Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 94 (2003)
Heft: 20

Artikel: Sicherheitsaspekte bei Electronic Commerce
Autor: [s.n.]
DOI: https://doi.org/10.5169/seals-857604

Sicherheitsaspekte bei Electronic Commerce

Electronic Commerce – oder kurz E-Commerce – ist in den letzten Jahren zu einem wichtigen wirtschaftlichen Faktor geworden. Der Beitrag informiert darüber, was Electronic Commerce ist, welche Sicherheitsprobleme damit verbunden sind und welche Möglichkeiten es gibt, diesen entgegenzutreten.

Die Informationstechnik stellt die Weichen für unsere gesellschaftliche und wirtschaftliche Entwicklung: Informationstechnik sichern und gegen Gefahren von innen und aussen steuern (Bild Siemens).

Quelle/Kontaktadresse
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
D-53175 Bonn
E-Mail: bsi@bsi.bund.de

BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit «Electronic Commerce»

Handelsgeschäfte, die elektronisch abgewickelt werden

Mit «Elektronischem Handel» oder «Electronic Commerce» sind alle Handelsgeschäfte gemeint, bei denen einer oder mehrere der folgenden Schritte elektronisch abgewickelt werden (Bild 1):

- Werbung, Angebotspräsentation
- Auswahl
- Bestellung
- Bezahlung
- Auslieferung
- Benutzung

Bereits seit längerem existierende Formen des «Elektronischen Handels» sind zum Beispiel EDI (Electronic Data Interchange) bei Business-to-Business-Transaktionen oder EFTPOS (Electronic Funds Transfer at the Point-of-Sale), beim elektronischen, bargeldlosen Bezahlen am Kaufort.

Im Gegensatz zu diesen Formen des elektronischen Handels wird unter E-Commerce heute hauptsächlich die Durchführung der einzelnen Transaktionsschritte über das Internet verstanden. Die Bezeichnung «Electronic Commerce» ist jedoch überzogen, wenn nur einzelne Transaktionsschritte, zum Beispiel die Angebotspräsentation, über das Internet angeboten werden, Bestellung und Bezahlung aber nur per Fax, Telefon oder andere «klassische» Wege möglich sind. Einer der wichtigsten Aspekte beim E-Commerce ist die Möglichkeit, sicher über das – offene und ungesicherte – Internet bezahlen zu können (Bild 2).

So bieten zwar immer mehr Händler ihre Waren über das Internet an, die Online-Bezahlung ist für den Kunden aber nach wie vor oft ein Problem. Es gibt zwar diverse Verfahren für Internet-Zahlungen, wovon die meisten auch sehr sicher sind, aber viele befinden sich noch im Stadium von Pilotversuchen oder leiden unter mangelnder Akzeptanz. Bis sich die ersten Verfahren «internet-weit» etabliert haben, wird es noch eine Weile dauern. Händler bieten deshalb Übergangslösungen für die Online-Bezahlung an. Die sind jedoch weniger sicher als die speziell für E-Commerce entwickelten Verfahren.

Gefährdungsbereiche beim Electronic Commerce

Eines der entscheidenden Merkmale für E-Commerce ist die Benutzung des Internets. Die Hauptprobleme lassen sich in drei Bereiche unterteilen:

- **Kommunikation**: In offenen Netzen kann die Kommunikation über viele Knotenpunkte gehen. Der Benutzer weiss meist nicht, wie gut die Nachrichten von anderen Systemen oder Netzbetreibern geschützt werden, wer alles die Möglichkeit hat, die Kommunikation mitzulesen oder zu

