Sicherheit von Online-Bezahldiensten

Als der New Yorker Frank McNamara 1950 in einem Restaurant die Rechnung nicht bezahlen konnte, überzeugte der den Restaurant-Besitzer, per Unterschrift zu bezahlen und das Geld später zu überweisen, die Idee der Kreditkarte war geboren. Zumindest erzählt es die Legende (vgl. [Franke]). Denn Kreditkarten wurden in USA von Hotels, Ölgesellschaften oder Kaufhäusern bereits seit den 20er Jahren an treue Kunden ausgegeben. Frank McNamara erweiterte das Konzept der Kundenkarten jedoch zur universellen Karte, mit der Menschen auch ohne persönliches Vertrauen ein Kreditverhältnis eingehen konnten. Die Firma Diners Club, die er 1950 zusammen mit Ralph E. Schneider gründete, übernahm eben diese Rolle des vertrauenswürdigen Mittlers, die für die eingegangen Kaufverpflichtungen gerade stand. Der Rest der Geschichte ist bekannt, Kreditkarten wie Diners Club, American Express, Visa oder Mastercard eroberten weltweit der Portemonnaies der Besserverdiener, deren Kreditwürdigkeit die Vorzüge des bargeldlosen Einkaufs ermöglichten. Mit der Virtualisierung des Bargelds stieg aber auch die Möglichkeit des Missbrauchs. Denn jede Kaufhandlung basiert auf dem Vertrauen der beiden Vertragspartner: Der Käufer vertraut darauf, dass der Händler die Ware liefert. Dieser vertraut, dass der Käufer den vereinbarten Preis bezahlt. Vertrauen ist die Grundlage von Handlungen in unsicheren Situationen. In der besten aller Welten gibt es diese Unsicherheit nicht, das in einen Menschen gesetzte Vertrauen wird nicht enttäuscht und ein System wie das von Frank McNamara funktioniert reibungslos. Zahle ich heute nicht, so doch gewiss morgen. Und habe ich gestern bereits gezahlt, lieferst Du gewiss heute.

Vertrauen aber kann enttäuscht und getäuscht werden. Mit der Komplexität des Prozesses steigt die Unsicherheit der Teilnehmer. Vertrauensbildende Maßnahmen sind erforderlich. Technische Sicherheit soll Vertrauen dort stärken, wo es enttäuscht werden kann. Fehlendes Vertrauen in einen Prozess wird damit durch Vertrauen in ein technisches Verfahren kompensiert. Wenn ich bspw. bei der Übermittlung eines Briefes befürchte, der Bote könne ihn lesen, kann ich den Inhalt verschlüsseln. Misstrauen in den Boten wird in diesem Fall durch Vertrauen in die Sicherheit des kryptografischen Verfahrens ausgeglichen.

Doch die Datenübertragung ist nur ein sicherheitskritischer Aspekt, der bei Online-Bezahlsystemen zu berücksichtigen ist. Um Vertrauen in die Sicherheit eines Verfahrens zu erzeigen, sind geeignete technische und soziale Fragen zu beantworten (vgl. [KompEC], S.67):

1. Wahrung der Anonymität
Gibt es eine Möglichkeit für den Käufer oder den Verkäufer, Waren anonym zu handeln oder ist jeder Kaufvorgang mit persönliche Daten verknüpft? Die Mehrheit der Online-Bezahlsysteme ist nicht anonym mit dem Argument, dies würde die Sicherheit der Transaktionen erhöhen. Der Mehrheit der Nutzer scheint der Umstand aber egal zu sein, dass sie eine der herausragenden Eigenschaften des Bargelds verlieren. Elektronisches Bezahlen wird immer noch als Überweisung oder Ausstellen eines Schecks gesehen und weniger als elektronische Umsetzung des Bargeldprinzips.

2. Echtheit der Vertragsparteien
Wie könne die Teilnehmer sicher gehen, dass die Anderen diejenigen sind, für die sie sich ausgeben? Neben Käufer und Verkäufer sind an einem Online-Kaufvorgang häufig noch vertrauensbildende Zwi-

scheninstanzen beteiligt. Wenn Händler und Kunde sich nicht trauen, können sie doch beide dem Vermittler glauben. Doch dafür muss auch dieser erst einmal seine Identität beweisen.

