Het vertrouwen van de e-tailer

Elektronisch betalen op internet

Drs. ing. W.F.M. van Egdom

Betaalsystemen op het internet worden talrijker. Steeds meer retailers bieden als e-tailer hun producten aan op het internet en laten bestellingen direct, on line afrekenen. De huidige elektronische betaalsystemen op de fysieke winkelvloer, zoals de pinpas, de Chipper en Chipknip, zijn aan strenge eisen onderhevig en worden onder verantwoordelijkheid van de Nederlandse banken uitgebreid getest en gecertificeerd. Bij internetbetaalsystemen is dit niet zo. Wie garandeert dat de e-tailer zijn geld daadwerkelijk ontvangt? Dit artikel verkent de mogelijkheden daartoe.

Inleiding

Stel een willekeurige retailer voor om zijn kassa's aan het internet te koppelen en hij verklaart je voor gek. Het lijkt inderdaad een onzinnige en vooral gevaarlijke gedachte om deze bedrijfskritische systemen toegankelijk te maken via een publiek netwerk. Uiteraard wordt de retailer verzekerd dat een 'state of the art'-beveiliging zal worden toegepast. Problemen met betalingen ten gevolge van onoordeelkundig gebruik of fraude zullen niet vaker voorkomen dan in de fysieke winkel het geval is.

Een publiekelijk toegankelijke winkelkassa is geen ondenkbare situatie. De manieren om op het internet betalingen te verrichten worden steeds talrijker. Was het voor een jaar alleen nog maar mogelijk om direct, on line te betalen met een creditcard, nu kan er tevens worden afgerekend met een normale bankpas (de pinpas), met een virtuele VISA-card of met een Rabobankpas. De kassa's waarmee consumenten betalingen uitvoeren moeten hiervoor toegankelijk worden gemaakt via het publieke internet. Gevolg hiervan is dat ook back-office systemen met productinformatie direct of indirect toegankelijk kunnen worden vanaf internet omdat kassa's nu eenmaal productinformatie zoals prijzen en artikelnummers nodig hebben om een betaling te kunnen uitvoeren. Vanuit beveiligingsoogpunt is dit een ware nachtmerrie voor de e-tailer.

Dit artikel vergelijkt de zekerheden ten aanzien van de betrouwbaarheid van reguliere betaalsystemen op de fysieke winkelvloer met zekerheden voor de betrouwbaarheid van betaalsystemen op internet. Op basis van een analyse van de risico's van het SET-betaalsysteem wordt beargumenteerd dat e-tailers meer aandacht moeten geven aan het testen en certificeren van systemen voor betalen op internet dan het geval is bij reguliere betaalsystemen.

Media en wetgeving: voornamelijk aandacht voor de surfende consument

In de media en de wetgeving wordt voornamelijk aandacht gegeven aan de consument die waarborgen moet krijgen voor zijn privacy, waarborgen dat het juiste bedrag van zijn rekening wordt afgeschreven en waarborgen dat het bestelde product daadwerkelijk wordt geleverd. Naarmate het gebruik van betalingen op het internet toeneemt, is het belangrijk tevens aandacht te geven aan waarborgen voor de e-tailer die voor zijn bedrijfsvoering afhankelijk is van een betrouwbare afhandeling van betaaltransacties. Voor een gezonde groei van e-commerce is het belangrijk e-tailers ervan te overtuigen dat betaalsystemen voor het internet even betrouwbaar zijn als betaalsystemen op de fysieke winkelvloer.

Ruilhandel en dukaten

De eerste vorm van betalen bestond uit ruil. Vertrouwen in de betalende partij kon direct worden getoetst aan de fysieke kwaliteit van het geruilde object; veelal zout, thee of andere waardevolle zaken. Belangrijk voor de ruilhandel was dat de te ruilen goederen makkelijk deelbaar waren en redelijk waardevast. Omdat ruil bij grote bedragen lastig werd is op een gegeven moment overgestapt op betalingen in goud, aangezien goud goed deelbaar is en behoorlijk waardevast. Het vertrouwen in de betalende partij kon direct worden getoetst door de gouden dukaat enkele eenvoudige tests te laten ondergaan. Slepen met zakken vol dukaten is zwaar, en daarom is later overgegaan op het in bewaring geven van goud bij goudsmeden die hiervoor waardepapieren afgaven. Deze waardepapieren waren makkelijk overdraagbaar. Belangrijk was wel dat de goudsmeden betrouwbaar waren. Omdat de goudsmeden op een gegeven moment meer goud in bezit hadden dan direct werd opgeëist, konden zij meer waardepapieren uitgeven dan werd gedekt door de fysieke voorraad goud. Hiermee was de eerste bank een feit.