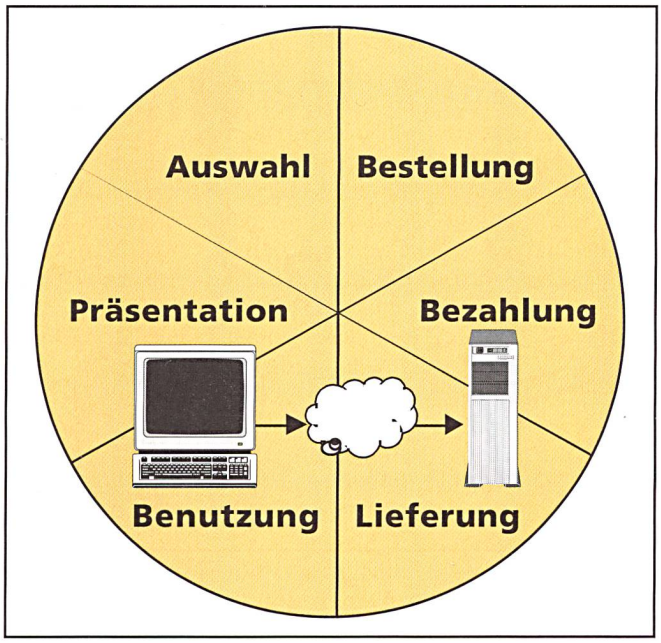

Bild 1 Handelsgeschäfte des «Electronic Commerce».

manipulieren. Es kann oft nicht einmal vorhergesagt werden, welchen Weg eine Nachricht nimmt: Eine E-Mail von Köln nach Bonn wird unter Umständen über die USA weitergeleitet.

- **Komponentensicherheit**: Alle Komponenten, die ans Internet angeschlossen werden – sei es ein Benutzer-PC oder ein Händler-Server – müssen adäquat gegen mögliche Angriffe über diese Verbindung geschützt werden, auch gegen einen Angriff vor Ort. Untersuchungen zeigen dabei immer wieder, dass nicht, wie zumeist angenommen, Hacker die grösste Gefahr für die Daten eines Unternehmens sind, sondern Innentäter. Die Motive dafür sind unterschiedlich: angefangen von Unachtsamkeit über mangelnde Erfahrung bis hin zu vorsätzlichen Manipulationen aus Frust oder zur persönlichen Bereicherung.
- **Identitätsfeststellung**: Ein weiterer Sicherheitsaspekt von E-Commerce-Systemen ist die eindeutige Feststellung der Identität der Kommunikationspartner. Woher weiss ich überhaupt, wer mein Gegenüber ist (Bild 3)? In offenen Netzen wie dem Internet kann man sich nicht darauf verlassen, dass Namensangaben korrekt sind. Unter www.xy-bank.com findet sich nicht unbedingt die XY-Bank, ebenso sind Absenderangaben bei E-Mails leicht zu fälschen. Daher müssen hier zusätzliche Massnahmen zur gegenseitigen Identifikation und Authentikation ergriffen werden.

Wie viel Sicherheit ist erforderlich?

Ausgehend von diesen drei Bereichen lassen sich eine Vielzahl von Gefährdungen identifizieren. Dazu zählen zum Beispiel das Herunterladen von Computerviren oder unkontrollierter Software aus dem Internet, Systemausfälle durch Denial-of-Service-Angriffe oder unbefugter Zugriff auf interne Informationen. Um diesen Risiken entgegenzuwirken, muss überlegt werden: Was kann passieren? Was soll dagegen unternommen werden? Dabei muss sehr genau geplant werden, welche Sicherheitsmassnahmen in welchem Umfang (und bis zu welcher finanziellen Obergrenze) umgesetzt werden sollen. Sicherheitsmassnahmen können billig, trivial oder allgemein anerkannter Mindeststandard, aber auch sehr teuer und aufwändig sein. Wichtig ist vor allem, dass sie auf das jeweilige Umfeld angepasst sein sollten.

Generell sind viele Gefährdungen und damit die resultierenden Sicherheitsmassnahmen von der Grösse, der Art und dem Ruf der Unternehmen, die Electronic Commerce betreiben, abhängig. Ein kleines oder mittleres Unternehmen, das typischerweise Standardsoftware für die Internetpräsentation einsetzt, hat andere Probleme als eine grosse Organisation, die selbst- oder weiterentwickelte Software verwendet. Treten Sicherheitslücken bei Standardsoftware auf, wird dies schnell publik. Mit Standardsoftware ausgestattete Server können daher sehr schnell Opfer eines Angriffs werden. Proprietäre Software enthält statistisch zwar genauso viele Fehler, allerdings muss ein Angreifer diese zunächst selbst identifizieren. Angriffe auf Server mit proprietärer Software sind daher anders motiviert, zum Beispiel vom Wert der dort vermuteten Informationen oder vom Renommee, das durch einen erfolgreichen Angriff zu gewinnen ist.