3. Sicherheit der übertragenen Daten
Wie wird verhindert, dass die für den Kaufvorgang relevanten Daten in falsche Hände gelangen? Besonders kritisch sind die Daten, mit denen der Bezahlvorgang unmittelbar ausgelöst wird, z.B. Kontonummern, PIN und TAN-Nummern beim Online-Banking. Werden diese Daten abgefangen oder auf dem Weg verändert, ohne dass die Vertragsparteien davon Kenntnis erlangen, können Finanzströme leicht in falsche Kanäle geleitet werden.

4. Zahlungs- und Liefersicherheit
Wie können Käufer und Verkäufer sicher stellen, dass der Partner seinen Zahlungs- bzw. Lieferverpflichtungen nachkommt? Welche Schutzmöglichkeiten haben sie im Problemfall? Die einfachste Lösung für den Händler ist es, erst nach Zahlungseingang zu liefern. Dummerweise sieht der Kunde das genau anders herum, er würde am liebsten erst nach Erhalt der Ware zahlen. Der Kompromiss ist die Zahlung während der Lieferung, doch muss gesichert sein, dass beide Parteien sich an diese Abmachung halten.

Elektronische Bezahlsysteme

Die eingangs erwähnten Kreditkarten sind nur eine von vielen Möglichkeiten, Geschäfte ohne Bargeld abzuwickeln. Grob lassen sich die Systeme in die folgenden sechs Kategorien einteilen (vgl. [IWW], [Krüger, Anhang B]). Tatsächlich gibt es noch weitere, z.B. elektronische Scheckkarten, Nachnahme oder Lastschriften, die hier jedoch nicht weiter behandelt werden.

1. Elektronische Rechnungen
2. Kreditkartenzahlung
3. Inkasso/Billing-Systeme
4. Email-Systeme: Paypal
5. Mobile Systeme: Paybox, net900
6. Elektronisches Bargeld

Im Folgenden werden diese Kategorien unter den oben benannten Sicherheits-Aspekten und an ausgewählten Beispielen diskutiert. Im Unterricht können sie in eigenen Unterrichtsstunden behandelt werden. Eine Gruppierung mehrerer Beispiele bietet sich z.B. nach dem Zeitpunkt des Bezahlvorgangs an: Die Beispiele 1-3 gehören zu den *Pay-Later-*, 4 und 5 zu den *Pay-direct-* und Beispiel 6 zu den *Pre-Paid-*Verfahren. Eingebettet und verknüpft werden können diese Stunden in Unterrichtseinheiten zum Thema Kryptographie, zu Modellieren mit Sicherheitsprotokollen, zu E-Commerce und digitaler Ökonomie oder auch zu dem Bereich Vertragsrecht. Die Ausarbeitung konkreter Unterrichtsentwürfe ist in Vorbereitung und wird zu einem späteren Zeitpunkt veröffentlicht (Ungeduldige können bei [Markmann] einen guten Einstieg finden).

1. Elektronische Rechnungen

Beispiel: Online-Banking

Online-Banking gehört zu den am häufigsten genutzten Internet-Diensten. Banken bieten Web-Interfaces für die wichtigsten Bank-Transaktionen an. Bei der Anmeldung identifizieren die Nutzer sich mittels der Kontonummer, die Authentifizierung erfolgt durch eine Geheimzahl, die Personal Identification Number (PIN). Jede Transaktion wird zusätzlich durch eine Transaktionsnummer (TAN) bestätigt. 100 dieser TANs bekommt der Nutzer auf dem Postweg zugesandt. Diese Kombination von online und offline-Sicherheit ist maßgeblich für das Vertrauen verantwortlich, das Nutzer dem Online-Verfahren entgegen bringen. Selbst wenn jemand widerrechtlich Zugang zu dem System erlangt, sind immer noch keine Transaktionen ohne Kenntnis der TANs möglich.