Retailers baseren hun vertrouwen in Nederlandse waardepapieren op het algemene vertrouwen in de Nederlandse banken. In de loop der eeuwen is na ruil, dukaten en waardepapieren in de recente jaren tachtig een voorzichtige start gemaakt met het gebruik van plastic geld: de pinpas. Eerst bij de benzinestations en na acceptatie door Albert Heijn langzamerhand door alle Nederlandse retailers. De betrouwbaarheid van deze elektronische betaalinfrastructuur wordt vanaf de start gecontroleerd en gegarandeerd door de Nederlandse banken. Met als resultaat dat al voor het eind van de jaren tachtig gold: pin is in!

Voor de banken is het essentieel dat het vertrouwen van retailer en consument in de elektronische betaalinfrastructuur op generlei wijze wordt beschaamd. Op het moment dat zou blijken dat betalingen soms niet resulteren in een creditering van het banksaldo van de retailer daalt het vertrouwen en is het met het gebruik van elektronisch betalen snel gedaan. Vandaar dat de banken hebben besloten om de implementatie en het gebruik van de betaalinfrastructuur goed te controleren. Hiervoor hebben zij al in het begin van de jaren tachtig een aparte organisatie in het leven geroepen. Interpay is verantwoordelijk voor het beheren, controleren en certificeren van de elektronische betaalinfrastructuur.

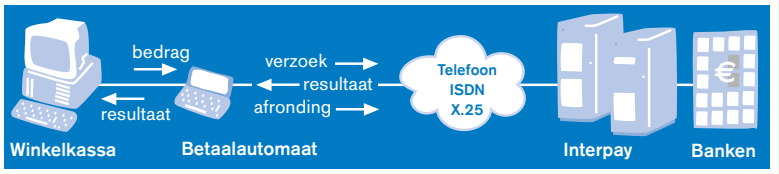
Elektronische betaaltransacties

In grote lijnen werkt de elektronische betaling met pinpas of creditcard[1] als volgt. Een klant die wil afrekenen maakt gebruik van een betaalautomaat die is gekoppeld met de kassa van de retailer. De kassa haalt met behulp van de barcode op het artikel artikelinformatie (zoals prijs, omschrijving, voorraad) op uit de back-office computer. Het te betalen bedrag wordt door de kassa naar de betaalautomaat gestuurd. De klant haalt zijn pinpas door de automaat en toetst zijn pincode in. Vervolgens ziet de klant het bedrag op het display van de betaalautomaat en accordeert de betaling door op de JA-toets te drukken. Op dat moment neemt de betaalautomaat contact op met de centrale computer van Interpay die op zijn beurt verbinding maakt met de bank van de klant. De bankcomputer controleert of de ingevoerde pincode correct is en of de klant voldoende saldo op zijn rekening heeft staan en stuurt, als alles goed is, een akkoord van betaling naar de betaalautomaat. De betaalautomaat geeft vervolgens een akkoord aan de kassa van de retailer en, nadat een bonnetje is geprint, is de betaling afgerond. De transactie tussen betaalautomaat en bankcomputer is beveiligd door onder meer de pincode te versleutelen en alle transactieberichten te voorzien van een digitale handtekening.[2] Na akkoord van de betaling zal de kassa een mutatiebericht sturen naar de back-office computer ten behoeve van voorraadadministratie en financiële verslaglegging.

Certificatie van de betaalinfrastructuur

Om te voorkomen dat er problemen ontstaan met de elektronische betaalinfrastructuur controleert en certificeert Interpay alle typen kassasystemen en betaalautomaten die in Nederland worden geïnstalleerd. Dit betekent dat alleen gecertificeerde betaalsystemen mogen worden geïnstalleerd. Het controle- en certificatieproces verloopt als volgt.

Een retailer die elektronisch wil gaan betalen, moet de kassa plus software die hij gaat gebruiken in combinatie met de betaalautomaat aanbieden aan Interpay voor certificatie. De leverancier van de kassa moet ervoor zorgen dat de koppeling met de betaalautomaat volgens specificaties werkt. Zijn collega die de betaalautomaat levert dient ervoor te zorgen dat de betaalautomaat volgens specificaties werkt. Hiervoor zullen deze leveranciers voordat de certificatie wordt aangevraagd een uitgebreid testtraject moeten doorlopen.