Welcher Handlungsbedarf sich aus den vielfältigen Bedrohungen für ein spezielles Electronic-Money- oder Electronic-Commerce-System ableitet, hängt davon ab,

- für wie wahrscheinlich der Eintritt gehalten wird,
- welche Schäden dadurch verursacht werden können,
- wie aufwändig die Durchführung eines entsprechenden Angriffs ist,
- wie hoch das Entdeckungsrisiko für einen Angreifer ist.

Der erforderliche Sicherheitsgrad wird nicht zuletzt von den ökonomischen Rahmenbedingungen beeinflusst. Wie viel Sicherheit angemessen ist und welche Sicherheitsmassnahmen dafür umgesetzt werden müssen, richtet sich unter anderem nach der Höhe der Zahlungsbeträge, den angebotenen Warenarten und den vorhandenen Kenntnissen über die Kun-

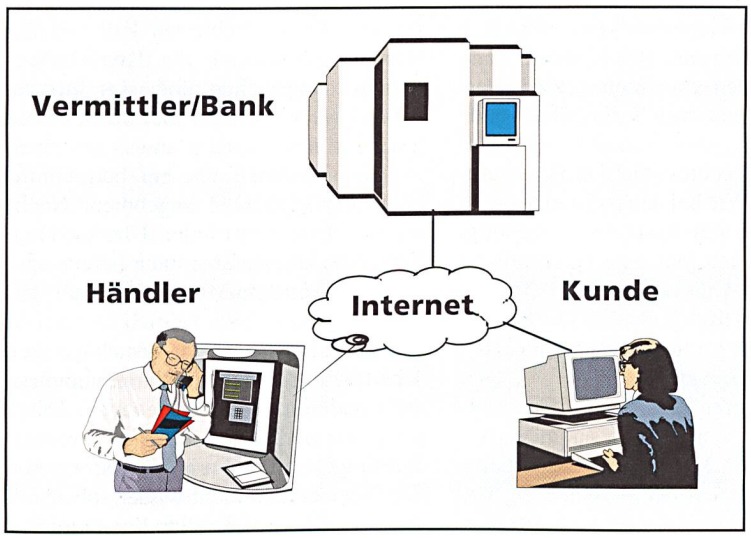

Bild 2 Immer mehr Händler bieten ihre Ware über das Internet an.

den. Das angestrebte Sicherheitsniveau ist immer auch eine Frage der Kosten-/Nutzen-Relation, also der Bezahlbarkeit der daraus resultierenden Massnahmen.

Es darf dabei nicht vergessen werden, dass es eine hundertprozentige Sicherheit im E-Commerce nicht gibt: Auch bei bestmöglichen Sicherheitsmassnahmen wird es immer Restrisiken geben, ebenso wie es auch immer Ladendiebe geben wird, solange Kunden ein Geschäft betreten dürfen. Daher sollten Notfallpläne für alle derzeit bekannten und vorstellbaren zukünftigen Bedrohungen erstellt werden. Im Falle eines Angriffs kann das betroffene Unternehmen eine Krise damit leichter abwenden.

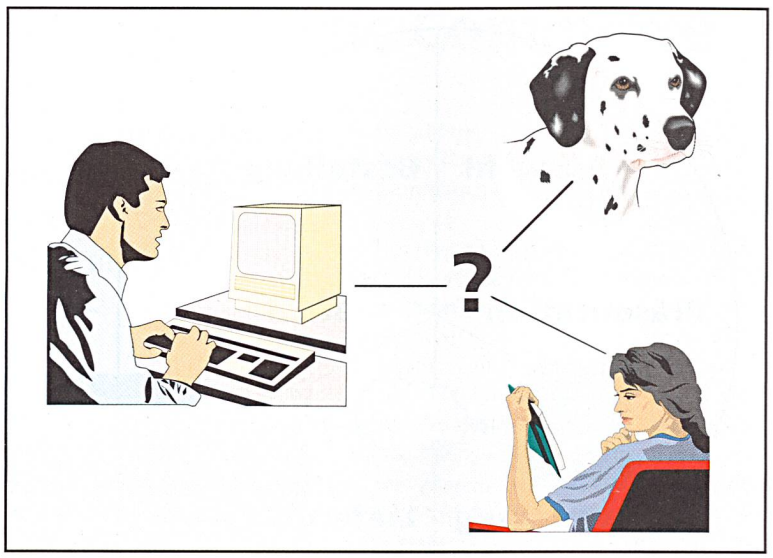

Bild 3 «Im Internet weiss niemand, dass du ein Hund bist.»