Die Datenübertragung wird beim Online-Banking über SSL gesichert. Das Verfahren ist inzwischen so zuverlässig, dass Betrüger sich zunehmend auf die Benutzer konzentrieren. Mit gefälschten Emails wird versucht, an die Zugangsdaten zu gelangen. Unter dem Vorwand eines technischen Problems werden Kunden aufgefordert, ihre PIN und mehrere TANs in ein Webformular einzutragen. Für dieses Vorgehen hat sich der Begriff *Passwort-Fishing* oder kurz *Phishing* durchgesetzt. Es scheint erfolgreich genug zu sein, dass die Phisher Probleme haben, die Nummern gewinnbringend einzusetzen. Denn sie können sich ja nicht einfach Geld auf ihr eigenen Konto überweisen. Also werden in einem zweiten Schritt Menschen gesucht, die als *finance manager* ihr Konto für gelegentliche Auslandsüberweisungen zur Verfügung stellen, 10% der Überweisungssumme inbegriffen. Als Konsequenz steht die Kriminalpolizei vor der Tür dieser Finanzmanager, die sich dem Vorwurf der Geldwäsche ausgesetzt sehen und regelmäßig schadensersatzpflichtig sind. Phishing ist eine ausdifferenzierte Form des social engineering, in dem Gutgläubigkeit, Naivität und Gier ausgenutzt werden. Der Schaden allein in Deutschland belief sich 2005 laut Focus und LKA-Quellen auf 4.5 Mio. Euro, Tendenz steigend. Als Gegenmaßnahme stellen deutsche Banken auf indizierte TAN (iTAN) um. Statt einer beliebigen TAN wird jede Transaktionen nun mit einer bestimmten TAN verknüpft. Als Reaktion versuchen Phisher zunehmend, die notwendigen Informationen per Telefon zu erfragen, indem sie sich z.B. als Service-Techniker der Hausbank ausgeben und eine bestimmte iTAN für Wartungsarbeiten benötigen. Auch Spyware- und Backdoor-Angriffe (s.u.) lassen sich durch iTANs nicht stoppen.

Sicherung: Die beste Sicherheit gegen Phishing ist Grundwissen über das Verfahren des Oline-Banking und vor allem über das Verhalten der Banken, die versichern, niemals Zugangsdaten per Mail oder Telefon zu erfragen.

2. Kreditkartenzahlung

Beispiele: MasterCard, Visa-Card, American Express

Sehr bequem und weit verbreitet ist die Online-Bezahlung per Kreditkarte. Drei der vier Sicherheitsfragen werden dem Kredikartenunternehmen übertragen. Es prüft die Volljährigkeit und Bonität des Karteninhabers, es garantiert die Zahlung und kümmert sich um die Rückzahlung des Kredits beim Kunden. Und ermöglicht es diesem, unberechtigte Zahlungsforderungen zu stornieren. Den Preis für diese

Übernahme von Geschäftsrisiken trägt einerseits der Händler mit Margen bis zu 7%, andererseits der Kunde durch Zahlung einer jährlichen Gebühr. Zur Sicherheit der Datenübertragung wird SSL verwendet. Dennoch verursacht Betrug mit gestohlenen Kreditkarten einen Schaden, der jährlich auf mehrere Hunder Mio. Euro geschätzt wird. Genaue Zahlen werden von den Kreditkartenunternehmen nicht veröffentlicht.Denn viele online-Transaktionen lassen sich lediglich mit Name des Karteninhabers, Kreditkartennummer und Gültigkeitsdatum tätigen. Bei internationalen Lieferungen oder gar bei Software-Downloads ist die Ware längst verschwunden, ehe der rechtmäßige Kontoinhaber auch nur Einspruch erheben kann.
Um die Echtheit der Vertragsparteien zu garantieren, wurde das Secure-Electronic–Transaction-Verfahren (SET) eingeführt. Hierbei Händler, Kunde und vermittelnde Bank werden über ein Zertifikat identifiziert und müssen darüber hinaus bestimmte Software auf ihren Rechnern installieren, der Kunde üblicherweise ein Browser-Plugin, mit der die Transaktionen verwaltet und verschlüsselt übertragen werden können.
Das SET-Protokoll ist gegen einfache Manipulationen der Daten gesichert. Die Zertifikate sichern die Identität der Teilnehmer. Doch eben dort liegt die Schwäche des Verfahrens. Mit gestohlenen Kreditkarteninformationen ist es einem Angreifer möglich, ein gefälschtes Zertifikat zu erwerben und damit Transaktionen durchzuführen. Das Hauptproblem dürfte aber die Trägheit der Anwender sein bzw. die fehlende Bereitschaft, ein Zertifikat und ein Plugin zu installieren. Insofern unterscheiden sich die Probleme bei online-Kreditkartengebrauch kaum von den Manipulationsmöglichkeiten, die offline möglich sind.
Informationen über Karteninhaber, Kartennummer und Gültigkeitsdatum stehen auf jedem Abrechnungszettel, die massenweise in Mülleimern vor Supermärkten, Tankstellen und Restaurants zu finden sind, eine Technik, die unter Spezialisten als *Dumpster Diving* bekannt ist. Da die gängigen Daten als kompromittiert gelten können, gehen Anbieter zunehmend dazu über, eine dreistellige Prüfnummer einzufordern, die auf der Rückseite der Kreditkarten zu finden ist und die gerade nicht auf Abrechnungen erscheint. Darauf reagieren die Phisher, indem sie per Telefon eben dieses Nummer erfragen, indem sie sich als Mitarbeiter des Kreditkartenunternehmens ausgeben.
Sicherung: Da das zentrale Problem beim Kreditkartensystem die Informationen sind, die auf der Karte bzw. auf den Abrechnungen zu finden sind, ist das Hauptangriffsziel nicht die Technik, sondern der Mensch. Die besten Sicherungsmöglichkeiten sind ähnlich wie beim Online-Banking Misstrauen und Vorsicht.

