Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 81 (2003)

Heft: 1

Artikel: Sicherheit : Bremse oder Schrittmacher?

Autor: Eckert, Claudia

DOI: https://doi.org/10.5169/seals-876604

Sicherheit – Bremse oder Schrittmacher?

Lockheed Martin

«Skynet 5 Artist» von Lockheed Martin: Kommunikationssatelliten erweitern die globale Vernetzung, bedingen damit aber auch globale Sicherheitssysteme.

In unseren normalen Lebensgewohnheiten haben wir Schutzvorkehrungen getroffen, um uns vor Gefahren wie Unfällen, Diebstahl oder das Eindringen in unsere Privatsphäre zu schützen. Die Existenz dieser Vorkehrungen nehmen wir aber kaum noch bewusst wahr. Das sichere Haus, das sichere Fahrzeug, die vertrauenswürdigen Instanzen wie beispielsweise die Verwaltung, der Notar oder die Bank gehören selbstverständlich zu unserem Alltag. Welchen Einfluss hat nun die Informations- und Kommunikationstechnologie auf diese Situation?

Der Beitrag beleuchtet die Bedeutung der IT-Sicherheit in unserer heutigen Informations- und Wissensgesellschaft. Er geht ferner darauf ein, welchen Stellenwert die IT-Sicherheit als Wirtschaftsfaktor und als Enabeling-

CLAUDIA ECKERT

Technologie für neue Anwendungsfelder wie das E-Business besitzt. Es werden die wichtigsten Problemfelder angesprochen und aktuelle Forschungs- und Entwicklungsprojekte vorgestellt. Der Beitrag soll verdeutlichen, dass die Sicherheitstechnologie nicht als ein Hemmnis und eine Bremse, sondern vielmehr als ein Schrittmacher für innovative Anwendungen zu betrachten und zu bewerten ist.

Gefährlicher Fortschritt?

Durch die Fortschritte in der Informations- und Kommunikationstechnologie sind bereits heute rund 70 bis 80% der Menschen direkt oder indirekt von der Informationstechnik abhängig. Wir produzieren und verarbeiten Informationen zu wertvollem Wissen, um dieses sowohl privat als auch geschäftlich zu nutzen. Solange wir unser Wissen auf Papier und in unseren Köpfen herumtragen konnten, war es (fast) so sicher und unter unserer Kontrolle wie ein materielles Gut. Das hat sich mit der Vernetzung und der Verfügbarkeit des weltweiten Wissens gravierend verändert. Unser Wissen und unser Umgang mit Wissen hat neue Begehrlichkeiten geweckt und die vermeintliche Sicherheit massiv verändert. Wir sind nicht nur physisch mobiler geworden, sondern auch Informationen und das Wissen werden zunehmend mobil, über Datennetze ausgetauscht, gemeinsam genutzt und bearbeitet. Wir haben nahezu zu jeder Zeit und an jedem Ort Zugang und Zugriff zu Informationen, ebenso können wir unsere Kommunikationsbedürfnisse jederzeit und ortsunabhängig erfüllen. Das ist angenehm, aber auch gefährlich. Wir sind

nicht sicher, ob unsere Information unverfälscht den Empfänger erreicht und dass nur der berechtigte Empfänger in den Besitz dieses Wissens gelangt. Unser Zugriffs- und Nutzungsverhalten ist beobachtbar, wodurch sich Angriffsmöglichkeiten für diejenigen bieten, die uns schaden wollen.