Figuur 1. Verloop van een elektronische betaling.

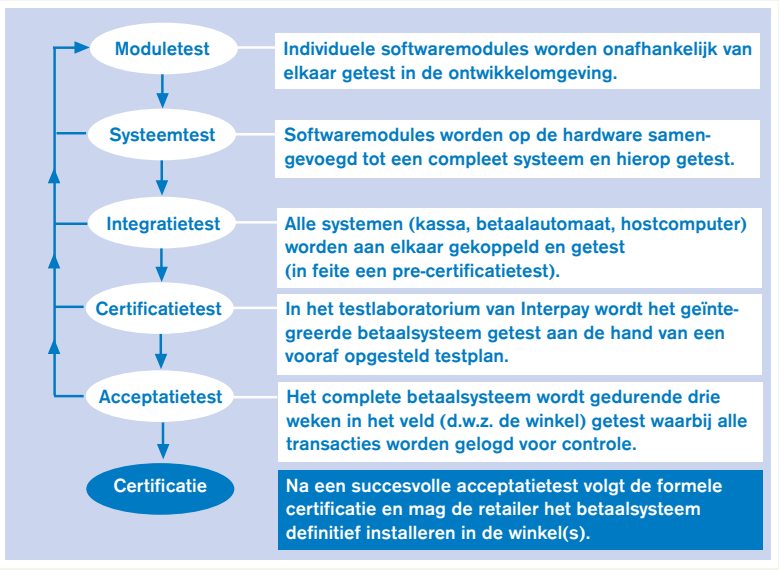
In de praktijk blijkt regelmatig dat fouten die optreden tijdens de certificatie zelden te maken hebben met de beveiliging zoals de DES-encryptie en MAC'ing (MAC: Message Authentication Code) van betaaltransacties. Betaalautomaten die al enkele maanden of zelfs jaren worden gebruikt, zijn dermate betrouwbaar dat er weinig tot geen fouten meer in voorkomen. Dit geldt niet voor de koppeling tussen de betaalautomaat en de kassa of tussen kassa's en back-office systemen. Elke nieuwe kassa die wordt gekoppeld aan een betaalautomaat blijkt eigen, specifieke problemen te hebben met timing, transactieverwerking, printen van kassabonnetjes, etc. Het komt bijvoorbeeld regelmatig voor dat tijdens een certificatietest blijkt dat de kassa aangeeft dat een betaling succesvol is verlopen terwijl de betaalautomaat aangeeft dat dit niet het geval is, of andersom. Dat deze problemen worden gevonden, is te danken aan het nauwkeurig testen door Interpay door testers die bedreven zijn in hun vak. Een gevolg van deze strenge certificatietests is dat de kassaleverancier aanpassingen moet maken in zijn software waardoor de kassa-applicatie robuuster wordt.

Vertrouwen in elektronisch betalen hoog

Voor de retailer is het bijzonder prettig dat een onafhankelijke partij alle componenten van zijn elektronisch betaalsysteem aan een nauwkeurige en vooral kritische certificatietest onderwerpt. De retailer betaalt Interpay voor deze (verplichte!) dienst. De retailer krijgt hierdoor zekerheid dat zijn betaalsysteem betrouwbaar is en voldoet aan de strenge eisen die worden gesteld door de Nederlandse banken. Een gevolg hiervan is dat het vertrouwen in elektronisch betalen hoog is. In het jaar 2000

1) Op dit moment worden alleen Eurocard-Mastercard en VISA afgehandeld via Interpay. Andere creditcards (Amex, Diners, JCB, etc.) worden direct door de creditcardmaatschappij afgehandeld.
2) In dit geval een Message Authentication Code, gebaseerd op een symmetrische sessiesleutel, 56 bits DES.

Figuur 2. Verloop controle- en certificatieproces.



