and data recovery plans should be used to protect all sensitive and high-risk e-banking systems, servers, databases and applications.'*

Code voor Informatiebeveiliging

De Code voor Informatiebeveiliging is door de International Organization for Standardization en de International Electrotechnical Commission opgesteld en biedt een uitgebreide lijst aan beheersingsmaatregelen voor informatiebeveiliging. Informatiebeveiliging wordt daarin omschreven als de beveiliging van informatie tegen een breed scala van risico's ([ISO05]).

Er wordt in de Code voor Informatiebeveiliging verwezen naar wet- en regelgeving op het gebied van de beveiliging van gegevens, privacy, intellectueel eigendom en de verwerking van gegevens:
- De organisatie dient te allen tijde rekening te houden met de gevolgen voor de informatiebeveiliging door het versturen van gegevens via het internet. Betaalopdrachten worden via het internet naar de bank verstuurd. Bij gevolgen kan worden gedacht aan ongewenste mutaties (juistheid), publiekelijk bekend worden van de inhoud (vertrouwelijkheid) en de kans

dat berichten niet of dubbel aankomen (volledigheid) c.q. het (achteraf) ontkennen dat berichten zijn verstuurd of klagen dat berichten wel zijn verstuurd maar niet zijn aangekomen (tijdigheid). Ook kan het voorkomen dat betaalopdrachten frauduleus door een andere afzender worden ingestuurd als ware het van de organisatie zelf (autorisatie).

- Het overtreden van wet- en regelgeving dient te worden vermeden. Hier valt onder andere te denken aan wetgeving voor privacy, waarbij naast het bedrag ook andere persoonlijke gegevens in de beschrijving/toelichting of in de aard van de betaling zelf in het geding kunnen zijn.
- Medewerkers moeten op de hoogte worden gesteld van hun verantwoordelijkheden ten aanzien van informatiebeveiliging en geheimhouding.

Enkele normen die in de Code voor Informatiebeveiliging worden genoemd zijn:

- *'Duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.'*
- *'Data protection and privacy should be ensured as required in relevant legislation, regulations and, if applicable, contractual clauses.'*

COSO Enterprise Risk Management

Het COSO ERM-raamwerk is een raamwerk voor administratieve organisatie en interne beheersing. Eén van de doelstellingen van dit raamwerk is 'safeguarding of resources', ook wel bekend als 'safeguarding of assets'. Er dienen volgens het COSO ERM-raamwerk dan ook beheersingsmaatregelen aanwezig te zijn die voorkomen dat bezittingen ten onrechte aan de organisatie worden onttrokken. Het proces van uitgaande betalingen is in het bijzonder een proces waar bezittingen (geld) de organisatie verlaten.

Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens schrijft voor dat organisaties persoonsgegevens op een zorgvuldige wijze verwerken, verstrekken en verzamelen (artikel 6, 7 en 8). In deze wet staat onder andere dat persoonsgegevens niet verwerkt mogen worden 'op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen' (artikel 9). De verantwoordelijke organisatie dient 'passende technische en organisatorische maatregelen' te nemen om 'persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking'. Deze maatregelen dienen 'een passend beveiligingsniveau' te garanderen 'gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen' (artikel 13).

Aansluitend is bepaald dat een bank voldoende waarborgen dient te bieden ten aanzien van 'de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen' (artikel 14) ([Overo9a]).

Binnen het betaalproces kunnen op diverse momenten en locaties persoonsgegevens worden opgeslagen en verstuurd. In het begin worden gegevens van medewerkers verzameld om bijvoorbeeld salarissen en declaraties te kunnen betalen. Deze gegevens in de betaalopdrachten bevatten de namen van de betreffende medewerkers, hun bankrekeningnummers, de bedragen (nettosalaris en declaraties) en een bijbehorende omschrijving. Maar ook gegevens over lidmaatschappen, donaties aan bijzondere doelen etc. die in de omschrijving van betalingen kunnen zijn vermeld, kunnen privacygevoelig zijn. Daarnaast dienen de gegevens tijdig weer te worden verwijderd. Het vrijstellingsbesluit ([Overo1]) geeft bij een aantal processen, zoals bij crediteuren en leveranciers, concrete aanwijzingen van bewaartermijnen van dergelijke gegevens (waaronder die van betalingen).