Sicherheit als Wirtschaftsfaktor

Innovationen entstehen durch Kreativität in einem weit gehend nicht reglementierten Umfeld, sodass sich die Frage erhebt, ob wir dies weiterhin so aufrechterhalten können, da wir ja unser wertvolles Wissen auch vor unerlaubtem Zugriff und vor Manipulationen schützen möchten. Unser eigentliches Problem in der schutzbedürftigen Wissensgesellschaft ist die weit verbreitete Unwissenheit über bestehende Risiken und Gefahren bzw. deren Ignoranz. Wir stehen vor der Aufgabe, unsere IT-Sicherheitstechnologien so selbstverständlich in unsere elektronischen Arbeitsabläufe und Freizeitaktivitäten zu integrieren, wie beispielsweise Sicherheitsgurte und Airbags in unsere heutigen Fahrzeuge. Zur Lösung dieser komplexen Aufgabe arbeitet das Fraunhofer Institut für Sichere Telekooperation [7] interdisziplinär mit Juristen, Arbeitswissenschaftlern und Anwendern zusammen.

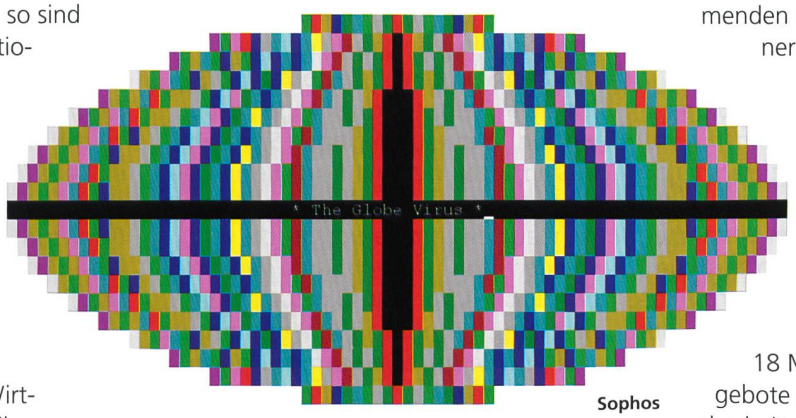
Fehlende Sicherheit als Hemmnis

Fehlt ausreichende Sicherheit, so sind einzelne Menschen, Organisationen und die Gesellschaft insgesamt inakzeptablen Risiken ausgesetzt. Dies wirkt sich zweifach als Wirtschaftsfaktor aus. Zum einen dadurch, dass sich die Risiken manifestieren und zu Schadensfällen werden. Zum anderen dadurch, dass – auch wenn nichts passiert – es nicht zu Wirtschaftsaktivitäten kommt, weil das Vertrauen fehlt. So wurden gemäss Umfrageergebnissen von den Befragten folgende Faktoren als die grössten Hindernisse im Electronic Commerce genannt:

- Regulatorische Defizite, Rechtssicherheit rund 70%
- Unsicherheiten bei Haftung und Copyright rund 65%
- Fehlender Datenschutz rund 60%
- Unsichere Zahlungsmöglichkeiten rund 60%
- Vertrauensprobleme mit Kooperationspartnern rund 60%
- Fehlende Integrität bei Datenübertragung rund 55%

Dass eine datenschutzgerechte, sichere Lösung für das sichere Einkaufen über das Internet möglich und effizient umsetzbar ist, hat beispielsweise das DASIT-Projekt [2] gezeigt.

Auch Unternehmen müssen Vertrauen in das Internet haben, um ihre Produkte und Dienstleistungen über das Internet anzubieten, Verträge abzuschliessen und abzuwickeln. Wird ihnen keine ausreichende Sicherheit geboten, werden sie vor weiteren Schritten hin zur digitalen Ökonomie und zur Internetökonomie zurückschrecken. Durch das Fehlen von Sicherheitsmassnahmen bleiben aber nicht nur neue Möglichkeiten verschlossen. Mehr noch sind heutige Unternehmen und Organisationen mit dem erreichten Stand der Vernetzung bereits so von der Informations- und Kommunikationstechnik abhängig, dass sie ohne diese ihren Betrieb nicht mehr aufrechterhalten können. Während früher Täter an den Angriffsort gehen mussten, genügen für die Angriffe über das Netz PC und Modem. Der Angriff kann vom heimischen Sessel aus in sicherer Entfernung und zeitlichem Abstand erfolgen. Dies lässt die Hemmschwellen deutlich sinken.