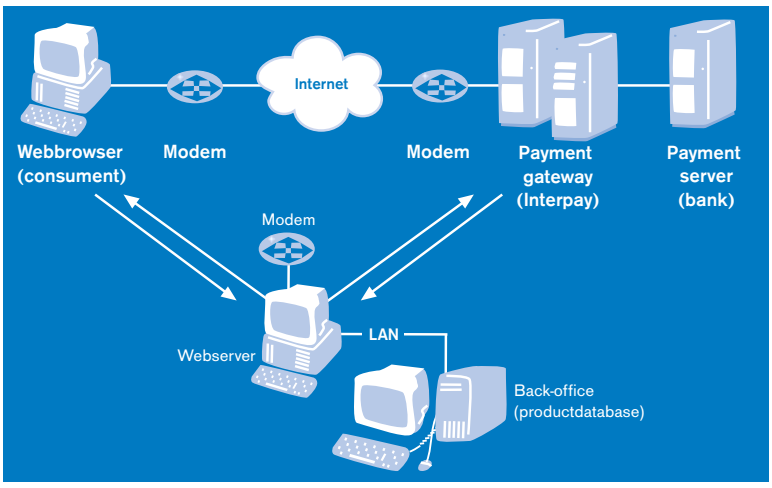
waren er in Nederland ruim 147.000 betaalautomaten geïnstalleerd die gezamenlijk zorgden voor 700 miljoen betaaltransacties per jaar[3].

Betalen op het internet

Het bouwen en installeren van betaalsystemen op internet is aanzienlijk vrijer dan het geval is in de fysieke wereld. Een e-tailer die zijn klanten wil laten betalen met creditcards kan dit doen zonder ook maar een enkele vorm van tests en certificatie. Er is dan ook lange tijd onzekerheid geweest over de mate van betrouwbaarheid van deze betaalsystemen. In eerste instantie hebben creditcardmaatschappijen e-tailers niet toegestaan betalingen te verrichten op internet zonder enige vorm van beveiliging. E-tailers werden verplicht om creditcardgegevens te ontvangen via een apart kanaal, zoals telefoon en fax, of gebruik te maken van encryptietechnieken, zoals SSL (zie hierna). Echter, certificatietests voor deze systemen zijn niet verplicht gesteld en het is eveneens de vraag in hoeverre e-tailers hun eigen betaalsystemen afdoende laten testen. Het komt bijvoorbeeld voor dat e-tailers niet in staat zijn te achterhalen of een betaling succesvol is verlopen of niet. Ook komt het regelmatig voor dat hackers toegang hebben weten te krijgen tot een e-commerceserver waardoor creditcardgegevens kunnen worden gestolen. Hoeveel geld e-tailers verliezen doordat zij artikelen leveren terwijl de betaling hiervoor niet correct is verlopen, is niet bekend. Wel is bekend dat e-tailers onbewust betalingen accepteren van frauduleuze creditcards en dat VISA en Mastercard hiervoor boetes eisen variërend van *f* 50 tot *f* 200 per transactie[4].

Op het moment dat e-commerceservers grote aantallen bestellingen en betalingen krijgen te verwerken is het van groot belang volledig te kunnen vertrouwen op de betrouwbaarheid van de toegepaste betaalsystemen. Elke mislukte betaling, ten gevolge van systeemfouten, configuratiefouten of hacking, heeft een negatieve invloed op marges en is ongunstig voor het algemene vertrouwen in e-commerce. Uit onderzoek van Gartner is gebleken dat een gemiddelde e-commerceserver op piektijden zeker twintig betaaltransacties per minuut te verwerken kan krijgen[5]. Voor de gemiddelde e-tailer kan omzetderving als gevolg van een onbetrouwbaar betaalsysteem bij deze aantallen transacties derhalve snel in de papieren gaan lopen.

3) Interpay 2000. Cijfers over 1999 en 2000.
4) Het Parool, zaterdag 13 mei 2000.
5) Gartner, november 1998.
6) Het inherente risico is gedefinieerd als: de kans dat een dreiging werkelijkheid wordt, waarbij wordt uitgegaan van de bestaande situatie, dat wil zeggen zonder dat er extra beveiligingsmaatregelen worden genomen. Kansen, impact en inherent risico zijn binnen ITAM gecategoriseerd naar Laag, Midden en Hoog.
7) Deze analysemethode kan ook worden gebruikt voor andere soorten betaalsystemen. Tabel 1 moet in dat geval enigszins worden aangepast.



Figuur 3. Betaalinfrastructuur via internet met SET.