Buiten de BIS-principles zijn de richtlijnen tamelijk generiek

Algemene voorwaarden

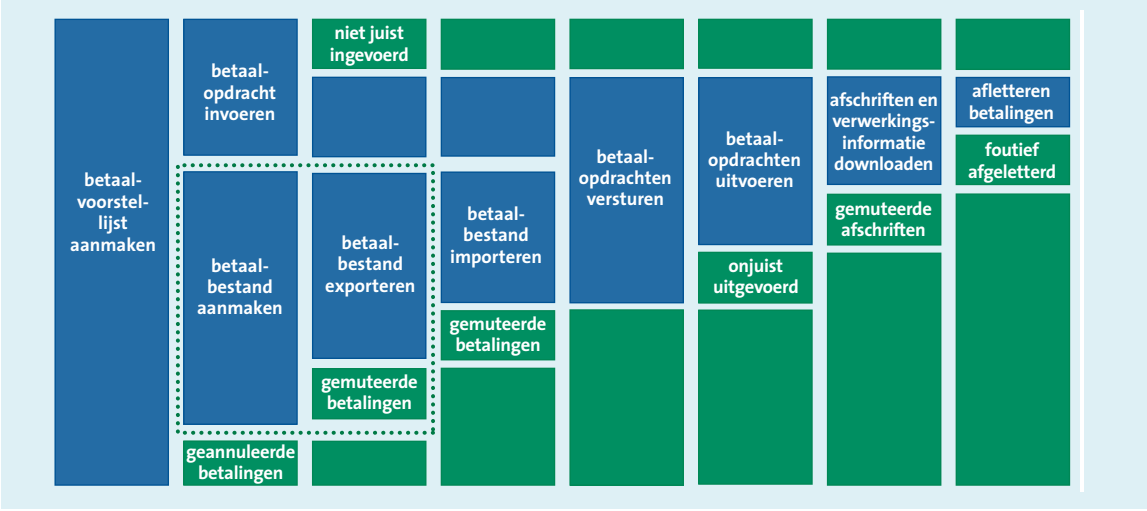
Organisaties dienen aan diverse voorwaarden van de bank te voldoen. Dit staat omschreven in de algemene voorwaarden voor (zakelijk) internetbankieren. Deze voorwaarden zijn van invloed op de wijze waarop de organisaties het betaalproces inrichten.

De algemene voorwaarden van deze banken hebben veel met elkaar gemeen. De organisatie dient zelf controles uit te voeren ten aanzien van de juistheid, volledigheid en tijdigheid van de verwerking van de betaalopdrachten. Verder eist de bank dat de organisatie over een beveiligde (internet)verbinding beschikt. Veelal hebben medewerkers van de organisatie persoonlijke authenticatiemiddelen waarvan men alle elementen geheim dient te houden en niet aan derden ter beschikking mag stellen.

Overige regelgeving

Bovenstaand zijn enkele richtlijnen weergegeven. Buiten de BIS-principles zijn de richtlijnen tamelijk generiek en ook van toepassing op andere processen met een hoog inherent risico of bewuste of onbewuste aanpassingen. Voor de accountantscontrole zijn natuurlijk ook de Nadere voorschriften controle- en overige standaarden (NV COS) en de general IT controls van belang.

Binnen NV COS van het NIVRA en het Besluit toezicht accountantsorganisaties wordt eveneens verwezen naar fraude. Fraude (van materieel belang) wordt in het Besluit toezicht accountantsorganisaties ([Overo9b]) (artikel 36) gedefinieerd als 'opzettelijk handelen […] om een wederrechtelijk voordeel te



Figuur 5. **Voorbeeld van uitwerking bucket-approach voor betaalproces.**

behalen en waarbij de aard of de omvang zodanig is dat beslissingen die in het maatschappelijk verkeer worden genomen op grond van de financiële verantwoording van de controlecliënt zouden kunnen worden beïnvloed door die misleiding'.