Sicherheitslösungen müssen so gestaltet sein, dass sie zu einer Verringerung des Schadenpotenzials führen.

Verletzliche Informationsgesellschaft

Viren, Würmer oder auch Trojanische Pferde [1] können die Informations- und Kommunikationsinfrastruktur eines Unternehmens so zerstören, dass sie zusammenbricht. Dies verursacht nicht nur betriebswirtschaftliche Risiken und gefährdet die Geschäftszwecke, das Kapital und die Arbeitsplätze eines Unternehmens, sondern auch die gesamte Volkswirtschaft. So verursachte beispielsweise der «I love you»-Virus einen weltweiten Schaden von etwa 20 Mia. US-$ durch den Ausfall von Rechnern, zerstörte Dateien und Reparaturmassnahmen. Im Jahr 2000 wurde mit 16 000 gemeldeten Hackerangriffen gerechnet. Die Dunkelziffer ist jedoch um ein Vielfaches höher. Elektronisch vermittelte Informationen sind oder werden zu einem entscheidenden Produktionsfaktor der Volkswirtschaft. Vor allem gilt dies für die Infrastrukturen, auf die unsere Gesellschaft angewiesen ist. Diese müssen als kritisch gelten, wenn eine Einschränkung ihrer Funktionsfähigkeit dazu führen kann, dass wichtige Aufgaben nicht mehr wahrgenommen werden können. Hierzu zählen etwa die Energie- und Wasserversorgung, der Güter- und Personenverkehr, die Gesundheitsversorgung und natürlich die Kommunikationsinfrastruktur. Die volkswirtschaftlichen Schäden, die aus einer solchen Abhängigkeit erwachsen, können gewaltig sein. So werden allein die Kosten für die weltweiten Anstrengungen, die über zwei bis drei Jahre hinweg zur Behebung des Jahr-2000-Problems unternommen wurden, auf 1000 Mia. US-$ geschätzt.

IT-Sicherheits-Lösungen

Die geschilderte Situation unzureichender Sicherheit tritt auf Grund der zunehmenden Anzahl publik gewordener Angriffe verstärkt ins Bewusstsein. Dadurch entsteht eine Nachfrage nach Sicherheit. IT-Sicherheit hat sich zu einem beachtlichen Markt entwickelt: Weltweit werden mit diesem Wirtschaftsgut über 18 Mia. US-$ umgesetzt. Angebote für die Unternehmenssicherheit sind das Hauptbetätigungsfeld der Sicherheitsindustrie. Dazu zählen Sicherheitsangebote für den Schutz der Unternehmen gegen Angriffe von aussen, aber auch von innen wie Firewalls, Zugangs- und Zugriffsschutz und vor allem auch der Virenschutz. Lösungen zum Selbstschutz des Nutzers sind dagegen noch selten und werden nur zögerlich angenommen. Auf Grund der Globalität des Internets kann sich ein Bürger aber nicht mehr auf den Schutz


Siemens

Ein Sicherheitssystem muss einwandfrei funktionieren und wird gründlich getestet; hier in Bezug auf die elektromagnetische Verträglichkeit.

durch seinen Staat verlassen. Er ist darauf angewiesen, sich selbst zu schützen und bedarf für diesen Selbstschutz technischer Unterstützung.
Noch nicht als Markt erkannt wurden bisher die Konzepte, Dienstleistungen und Technologien, die es ermöglichen, die Verletzlichkeit der Informationsgesellschaft zu reduzieren. Bisher wurden noch keine geeigneten Sicherheitsinfrastrukturen aufgebaut, die den elektronischen Handel absichern könnten.
Ebenso wie Qualität als ganzheitlicher Unternehmensprozess verstanden wird, wird das Thema Sicherheit zunehmend als «Corporate Security» verstanden. Die IT-Sicherheit ist ein wichtiger Bestandteil zur Unterstützung dieses ganzheitlichen Prozesses. Zu jeder Unternehmensstrategie gehört zukünftig ein Sicherheits- und ein Qualitätshandbuch, dessen Regeln dynamisch den Unternehmenszielen angepasst und allen Mitarbeitern vermittelt werden müssen. Ebenso gehört dazu eine regelmässige Sicherheitsüberprüfung mit anschliessender Aktualisierung der Unternehmensprozesse und der organisatorischen und technischen Implementierung.