Secure Sockets Layer (SSL)

De meest toegepaste methode om betalingen met creditcards te beveiligen is SSL. SSL komt neer op het versleuteld versturen van alle transactiegegevens van de consument naar de e-tailer. Tevens biedt SSL de consument de mogelijkheid na te gaan of de e-tailer beschikt over een certificaat waarmee de betrouwbaarheid van de e-tailer kan worden aangegeven. Dit certificaat heeft een meer of minder beperkte waarde afhankelijk van de organisatie die het heeft uitgegeven. Ook biedt SSL de e-tailer de mogelijkheid na te gaan of de consument is wie hij zegt te zijn. In de praktijk wordt van deze optie geen gebruik gemaakt omdat het verstrekken van certificaten aan consumenten niet eenvoudig is. Voor de e-tailer is er derhalve geen garantie dat de consument is wie hij zegt dat hij is en of de gebruikte creditcard frauduleus is of niet. Om dit hogere frauderisico af te dekken zijn de provisies die op creditcardbetalingen moeten worden afgedragen aan de creditcardmaatschappij aanzienlijk hoger dan in de fysieke wereld het geval is. Tevens is de privacy van de consument niet gewaarborgd omdat transactiegegevens alleen tijdens transport zijn beveiligd.

I-Pay met SET

Een andere manier om betaaltransacties over internet te beveiligen is gebruik van het Secure Electronic Transaction (SET)-protocol. SET biedt een hogere betrouwbaarheid van betaaltransacties dan bij SSL het geval is. Bij SET wordt zowel de e-tailer als de consument geauthenticeerd waarbij de digitale certificaten worden uitgegeven door de organisatie die een nauwe band heeft met de uitgever van het betaalmiddel. In Nederland verstrekt Interpay certificaten aan consumenten die willen betalen met hun pinpas en/of creditcard en aan e-tailers die deze betaalmiddelen willen accepteren en betalingen willen laten bijschrijven op hun Nederlandse bankrekening.

Risicoanalyse I-Pay met SET

Het is mogelijk een analyse te maken van de risico's die een e-tailer loopt bij het accepteren van betalingen over het internet. Voor deze risicoanalyse kan bijvoorbeeld gebruik worden gemaakt van de Internet Threat Assessment Methodology (ITAM) van KPMG. De risicoanalyse binnen ITAM maakt gebruik van de volgende variabelen:

- dreigingen;
- de kans dat deze dreigingen optreden;
- de impact van een dreiging op de bedrijfsvoering;
- het inherente risico[6] voor de e-tailer als gevolg van een mogelijke dreiging.

In deze analyse wordt uitgegaan van een e-tailer die gebruikmaakt van I-Pay met SET[7]. Een SET-betaling is opgebouwd uit meerdere deeltransacties tussen de afzonderlijke systeemonderdelen. Een transactie bestaat uit het versturen en vervolgens bewerken van een bericht, het ontvangen en bewerken van de respons op dat bericht en het opslaan van het resultaat.

De SET-betaling verloopt in grote lijnen als volgt:
* De kassa op de e-commerceserver haalt de artikelgegevens (prijs, artikelnummer) op uit de back-office.
* De kassa verstuurt de artikelgegevens naar de www-browser van de consument.
* De wallet van de consument stuurt de betaalopdracht (rekeningnummer, kaartnummer, bedrag) naar de SET-applicatie in de webwinkel.
* De SET-applicatie stuurt de OI (order information) naar de kassa voor verwerking.
* De SET-applicatie stuurt het autorisatieverzoek (PI - payment instructions) naar de payment gateway en ontvangt de autorisatierespons.
* De SET-applicatie stuurt de autorisatierespons naar de kassa.
* De kassa stuurt de autorisatierespons naar de back-office voor verwerking en opslag.
* De SET-applicatie stuurt de autorisatierespons naar de wallet van de consument.

Voor elke deeltransactie kunnen dreigingen worden onderkend. Er zijn dreigingen ten aanzien van de integriteit, vertrouwelijkheid en beschikbaarheid van transacties. Deze dreigingen kunnen optreden tijdens het

back-office	↔	kassa					art.nr. en bedrag
		kassa	↔			www-client	bedrag
		kassa	↔			www-client	zet in shopping basket
				SET	E ↔	wallet	bedrag
		kassa	↔	SET	E ↔	wallet	betaalgegevens (OI en PI)
				SET	E ↔	gateway	autorisatie
back-office	↔	kassa	↔	SET	E ↔	gateway	respons op autorisatie
					E ↔	wallet	respons op autorisatie

Figuur 4. Globaal verloop van een SET-betaaltransactie.