NV COS 240 ([NIVR09a]) schrijft voor dat de accountant verantwoordelijk is voor 'het onderkennen van het risico van fraude in het kader van de controle van financiële overzichten'. Hierbij wordt voorgeschreven dat de accountant een 'professioneel-kritische instelling' moet aannemen en 'afwijking van materieel belang als gevolg van fraude' moet bespreken.

De accountant dient 'het risico van een afwijking van materieel belang als gevolg van fraude' in te schatten, zoals in NV COS 315 ([NIVR09b]) staat geschreven. Aansluitend daarop zal hij aanvullende controlewerkzaamheden moeten verrichten.

Analyse met behulp van datamining

Naast een goede inrichting met voldoende beheersingsmaatregelen in het proces kan met behulp van data-analyse een goed inzicht worden verkregen in de betaalstromen en de omvang en aard van eventuele uitval in het betaalproces. Bij uitval zal vrijwel altijd handmatige actie nodig zijn, die veelal fraudegevoeliger is en ook meer risico van het maken van onbewuste fouten oplevert.

Per processtap, zoals eerder beschreven, kan door diverse oorzaken uitval ontstaan. In figuur 5 is op basis van de zogenaamde 'bucket-approach' inzicht gegeven in de stappen uit het betaalproces (verticale kolommen) en buckets waar betaalgegevens per stap zijn opgenomen. De bucket voor de hoofdstroom aan de linkerkant zou idealiter gelijk zijn aan de bucket aan de rechterkant, want dan zijn er geen ongeregeldheden geweest.

Zo kan bijvoorbeeld bij het importeren van het betaalbestand uitval ontstaan ten opzichte van de originele aangemaakte betaalvoorstellijst door gemuteerde betalingen in het betaalbestand. Dit is met stippellijnen weergegeven in figuur 5. De volgende vergelijking moet dan opgaan:

aantal geëxporteerde betalingen = aantal geïmporteerde betalingen + aantal gemuteerde betalingen

Per bucket is zo inzichtelijk te maken hoeveel van de oorspronkelijk te betalen crediteuren uiteindelijk juist en tijdig zijn betaald. Dit kan worden gedaan door per bucket door middel van data-analyse de bestanden/tabellen te analyseren en zo te bepalen hoeveel euro en/of betalingen het betreft. Zo wordt exact inzichtelijk hoeveel betalingen er uitvallen. Uitval heeft als nadeel dat de betreffende betalingen veelal handmatig moeten worden gecorrigeerd, met alle risico's van dien.

Naast het feit dat de betreffende crediteuren niet juist en tijdig zijn betaald, levert dergelijke uitval uitzoekwerk op dat handmatig dient te worden verricht. Het is daarom van belang de omvang van deze uitval te beperken. Hierdoor is het betaalproces als geheel efficiënter te maken: minder handmatige acties.

Verbeteringen

Het betaalpakket brengt traditiegetrouw veel handmatige activiteiten met zich mee, wat tot onnodige risico's leidt.

De combinatie van onversleutelde open bestandsformaten (bijvoorbeeld zoals CLIEOP03) en de tussenkomst van personen in het betaalproces is niet wenselijk. Dergelijke bestanden zijn zeer eenvoudig aan te passen zonder dat dit conflicten met de controletotalen oplevert.

Idealer zou een systeem zijn waarbij de tussenkomst van personen wordt beperkt en betaalbestanden vanuit de financiële administratie via het netwerk naar de bank worden verstuurd. Hierdoor neemt het risico af dat betaalbestanden worden gemuteerd. Banken bieden echter veelal geen mogelijkheid om een geautomatiseerde koppeling (door middel van bijvoorbeeld FTP of SQL) aan te gaan rechtstreeks vanuit de financiële administratie.