3. Inkasso/Billing-Systeme

Beispiele: Click & Buy (FirstGate); Bill-it-easy (montax)
Ebenfalls auf SSL setzt Firstgate Click&Buy, ein Micropayment-System für Transaktionen mit kleinen Beträgen, bevorzugt für den Erwerb von Digitalen Medien, z.B. Dokumente, Zeitungsartikel, Software oder Musikdateien . Firstgate sammelt die Rechnungsbeträge (billing) und bucht sie monatlich vom Konto des Kunden ab (Inkasso), der gleichzeitig Kunde von Firstgate sein und seine persönlichen Daten hinterlegen muss. Die Bezahlung läuft über ein Lastschriftverfahren. Bill-it-easy von montax payment services rechnet über die Provider-Rechnung ab, der natürlich eine Partnerschaft mit montax eingehen muss. Ähnlich wie beim Kreditkartensystem werden Vertrauens- und Bonitätsprüfungen damit auf eine dritte Instanz übertragen, in diesem Fall die Bank bzw. der Provider. Die Transaktionen können vom

Kunden jederzeit eingesehen werden, denn Firstagte speichert Informationen über «Den Anbieter, von dem Sie kaufen, Beschreibung des Inhalts/Produktes, Preis, Datum, Uhrzeit und Dauer der Zugangsberechtigung.»

So sicher SSL ist, so unsicher ist Sicherung der Zugangsdaten. Denn der Benutzer benötigt lediglich sein Login/Passwort von Firstgate, um eine Transaktion zu bestätigen. Wie bei den anderen Verfahren kann auch diese Information Angriffsziel von Phishing-Attacken werden. Da Click&Buy aber vor allem für kleine Beträge eingesetzt wird und jede Transaktion per Email dokumentiert wird, sind größere Betrugsfälle nicht bekannt, weil es lohnendere Angriffsziele gibt.

4. Email-Systeme

Beispiele: Paypal (E-Bay); Moneybookers
Paypal agiert als alternative Bank vor allem für Einkäufe bei E-Bay, zu der das Unternehmen seit 2002 gehört. Der Kunde kann einen Rechnungsbetrag per Email von seinem Paypal-Konto an das Paypal-Konto des Empfängers senden. In «echtes» Geld umgewandelt wird es per Lastschrift, Prepaid-Guthaben Überweisung oder, vor allem bei internationalen Geschägten, per Kredikarte. Auch hier wird Vertrauen auf bewährte Institute übertragen. Sollte es zu Schwierigkeiten kommen, ist die Transaktion bis zu 500 Euro versichert. Dadurch, das beide Transaktionspartner ein Konto bei Paypal haben müssen, ist eine Online-Bezahlung per Email möglich. Es ist damit deutlich unsicherer als Online-Banking. Dass es aber nicht zum Ziel intensiver Phishing-Attacken geworden ist, verdankt sich dem Umstand, dass mit Paypal vor allem kleine Beträge gehandelt werden, für die sich der Aufwand nicht lohnt. Denn es müssen ja nicht nur Zugangsdaten erschwindelt, sondern auch der Inhaber eines geeigneten Zielkontos gefunden werden, der nach einem erfolgreichen Betrug natürlich nicht mehr zur Verfügung steht. Dieser Aufwand lohnt sich nur bei großen Summen, wie sie bei Online-Banking oder Kreditkartenbezahlungen möglich sind.