Electronic-Money-Verfahren

Parallel zur rasanten Entwicklung des Internet wurde eine Vielzahl von Online-Zahlungssystemen entwickelt. Davon sind die meisten allerdings bereits wieder verschwunden. Zu den bekanntesten gehören SET, ecash, CyberCash, Millicent und First Virtual.

First Virtual bot eine interessante Variante für ein elektronisches Zahlungssystem an. Das Verfahren ist allerdings nach anfänglich beachtlichen Erfolgen im Juli 1998 eingestellt worden. Das System arbeitete völlig kryptographiefrei. Die Kunden benötigten ausserdem keinerlei spezielle Soft- oder Hardware, um daran teilnehmen zu können. Zudem räumte First Virtual den Kunden ein «Rückgaberecht» ein. Nach der Einstellung wurde den Kunden die Übernahme des CyberCash-Verfahrens empfohlen.

ecash ist eines der wenigen Electronic-Money-Verfahren, bei dem versucht wurde, die Eigenschaften von Münzgeldzahlungen nachzuahmen. Das System ist eng verwandt mit dem ebenfalls von David Chaum konzipierten Chipkarten-Zahlungssystem CAFE. In Deutschland wurde das ecash-Verfahren von der Deutschen Bank angeboten, im Jahr 2001 jedoch wieder eingestellt. Bei ecash werden digitale Geldmünzen über das Internet ausgetauscht. Dazu erhält ein Kunde ähnlich wie bei elektronischen Geldbörsen oder Wertkarten gegen Vorkasse «elektronische Münzen», mit denen er im Internet anschliessend Waren kaufen kann. Für diese Münzen wird ein Konto bei einer digitalen Bank angelegt, bei der der Kunde seine «elektronischen Münzen» abheben und einzahlen kann. Für den Umgang mit ecash bekommt der Kunde die entsprechende Software zur Verfügung gestellt, um Geld zu speichern und auszugeben.

Ein weiteres Online-Zahlungssystem ist CyberCash. Unter diesem Oberbegriff werden im Wesentlichen drei verschiedene elektronische Zahlungssysteme zusammengefasst:

- ein kreditkartenbasiertes System, bei dem die Weitergabe der Kreditkarteninformationen durch Verschlüsselung abgesichert ist. Hierfür wird das SET-Protokoll verwendet.
- ein lastschriftbasiertes Zahlungssystem, bei dem der Kunde eine schriftliche Einzugsermächtigung an die CyberCash GmbH erteilt und dann bei CyberCash-Vertragshändlern einkaufen kann.
- CyberCoin als Prepaid-Zahlungssystem für Kleingeldzahlungen.

CyberCash-Dienstleistungen wurden in Deutschland unter anderem von der Dresdner Bank und von der Commerzbank angeboten. Ende 2000 hat die CyberCash GmbH die gleichnamige virtuelle Währung wegen mangelndem Kundeninteresse eingestellt.

Ein Verfahren, das speziell für die Zahlung von Kleinstbeträgen entwickelt wurde, ist Millicent. Bei Millicent kann mit Bruchteilen von Cents gezahlt werden, mit so genannten Scrips. Der Kunde muss sich an einen Vermittler (Broker) wenden, um «echtes» Geld in Scrips umzutauschen. Wie bei den meisten anderen Electronic-Money-Systemen benötigt der Kunde auch hier eine elektronische Geldbörse («Wallet») als Plug-In für seinen Browser, in die die Scrips geladen werden. Auch Millicent hat sich nicht am Markt etablieren können.

Das Verfahren SET (Secure Electronic Transaction) wurde in Zusammenarbeit von VISA und Mastercard ausgearbeitet und dient speziell der Absicherung von Kreditkartentransaktionen über unsichere Netze wie das Internet. Bei SET werden sowohl symmetrische als auch asymmetrische kryptographische Verfahren ebenso wie Hashverfahren eingesetzt, um die übertragenen Informationen abzusichern. Bei der Verwendung von SET wird ausserdem einer Maskerade der Kommunikationspartner vorgebeugt. Ein Kunde kann nur über SET zahlen, wenn er eine gültige Kreditkarte besitzt; ein Händler, der SET-Zahlungen entgegennimmt, muss als Akzeptanzstelle zugelassen sein. Unter der Bezeichnung «Verified by Visa» bietet VISA seit kurzem ein Nachfolgesystem von SET an. Es kommt ohne zusätzliche Software auf den PCs der Karteninhaber aus und verwendet Passwörter als Sicherheitsmechanismen.