Het proces is zo standaard geworden, dat de aandacht voor de risico's lijkt te zijn weggeëbd

Hierbij is het tevens aan te raden een vorm van communicatie te hanteren waarbij de inhoud niet (voor personen) leesbaar is om zo de mogelijkheden om betaalopdrachten te kunnen muteren drastisch terug te dringen. Hiervoor moet de financiële administratie wel in staat zijn een dergelijk formaat of dergelijke versleuteling toe te passen. De bank zal dan als enige over de mogelijkheid moeten beschikken het versleutelde bestand te ontsleutelen. Dit is vergelijkbaar met encryptie waarbij een publieke sleutel en een geheime privésleutel worden gebruikt:

- Voor de vertrouwelijkheid gebruikt de verzender de publieke sleutel van de ontvanger. De ontvanger kan het bericht dan lezen met zijn eigen privésleutel.
- Als het om authenticiteit gaat, versleutelt de verzender het bericht met zijn eigen privésleutel. Zo kan iedereen aan de hand van zijn publieke sleutel controleren of de verzender is wie hij zegt dat hij is.

Conclusie

Elektronisch betalingsverkeer is al geruime tijd het normale medium voor het verrichten van betalingen van organisaties via de eigen bank. Er zijn diverse betaalpakketten die door banken worden aangeboden. Naar hun aard kent het betaalproces, waarbij geld de organisatie verlaat en schulden worden afgeboekt, een hoog inherent risico. Dat risico betreft natuurlijk enerzijds de gevolgen voor een organisatie indien betalingen onjuist worden gedaan, maar anderzijds ook een hoog frauderisico.

Inmiddels is het proces zo standaard geworden, dat de aandacht voor de risico's lijkt te zijn weggeëbd. Toch komen er nog regelmatig fouten en fraudes voor, ook al halen alleen de meest bijzondere fraudes zoals met betaalautomaten de krant.

In het artikel is aangegeven dat de beschikbare regelgeving en richtlijnen voor de inrichting heel beperkt zijn en dat er veelal gesteund moet worden op de meer generieke richtlijnen voor informatiebeveiliging. In het referaat van Lodewijk Benjaminse is op basis van de richtlijnen en aanvullend concreet inzicht een uitgebreid normenstelsel voor de inrichting uitgewerkt.

Voor de beoordeling van de betaalstromen en inzicht in de stroom van betalingen (geautomatiseerd en/of handmatig) en de uitval is data-analyse met behulp van auditsoftware effectief gebleken. Daarbij kan de bucket-approach worden gehanteerd, waardoor in één oogopslag de stroom in aantallen betalingen of omvang van bedragen inzichtelijk wordt gemaakt. Aan de hand van dat overzicht kunnen eventuele bijzonderheden (zoals uitval) worden geanalyseerd.

Literatuur

[Base03] Basel committee on banking supervision, *Risk management principles for electronic banking*, juli 2003 (http://www.bis.org/publ/bcbs98.pdf).

[Boer96] J.C. Boer RE RA, ir. J.A.M. Donkers RE, drs. R.M. Renes en prof. dr. P. Wallage RA, *Corporate Governance; de betekenis voor de ICT-Auditor*, Compact 1996/5.

[Comm04] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management, Integrated Framework*, september 2004.

[Groo08] R. de Groot, M. Grummel en B. Prins, *Het banksaldo aangevuld*, januari 2008 (http://www.accountant.nl/Accountant/Fraude+in+praktijk/Het+banksaldo+aangevuld).

[ISO05] ISO/IEC Standard, *Information technology: Security techniques, code of practice for information security management*, juni 2005.

[NIVR09a] NIVRA, *Handleiding regelgeving accountancy: NV COS 240 (De verantwoordelijkheid van de accountant voor het onderkennen van het risico van fraude in het kader van de controle van financiële overzichten*, oktober 2009 (http://www.nivra.nl/Sites/nivra_site/HRA/200903/html/38351.htm).

[NIVR09b] NIVRA, *Handleiding regelgeving accountancy: NV COS 315 (Kennis van de entiteit en haar omgeving en het inschatten van het risico van een afwijking van materieel belang)*, oktober 2009 (http://www.nivra.nl/Sites/nivra_site/HRA/200903/html/38644.htm).

[Over01] *Vrijstellingsbesluit*, Staatsblad van het Koninkrijk der Nederlanden, 2001 250.

[Over09a] Overheid.nl, *Wet bescherming persoonsgegevens*, oktober 2009 (http://wetten.overheid.nl/BWBR0011468).

[Over09b] Overheid.nl, *Besluit toezicht accountantsorganisaties*, oktober 2009 (http://wetten.overheid.nl/BWBR0020184).