5. Mobile Systeme

M-Pay (Vodaphone), T-Pay (Telekom), Allpay (Brunet), Paybox, Moxmo, PayBest, PurePay, StreetCash (Vgl. [Lenz])
Die Deutsche Telekom bietet mit T-Pay ein System, das verschiedene Zahlmodalitäten zulässt. Neben den bereits diskutierten Verfahren der Rückbindung des Zahlungsbetrags an die Kreditkarte oder an die Hausbank gibt es hier auch die Möglichkeit, den Betrag über die Telefonrechnunge abbuchen zu lassen, entweder über die T-Com-Rechnung, wobei der Kunde einen Telefonanschluss der Deutschen Telekom benötigt, oder über eine spezielle Servicenummer auch als Verbindungsentgeld in der Abrechnung anderer Netzanbieter. Das Vertrauen in den Kunden wird bei mobilen Systemen also den Telefonanbietern übertragen, die Datenübertragung per SSL gesichert.
Doch wenn das Handy zum Portemonnaie wird, kann der Verlust eines eingeschalteten Geräts teuer werden. Auch die Variante, nach Eingabe eines Passworts den Betrag von der Telefonrechnung zu buchen, erfordert eine Passwortsicherung auf Kundenseite, die nicht immer gegeben ist. Wie andere Mikropayment-Systeme schützt vor allem die geringe zu erwartende Beute und die Schwierigkeit, Kleinstbezahlungen wieder in Bargeld umzuwandeln, vor systematischen Phishing-Attacken.

6. Elektronisches Bargeld

Web.Cents, iclear(EuroCoin)

Elektronisches Bargeld soll dem normalen Bargeld am Nächsten kommen. Ein Online-Konto oder eine Chipkarte wird mit einer Einzahlung gefüllt und das darauf gespeicherte Geld kann im Folgenden ausgegeben werden. Beispiele sind die Geldkarte oder die Webcents von Web.de. Projekte aus den 90er Jahren wie eCash oder CyberBucks wurden mangels Nachfrage wieder eingestellt. Es scheint, dass die meisten Nutzer einer rein virtuellen Geldbörse zu wenig Vertrauen entgegen bringen. Die Geldkarte hat sich bei Kleinstbeträgen bewährt, kommt für Online-Einkäufe aber nicht in Frage, da der Kunde erst ein zertifiziertes Lesegerät kaufen müsste, wobei die Datenübertragung verstärkt dem Risiko der Fälschung ausgesetzt wäre. Elektronisches Bargeld als anonymes elektronisches Zahlungsmittel bleibt daher auf absehbare Zeit ein ausgearbeitetes Konzept das aber nicht oder nur in sehr überschaubaren Nischen implementiert ist.

Zusammenfassende Betrachtungen

In Bezug auf die oben erwähnten Sicherheitsaspekte fallen drei Dinge auf: 1. Jedes Verfahren misstraut vor allem dem Kunden. Durchgängig wird eine vertrauenswürdige Instanz eingeschaltet, mit denen die Kunden bereits in geschäftlichem Kontakt stehen. Das kann die Bank, ein Kreditkartenunternehmen, ein Telefonanbieter oder der Provider sein über deren Abrechnungssystem die Bezahlung beglichen wird. Lediglich Prepaid-Verfahren können auf derartige Bürgen verzichten.
2. Durch den Einsatz von vertrauenswürdigen Instanzen ist praktisch kein elektronischer Einkauf vollkommen anonym, da zumindest die Mittelsmänner wissen, wer wann wo wieviel bezahlt hat, häufig auch, was gekauft wurde. Angepriesen wird dies als Sicherheit für den Kunden vor Betrug, aber die Erstellung eines detaillierten Kaufprofils ist natürlich nicht für jedermann erstrebenswert.
3. Elektronische Bezahlsysteme sind aus technischer Sicht inzwischen verhältnismäßig sicher sind. Zwar sind Spoofing oder Sniffing ein Problem jedes Netzverkehrs, aber Angriffe gegen die Netzinfrastruktur gehören eher zu den theoretischen Gefährdungen, da sie umfangreichen Zugriff auf Router voraussetzen. Auch gehört der Einsatz kryptografischer Methoden inzwischen zum Standardrepertoire von online-Verkäufern