Entwicklungstrends bei elektronischen Zahlungsverfahren

Viele Internet-Händler, insbesondere ausländische, bieten zwar interessante und preisgünstige Waren an, sehen aber häufig als Zahlungsmittel nur Kreditkarten vor. Im schlechtesten Fall soll die Bestellung inklusive der Kreditkartennummer ungesichert über das Internet weitergegeben werden. Bei inländischen Transaktionen werden meist dieselben Zahlungsvarianten wie im herkömmlichen Versandhandel angeboten: Nachnahme, Lastschrift oder Überweisung. Teilweise können aber auch bereits spezielle Electronic-Money-Systeme benutzt werden.

Das BSI rät von der unverschlüsselten Übertragung von Kreditkartennummern oder anderen zahlungsrelevanten Daten ab. Denn die Daten können im Zweifelsfall mitgelesen und missbraucht werden. Der Kunde kann nicht wissen, ob er mit einem «echten» Händler kommuniziert

oder mit einem Betrüger, der auf diese Weise Kreditkartennummern sammelt (Bild 3). Das grösste Risiko bei der Akzeptanz von Kreditkarten bei Internet-Bestellungen liegt aber auf der Seite des Händlers. Für Händler gelten hierbei dieselben Rahmenbedingungen wie für andere Kreditkartenzahlungen, bei denen der Kunde keine Unterschrift leisten muss. Wenn der Kunde die Bestellung bestreitet, die Zahlung widerruft oder gar kein Kunde zur Kreditkartennummer existiert, trägt der Händler das alleinige Risiko.

Um diesen Sicherheitsproblemen entgegenzutreten, sollten die Bezahlinformationen angemessen geschützt werden. Dies kann beispielsweise mit dem bereits beschriebenen SET-Verfahren oder mit Hilfe von SSL erfolgen. Das setzt jedoch einen ordnungsgemässen und sicherheitsbewussten Umgang mit diesen Technologien voraus.

SSL ist bereits in vielen Browsern integriert und kann zum Schutz der Vertraulichkeit beziehungsweise Integrität übertragener Informationen wie Kreditkartennummern benutzt werden. Dabei sollten allerdings einige Punkte beachtet werden:

Aufgrund der US-Exportrestriktionen für Verschlüsselungsverfahren waren in früheren Browser-Versionen häufig nur Verfahren mit sehr kurzen Schlüssellängen (40 Bit) integriert. Mittlerweile sind diese Exportrestriktionen zwar weitgehend aufgehoben, einige im Betrieb befindliche Produkte arbeiten aber immer noch mit zu kurzen Schlüssellängen. Diese halten Brute-Force-Angriffen, das heisst einfachen Angriffen durch Ausprobieren, nicht lange stand. In vielen Fällen reichen die Schlüssellängen zwar aus, bei der Übertragung von Finanztransaktionen sollte aber mit längeren Schlüsseln gearbeitet werden. Deshalb ist es ratsam, eine Browser-Version zu verwenden, die ausreichend lange Schlüssel (128 Bit) unterstützt.

SSL schützt allerdings nicht vor anderen Sicherheitsproblemen: So können die Kommunikationspartner zwar davon ausgehen, dass die empfangenen Informationen integer sind, aber nicht davon, dass sie auch echt sind. Beispielsweise kann ein Händler nicht sicher sein, ob die übermittelte Kreditkartennummer gültig ist. Die Verwendung dieser Verfahren sagt auch nichts darüber aus, wie die empfangenen Informationen weiterverarbeitet werden, also ob zum Beispiel Kundenprofile erstellt werden oder ob die Informationen vor unbefugtem Zugriff gesichert gespeichert werden.

Daher sollten alle E-Commerce-Teilnehmer, egal ob Kunde oder Händler, darauf drängen, dass speziell dafür entwickelte Zahlungsverfahren angeboten beziehungsweise eingesetzt werden. Nur diese bieten eine für alle Teilnehmer akzeptable Sicherheit.