Sicherheitsforschung als Innovations-Schrittmacher

Wenn Forschung beitragen kann, Sicherheit für die Wirtschaft zu gewährleisten, ist sie ein Schrittmacher für wirtschaftliche Tätigkeit. Sicherheit ist ein Schlüsselfaktor für die Internetökonomie.

Anforderungen

Wesentlich dafür ist, dass die erforderlichen technischen Werkzeuge möglichst nahtlos und einfach nutzbar in Anwendungssysteme integriert werden. Nicht technische Brillanz an sich, sondern der Anwendernutzen ist gefragt. Das ist derzeit beispielsweise das Hauptproblem mit digitalen Signaturen, die noch zu sehr allein als Sicherheitstechnik angeboten werden. Wozu sollen digitale Signaturen nutzen, wenn man mit ihnen keinen relevanten Vertrag abschliessen und sie nicht als Beweismittel vor Gericht verwenden kann? Daher müssen Verfahren der digitalen Signatur so gestaltet sein, dass ihre Ergebnisse als Schriftformersatz und als belastbare Beweismittel in Behördenverfahren und Gerichtsprozessen genutzt werden können. Analoges gilt auch für andere Sicherheitstechnologien. Sicherheitslösungen müssen so gestaltet sein, dass sie zu einer Verringerung des Schadenpotenzials und damit der Verletzlichkeit führen und eine autonome Sicherheitseinschätzung und -entscheidung der Nutzer ermöglichen.

Aktuelle Forschungs- und Entwicklungsarbeiten

Anwendungen in allen Bereichen der Informations- und Wissensgesellschaft erfordern skalierbare Lösungen zur IT-Sicherheit. Vertraulichkeit, Vertrauenswürdigkeit und Verlässlichkeit von Informationen, Schutz vor nicht autorisiertem Informationszugang sowie Datenschutz und Schutz des geistigen Eigentums müssen in den unterschiedlichsten Anwendungsgebieten gewährleistet werden. Komplexe elektronische Prozesse mit einer Vielzahl von beteiligten Partnern und Organisationen unter gleichzeitiger Berücksichtigung wachsender Mobilität erfordern grundlegende Forschungs- und Entwicklungsarbeiten im Bereich der IT-Sicherheit.
Nachfolgend sind einige wichtige Themenkomplexe benannt, die unter anderem auch vom Institut für Sichere Telekooperation bearbeitet werden.

Public-Key-Infrastrukturen

Obwohl das Konzept der Public-Key-Infrastrukturen (PKI) im Zusammenhang mit der digitalen Unterschrift schon älter als zehn Jahre ist, wird die zugehörige Technik in Unternehmen nur zögerlich angewendet. Ein wesentlicher Grund dafür ist der hohe Aufwand, der auf jedem Rechner erbracht werden muss, um Unterschriften zu prüfen, Zertifikate zu suchen und Zertifizierungspfade aufzubauen. Die Benutzbarkeit der PKI-Technologie kann durch eine Verlagerung dieser komplexen Funktionalität auf die Seite einer oder weniger unternehmenszentraler Instanzen entscheidend verbessert werden. Eine solche skalierbare und kostenreduzierende Sicherheitsinfrastruktur wird in dem NSI-Projekt [5] entwickelt und erprobt.