Dreigingen ten aanzien van Integriteit	Kans	Impact	Risico
Gegevenswijziging tijdens opslag Artikelgegevens (prijs, artikelnummer) in de back-office kunnen worden gewijzigd. Met enige technische kennis van zaken is dit mogelijk zowel van binnen de organisatie als van buiten.	M/H	H	H
Het resultaat van een betaling wordt opgeslagen in de back-office en kan worden gewijzigd. Afhankelijk van de verwerking van transacties (real time of in batch) is deze dreiging middelmatig tot hoog.	M/H	H	H
Gegevenswijziging tijdens transport Artikelgegevens kunnen tijdens het transport van de back-office naar de webserver/ kassa-applicatie worden gewijzigd.	M	H	H
Artikelgegevens kunnen tijdens transport tussen kassa-applicatie en SET-applicatie worden gewijzigd. De kans op deze dreiging is afhankelijk van de implementatie. Deze dreiging is het hoogst wanneer transport plaatsvindt over een externe datacommunicatieverbinding en het laagst wanneer de kassa- en SET-applicaties op dezelfde machine draaien.	L/M	H	M
Artikelgegevens kunnen tijdens het transport van de SET-applicatie naar de walletapplicatie (en terug) worden gewijzigd. De encryptie die in SET wordt gebruikt, is op dit moment 56 bits voor de symmetrische sessiesleutel. Het vinden van deze sleutel tijdens de transactie (een korte sessie) kan als onmogelijk worden beschouwd, zodat de kans van optreden laag is.	L	H	L
De prijs kan in het autorisatieverzoek naar de payment gateway worden gewijzigd en in de respons. De SET-beveiliging maakt de kans op deze dreiging laag.	L	H	L
Het resultaat van een betaling kan tijdens het transport van de SET-applicatie naar de kassa-applicatie en/of de back-office worden gewijzigd. Afhankelijk van de gekozen implementatie is de kans van optreden van deze dreiging laag tot hoog[8].	L/H	H	H
De autorisatierespons kan tijdens transport naar de wallet worden gewijzigd. Laag vanwege de SET-beveiliging.	L	M	L
Gegevenswijziging tijdens verwerking Artikelgegevens kunnen tijdens verwerking door de kassa-applicatie worden gewijzigd doordat (1) de kassa-applicatie (bijvoorbeeld een cgi bin bestand) wordt gewijzigd of dat de programmeur van de kassa-applicatie een trapdoor inbouwt (wat in de praktijk al is gebeurd) of (2) een hacker het webformulier dat de artikelgegevens bevat, wijzigt[9].	M/H	H	H
De prijs kan tijdens verwerking in de SET- of walletapplicatie worden gewijzigd. Aangezien SET-applicaties zijn beveiligd met een certificaat is de kans van optreden laag.	L	H	L

Tabel 1. Inherente risico's van SET-betalingen ten aanzien van Integriteit.

8) SET biedt de mogelijkheid om de SET-applicatie remote te draaien. Het transactieresultaat wordt dan onversleuteld naar de retailer verstuurd per e-mail. De kans van optreden van gegevenswijziging tijdens transport is dan hoog (zie handleiding KASAPI, I-Pay, 14-01-2000, pag. 20).

9) Dit is meermalen voorgekomen en wordt onder meer gemeld door ISS - Xforce die elf shopping basket-applicaties heeft onderzocht die kwetsbaar zijn voor een dergelijke aanval. Zie http://xforce.iss.net/alerts/advise42.php3.

Tabel 2. Inherente risico's van SET-betalingen ten aanzien van Vertrouwelijkheid en Beschikbaarheid.

Dreigingen ten aanzien van Vertrouwelijkheid en Beschikbaarheid	Kans	Impact	Risico
Schending vertrouwelijkheid van gegevens Onbevoegd inzien van persoonlijke gegevens van klanten en hun koopgedrag. Deze gegevens kunnen zijn opgeslagen in de back-office. Afhankelijk van de implementatie is deze kans laag tot hoog.	L/H	M	H
Onbevoegd inzien van betaalgegevens van klanten (rekeningnummers en in geval van creditcards: kaartnummers en vervaldata). Aangezien SET deze gegevens sterk beveiligt, is de kans op deze dreiging laag.	L	M	L
Te lage beschikbaarheid van systemen Onvoldoende processing power in de server van de e-tailer voor het uitvoeren van de noodzakelijke encryptie- en decryptieslagen. Met name SET-applicaties vragen relatief veel processing power. Deze dreiging is afhankelijk van de capaciteit van beschikbare systemen[10].	L/H	H	H

transport, de bewerking en de opslag van transactiegegevens. Als we de kans dat een dreiging daadwerkelijk optreedt combineren met de impact die deze dreiging heeft op de bedrijfsvoering van de e-tailer, kunnen we een schatting maken van het intrinsieke risico voor elke dreiging. De dreigingen met bijbehorende kans van optreden en het hieruit resulterende inherente risico zijn weergegeven in de tabellen 1 en 2.