Die technischen Aspekte werden durch das Gütesiegel «Geprüfter Online-Shop» des EuroHandelsInstituts (EHI) garantiert, darunter:

1. Alle persönlichen Zahlungsinformationen (Kreditkartennummer, Kontodaten,...) sind bei der Übertragung zu verschlüsseln.
2. Die Verschlüsselung anderer Daten (z.B. Bestelldaten) ist optional.
3. Soweit die Zahlungsinformationen im Rahmen des Protokolls SSL verschlüsselt werden, ist eine Schlüssellänge von 1024 Bit für den Schlüsselaustausch und eine starke Kryptographie (z.B. Triple DES) für die Verschlüsselung der Zahlungsinformationen zu verwenden.

http://www.shopinfo.net/sicherheitsstandards.shtml

Da Online-Händler zunehmend diesen technischen Anforderungen genügen, werden Angriffe gegen technische Infrastrukturen immer schwieriger und sind für Kleinkriminelle kaum mehr praktikabel. Die Alternative ist das Abfangen sensibler Daten auf dem Rechner des Opfers durch Trojaner und Hintertüren. Hier könnten Virenscanner und Firewalls schützen. Doch selbst diese Schutzwälle sind umgehbar, denn bekanntlich sind zwei Dinge unendlich: das Universum und die menschliche Dummheit (wobei Einstein, der Autor dieses Satzes, beim Universum noch Unsicherheiten einräumte). Also spezialisieren Betrüger sich inzwischen auf die Gutgläubigkeit ihrer Opfer. Da werden Email-Anhänge ungeprüft geöffnet, PINs und TANs auf dubiosen Webseiten eingetragen, Kreditkartennummern am Telefon offenbart oder Kontoinformationen an obskure Adressen verschickt. Hier hilft nicht mehr Technik, sondern Aufklärung und Sensibilisierung.
Denn alle Probleme des offline-Bezahlens sind auch online zu finden, vom Betrug über Diebstahl bis zum Falschgeld. Hinzu kommen alle anderen Straftatbestände, die im Zusammenhang mit Geld verübt werden: Raub, Erpressung, Geldwäsche und Hehlerei. Die meisten dieser Probleme sind allerdings nicht technischer sondern sozialer Natur. Gerade hier müssen die Nutzer über drohende Gefahren aufmerksam gemacht werden, damit sie sich nicht blind auf Sicherheitsversprechungen der Anbieter verlassen. Nun könnte man die Erziehung zur Verbrechensprävention, wie bei offline-Kriminalität auch, dem Elternhaus überlassen. Da wir am Übergang zur Informationsgesellschaft aber mit der historisch einzigartigen Situation konfrontiert sind, dass die Kinder besser informiert ist als ihre Eltern, kann man sich beim Thema Computer- und Onlinesicherheit nicht auf diese verlassen. Vielmehr kann man davon ausgehen, dass, was die Kinder nicht wissen, die Eltern erst recht nicht verstehen. Unterrichtseinheiten zum Thema Sicherheit gehören daher in den Schulunterricht, wenn Schule ihren Bildungsauftrag erfüllen und Schülerinnen und Schüler auf ein Leben in der Informationsgesellschaft vorbereiten möchte.

Quellen

Franke, Dirk (2005): *Kreditkarten. Mehr als nur Zahlungsmittel.*
http://www.die-bank.de/media/042005/0504-thema.pdf

IWW, Institut für Wirtschaftspolitik und Wirtschaftsforschung: *Informationen und Hintergründe.*
http://www.iww.uni-karlsruhe.de/reddot/894.php

KompEC, Kompetenzzentrum Elektronischer Geschäftsverkehr Bonn/Rhein-Sieg (Hg.) (2001): *E-Payment im Internet für kleine und mittlere Unternehmen.*
http://www.leischner.inf.fh-bonn-rhein-sieg.de/PDF/ePayment.pdf

Krüger, Matte et al. (2006): *Internet Zahlungssysteme aus der Sicht der Verbraucher.*
http://www.iww.uni-karlsruhe.de/reddot/download/izv8_internet_version.pdf

Lenz, Harald: *M-Payment, Zahlungsmethoden im MCommerce.*Wien 2004

Markmann, Monika *Elektronischer Zahlungsverkehr.*
http://www.lehrer-online.de/url/e-payment