Biometrische Authentifizierung

Die Smartcard hat sich in den vergangenen Jahren als wichtigster Vertreter eines «Secure Signature Creation Device» (SSCD) etabliert. Um sicherzustellen, dass nur der rechtmässige Besitzer die Karte benutzen kann, wird fast ausschliesslich ein wissensbasiertes Verfahren, der PIN, benutzt. Biometrische Verfahren finden kaum Anwendung, obwohl sie eine wesentlich stärkere Bindung zwischen Person und Karte herstellen. In aktuellen Forschungsarbeiten wie dem TruPoSign-Projekt (Trusted Pocket Signer [6]) wird untersucht, welche biometrischen Verfahren für den Einsatz im Smartcard-Bereich geeignet sind, wie hoch die Fehlerraten sind und wie die Kommunikation zwischen dem biometrischen Sensor und

dem Smartcardchip abgesichert werden kann.

Sicherheit als Prozess
Um wirklich Sicherheit im Gesamtsystem zu gewährleisten, muss die Kette von den Anforderungen, den Mechanismen, ihrer Implementierung und der organisatorischen Umsetzung über ihre gesamte Lebensdauer betrachtet werden [1]. Einmal eingeführte Mechanismen müssen ständig auf ihre Einhaltung untersucht und Zweckerfüllung getestet werden. Ein Werkzeug, das diese notwendigen dynamischen Kontrollen unterstützt, wird zurzeit mit dem so genannten Sicherheitsinspektor im SKe-Projekt [8] entwickelt.

Sicherheit für mobile Benutzer
Mobiltelefone und PDAs (Personal Digital Assistant) werden in Zukunft immer mehr zu Smartphones zusammenwachsen. Sie ermöglichen es dem mobilen Nutzer, ortsabhängige Dienste zu nutzen (Location-based Services) und jederzeit von überall auf die Daten im Unternehmen wie E-Mails, Datenbankinformationen und Terminkalender zuzugreifen. Dies eröffnet jedoch auch neue Missbrauchsmöglichkeiten [3]. Sowohl der Diensteanbieter als auch der Kunde haben dabei berechtigte Sicherheitsanforderungen. Bei Letzterem spielt der Datenschutz eine wichtige Rolle. Im MOBILE-Projekt [4] wird eine agentenbasierte Sicherheitsplattform für mobile Endgeräte entwickelt, die den Spezifika der mobilen Nutzung Rechnung trägt.


Swisscom réprotechnique

Spezielle Schutzvorkehrungen schützen Menschen und Unternehmen vor Gefahren, wie das Eindringen von nicht autorisierten Personen.

Virtuelle, sichere Zusammenarbeit
Die Arbeitswelt der Zukunft wird durch ein hohes Mass an Vielfalt, Dynamik und Flexibilität geprägt sein. Virtuelle Organisationen mit organisationsübergreifenden, räumlich verteilten und mobilen Teammitgliedern sind Beispiele dafür. Die Informationstechnologie, unter wesentlicher Beteiligung der Sicherheitstechnik, muss Plattformen schaffen, um diese Arbeitsweise auf der Basis etablierter Standards zu unterstützen. Die Plattformen müssen dabei über inhärente, modulare Sicherheitsfunktionalitäten verfügen. Nur so lässt sich die Forderung nach Sicherheit und Einfachheit für den Benutzer erfüllen. Im europäischen Projekt UNITE [9] wird eine Plattform für eine teamorientierte, virtuelle Zusammenarbeit entwickelt und zur Verfügung gestellt.