Op basis van de risicoanalyse kunnen we stellen dat bij het betalen met SET de hoogste risico's worden gelopen bij:

* het ontvangen en versturen van gegevens tussen de back-office en de kassa;
* het ontvangen en versturen van gegevens tussen de kassa en de SET-applicatie;
* het opslaan van gegevens op de back-office;
* de beschikbaarheid van transactieverwerkende systemen ten aanzien van encryptie.

De betrouwbaarheid van een betaalsysteem dat gebruikmaakt van SET is derhalve met name afhankelijk van de betrouwbaarheid van de achterliggende systemen. Vandaar dat bij het testen van een SET-betaalsysteem de nadruk moet liggen op de achterliggende systemen. Een integratietest waarbij het totale betaalsysteem wordt getest, is derhalve onmisbaar.

Testen en certificeren van e-betalen

Voor betaalsystemen met SET is een certificatie verplicht gesteld door SETCO, de organisatie die het SET-protocol beheert. Een e-tailer mag alleen het officiële SET-logo plaatsen in zijn webwinkel als hij gebruikmaakt van een gecertificeerde SET-applicatie. De certificatie die SETCO verplicht stelt beperkt zich echter tot de transactieafhandeling tussen SET-applicatie, wallet en payment gateway. De kassa-applicatie van de e-tailer en de bijbehorende back-office maken geen deel uit van de certificatie.

Een integratietest en acceptatietest worden door SETCO niet verplicht gesteld. Een belangrijk deel van de risico's voor de e-tailer wordt derhalve niet gedekt door middel van een formeel certificatietraject. We hebben gezien dat dit voor betaalsystemen in fysieke winkels wel het geval is. Tevens is aangegeven dat in certificatietests (i.c. integratietests) vaak blijkt dat juist de achterliggende systemen debet zijn aan het niet correct afhandelen van betalingen. E-tailers dienen zich te realiseren dat een integratietest (bij voorkeur gecombineerd met een acceptatietest) noodzakelijk is om de betrouwbaarheid van het internetbetaalsysteem aan te tonen.

Conclusies

We kunnen concluderen dat op dit moment de integratie van SET-applicaties in een e-commerceomgeving de volledige verantwoordelijkheid is van de e-tailer. Het vertrouwen dat de retailer tot nog toe kon hebben in de betrouwbaarheid van elektronische betaalmiddelen is voor de e-tailer voor een significant deel verschoven van de bank naar de e-tailer zelf.

Op het moment dat in de praktijk blijkt dat e-tailers problemen blijven houden met het ontvangen van internetbetalingen ten gevolge van configuratiefouten, systeemfouten of hackers, zal de aandacht voor het zorgvuldig en compleet testen van deze betaalsystemen toenemen. Omdat e-tailers weinig tot geen ervaring hebben met het definiëren en uitvoeren van systeem-, integratie- en acceptatietests zullen zij ondersteuning vragen van organisaties die dit wel hebben. Het is niet ondenkbaar dat organisaties vormen van certificatie zullen introduceren voor betaalsystemen op het internet. Ervaring uit de wereld van het fysieke betalen leert dat de e-tailer die gebruikmaakt van een gecertificeerd internetbetaalsysteem zich minder ongerust hoeft te maken of hij zijn geld wel ontvangt.

10) Gartner heeft een uitgebreide studie gedaan naar de performance-eisen voor systemen die SET- en SSL-transacties verwerken (SET comparative performance analysis, Gartner, 2 november 1998).

Drs. ing. W.F.M. van Egdom is als manager werkzaam bij KPMG Information Risk Management in Amstelveen. Hij heeft in de periode van 1993 tot heden uitgebreide ervaring opgedaan met elektronische transactiesystemen, zowel in de rol van technisch consultant als in de projectleiderrol.