Langfristig wird der Trend zu einem höheren Sicherheitsniveau gehen. So macht es das Nutzer- und Nutzungsverhalten im Internet erforderlich, dass neben der Kommunikation auch die Rechner der Anbieter und Kunden abgesichert werden. Die Kunden benötigen dazu sichere und geprüfte Komponenten. Hierbei geht die Entwicklung in Richtung Chipkarten als sichere und transportable Medien zur Speicherung und Verarbeitung von Zugangsberechtigungen und kryptographischen Schlüsseln. Dazu müssen sich aber einige Verfahren am Markt durchsetzen und die entsprechende Verbreitung finden.

Wie können sich Kunden absichern?

Die Nutzer von Internet-Dienstleistungen können bestehende Risiken minimieren, wenn sie einige Verhaltensregeln beachten. Das sichere Einkaufen über das Internet erfordert die Umsetzung folgender Massnahmen:

- **Beachtung der Sicherheitsempfehlungen**: Beachten Sie die vom Internet-Dienstleister bereitgestellten Informationen und Sicherheitsempfehlungen. Sind diese nicht aussagekräftig genug, fordern Sie die erforderlichen Informationen ein.
- **Datensicherung**: Erstellen Sie besonders von den finanzrelevanten Daten regelmässig eine Datensicherung. Damit bleiben die Daten selbst bei technischen Defekten oder anderweitigen Schäden erhalten.
- **Schutz vor Computer-Viren**: Schützen Sie den für die Internet-Transaktionen genutzten Rechner vor Computerviren, Trojanischen Pferden oder dubioser Software. Das BSI empfiehlt die Installation von aktuellen Virenschutzprogrammen und Personal Firewalls.
- **Sichere Aufbewahrung von Zugangsmitteln**: Bewahren Sie Zugangsmittel wie Passwörter, PINs, TANs oder Chipkarten sicher auf und speichern Sie sie nach Möglichkeit nicht im IT-System ab. Die ausserhalb der elektronischen Systeme dokumentierten Zugangsdaten sollten verschlossen aufbewahrt werden.
- **Auf Verschlüsselung achten**: Zum Schutz der eigenen Daten können Internet-Dienstleister eine Vielzahl von Verfahren anbieten. Achten Sie darauf, dass Ihre Daten bei der Übertragung über das Internet verschlüsselt werden! Häufig wird dafür das in jedem WWW-Browser integrierte TLS/SSL-Protokoll verwendet. Dabei werden Vertraulichkeit und Integrität der Daten mit Hilfe kryptographischer Verfahren geschützt. Eine TLS/SSL-Verbindung erkennt man im Browser daran, dass die Adresse (URL) mit https: statt mit http: beginnt, und bei den gängigen Browsern auch an einem besonderen Symbol, zum Beispiel einem geschlossenen Schloss.
- **Verzicht auf aktive Inhalte**: Kunden sollten immer die Möglichkeit haben, Techniken oder Methoden auszuschliessen, die Sicherheitsprobleme mit sich bringen können. Dazu gehören aktive Inhalte wie JavaScript oder ActiveX. Aktivieren Sie diese in Ihrem WWW-Browser nur dann, wenn Sie sich auf vertrauenswürdigen Webseiten befinden. Da dies für Kunden kaum nachvollziehbar ist, sollten sicherheitsbewusste Anbieter immer auch einen zweiten Weg anbieten. Ein kurzes Beispiel: Viele animierte Demonstrationen auf Webseiten verlangen aktive Inhalte wie JavaScript. Als Kunde sollten Sie darauf hin gewiesen werden, dass für eine Demonstration JavaScript im Browser eingeschaltet sein muss, aber diese auch ohne JavaScript als einfache Bilderfolge betrachtet werden kann.

Literatur

BSI-Schriftenreihe zur IT-Sicherheit im Bundesanzeiger Verlag. Internet: www.bundesanzeiger.de/E-Mail: vertrieb@bundesanzeiger.de

Aspects de la sécurité relatifs au commerce électronique

Au cours des dernières années, le commerce électronique – ou E-Commerce – est devenu un facteur économique important. L'article définit le commerce électronique, informe sur les problèmes qui peuvent survenir au niveau de la sécurité et sur les possibilités de les combattre.