Sicherheitskritische Infrastrukturen
Wir sind bereits heute in hohem Mass von verschiedenen Infrastrukturen abhängig, zwischen denen starke Wechselwirkungen bestehen, sodass sich Fehlfunktionen einzelner Komponenten fortpflanzen und in kürzester Zeit das gesamte globale System kollabieren lassen können. Eine wesentliche Herausforderung für zukünftige Forschungs- und Entwicklungsarbeiten im Bereich der Sicherheit besteht deshalb darin, mittels geeigneter Modellierungs- und Simulationstechniken die komplexen Systemzusammenhänge besser zu erfassen und zu verstehen. Zur Absicherung global vernetzter, sicherheitskritischer Infrastrukturen sind neue Technologien sowohl zur Gewährleistung der Zuverlässigkeit als auch der Datensicherheit zu entwickeln und in die bestehenden Infrastrukturen zu integrieren. Forschungsinstitute der verschiedensten Bereiche, wie beispielsweise aus dem IuK-Bereich, dem Bereich der Konstruktionstechnik und der Materialforschung oder aber auch aus dem Bereich der Verkehrs- und Infrastruktursysteme, müssen gemeinsame Forschungsanstrengungen unternehmen, um Lösungen zu entwickeln, die den Bürgern künftig ein solides Vertrauen in die Zuverlässigkeit und Sicherheit kritischer Infrastrukturen verschaffen.

Fraunhofer Institut SIT
Das Fraunhofer Institut SIT ist das führende deutsche Institut in IT-Sicherheitsfragen. In Zusammenarbeit mit industriellen Partnern und Forschungsinstitutionen werden neue, anwendungsnahe Lösungen entwickelt, und über Beratungs- und Entwicklungsdienstleistungen werden innovative Ergebnisse auch kleinen und mittleren Unternehmen verfügbar gemacht. Info: E-Mail: claudia.eckert@sit.fraunhofer.de, Homepage: www.sit.fraunhofer.de

Neue sicherheitssensitive Anwendungen
Im Internet werden permanent neue sicherheitssensitive Anwendungen kreiert. Diese sind daraufhin zu untersuchen, ob sie neuartige Sicherheitsanforderungen stellen, die Anlass zu einer Fortentwicklung von Sicherheitsarchitekturen und -mechanismen geben. Beispiele für Anwendungen dieser Art sind:
- Anwendungen im Bereich E-Government, insbesondere sicherheitssensitive Online-Dienste
- Sicherheitsfragen bei der E-Logistik
- Anwendungen zum Thema «Supply Chain Management»
- Anwendungen im Gesundheitsbereich

Fazit
Informationen und Wissen gehören zu den wertvollsten Produktionsfaktoren einer Hochtechnologiegesellschaft, sodass deren Schutz von hoher wirtschaftlicher Bedeutung ist. Damit werden Forschungs- und Entwicklungsarbeiten im Bereich der IT-Sicherheit zu kritischen Erfolgsfaktoren der gesamten Wirtschaft. Die Sicherheitstechnik ist als eine Schrittmacher-Technologie zu sehen, durch die erst die vielfältigen Möglichkeiten der Telekommunikation grossflächig nutzbar werden. Der Wissenschaft und der industrienahen Forschung stellt sich die Aufgabe, integrative, einfach zu nutzende Sicherheitslösungen zu entwickeln, durch die neue Märkte erschlossen, Kosten eingespart und die Flexibilität von unterneh-

merischen Abläufen gesteigert werden können. Das Fraunhofer Institut für Sichere Telekooperation (FHI-SIT) erarbeitet mit industriellen Partnern in verschiedenen Projekten Lösungen für aktuelle Fragestellungen im Zusammenhang mit der IT-Sicherheit. [4]

Das Buch zum Thema: «IT-Sicherheit»

Mit der rasanten Verbreitung des Internets und dessen Nutzung für private und geschäftliche Transaktionen (z. B. E-Business) steigt der Bedarf an sicheren informationstechnischen Systemen. Diese müssen sorgfältig geplant werden. Welche Aspekte dabei eine Rolle spielen und welche verschiedenen Ansätze verfolgt werden können, wird in diesem Buch systematisch beschrieben. Die zur Umsetzung der Sicherheitsanforderungen benötigten Verfahren und Protokolle werden detailliert vorgestellt und anhand von Fallbeispielen erläutert. Ausgangspunkt sind die Beschreibung typischer Bedrohungen wie «Buffer Overflows» oder Viren und die organisatorischen und technischen Massnahmen, die zu deren Abwehr notwendig sind:

- Sicherheitsbedrohungen durch Buffer Overflows, Viren, Würmer
- Internet-(Un)Sicherheit
- Sicherheitsmodelle
- Kryptografische Verfahren und digitale Signaturen
- Schlüsselmanagement
- Authentifikation
- Zugriffskontrolle
- Firewalls, Netzwerksicherheit und sichere Anwendungen
- Sichere mobile Systeme

Dieses Buch ist ein Muss für jeden, der sich mit dieser hoch aktuellen Problematik beschäftigt.

Claudia Eckert, «IT-Sicherheit», Konzepte – Verfahren – Protokolle, Oldenbourg Verlag, München, 2., überarbeitete und erweiterte Auflage 2002, geb., 720 S., € 54.80, ISBN 3-486-27205-5.

Professorin Dr. Claudia Eckert *promovierte und habilitierte an der Technischen Universität München für das Fach Informatik. Nach Aufenthalten an verschiedenen Universitäten folgte sie 2001 dem Ruf an die Technische Universität Darmstadt und gleichzeitig dem Ruf der Fraunhofer Gesellschaft in die Institutsleitung des Fraunhofer Instituts für Sichere Telekooperation (SIT). Als Ordinaria für Sicherheit in der Informationstechnik beschäftigt sie sich mit Fragen der IT-Sicherheit in vernetzten und mobilen Systemen, von der Hardware bis hinauf zu den Anwendungen. Sie ist Mitgründerin des Darmstädter Zentrums für IT-Sicherheit (DZI) an der Technischen Universität Darmstadt.*

Literatur

[1] Eckert, C., «IT-Sicherheit – Konzepte, Verfahren und Protokolle», Oldenburg-Verlag, München, 2. Auflage, 2003.
[2] Eckert, C. und Enzmann, M., «Pseudonymes Einkaufen physischer Güter für Internet-Shops ohne Zwischenhändler», Konferenz Elektronische Geschäftsprozesse, 2002.
[3] Eckert, C. und Baumgarten, U., «Mobil und trotzdem sicher?», In: it+ti Informationstechnik und Technische Informatik, 2001.
[4] Hoffmann, M., Peters, J. und Pinsdorf, U.: «Multilateral Security in Mobile Applications and Location Based Services», Information Security Solutions Europe, ISSE, Oct 2002.
[5] NSI, Homepage: www.sit.fraunhofer.de/german/SICA/sica_projects/NSI/index.html
[6] TruPoSign, Homepage: www.sit.fraunhofer.de/english/SICA/sica_projects/TruPoSign/index.html
[7] SIT, Fraunhofer Institut für Sichere Telekooperation (SIT), Homepage: www.sit.fraunhofer.de
[8] SKe, Homepage: www.sit.fraunhofer.de/german/MINT/mint_projects/index.html
[9] Zapf, M., Reinema, R., Wolf, R., Türpe, S., «UNITE – an Agent-oriented Teamwork Environment», Fourth International Workshop on Mobile Agents for Telecommunication Applications (MATA '02), 23./24. Oktober 2002.

Summary

IT Security – Constraint or Pacesetter?

In our day-to-day lives we have developed measures aimed at protecting ourselves from risks such as accidents, theft or intrusion into our personal privacy. We tend, however, to take such measures for granted. Home security, vehicle safety, trustworthy institutions such as public authorities, lawyers or banks have become part and parcel of our everyday lives. What impact is information and communications technology having on this situation? This article takes a look at the role of IT security in today's information and knowledge society. It examines the value of IT security as an economic factor and as an enabling technology for new fields of application such as e-business. It addresses the critical problem areas and presents a number of current research and development projects. The article aims to show how security technology should be viewed not as an inhibitor but rather as driving force for innovative applications.