Barcal Thomas 9150876
Bauer Michael 8920516
Hofmann Peter 9150172
Paukovits Christian 9152216
Rudorfer Leopold 9151587
Schlossinger Ines 9032262
Zelenka Georg 8805408
Zeller Harald 9104359

Seminararbeit

WS 1996/1997

„Sicherheitsanforderungen im Inter- und Intranet

Fallbeispiele österreichischer Anwender verschiedener Branchen“

aus Wirtschaftsinformatik
WI-SE C
Dr. Neumann-Alkier L.
Prof. Dr. Neumann G.

INHALTSVERZEICHNIS

1.

Einleitung

1..1 Bedeutung der Sicherheit

Sicherheit ist ein Thema, das in den Bereichen Internet und Intranet immer mehr an Bedeutung gewinnt. Setzt man sich damit auseinander, dann muß man sich zuerst überlegen, was das Wort Sicherheit überhaupt bedeutet.

„Sicherheit, Zustand des Unbedrohtseins, der sich objektiv im Vorhandensein von Schutz[einrichtungen] bzw. Im Fehlen von Gefahr[enquellen] darstellt und subjektiv als Gewißheit von Individuen oder sozialen Gebilden über die Zuverlässigkeit von Sicherungs- und Schutzeinrichtungen empfunden wird.„[1].

Verschärfte Sicherheitsanforderungen gelten ebenso für den gesamten EDV Bereich, insbesondere für die Bereiche des Intra- und Internet. Es muß zum Beispiel verhindert werden, daß wichtige, vertrauliche Daten von jeder Person abgerufen oder verändert werden können. Dieses Problem ist unternehmensintern noch relativ gut in den Griff zu bekommen (Bsp. Passwortvergabe etc.). Der Personenkreis ist relativ klein und die Mitarbeiter sind bekannt. Im Internet aber „surfen„ täglich tausende unbekannter Personen und alle diese Personen stellen für das Unternehmen eine potentielle Gefahr dar. Denn mit dem entsprechenden Know-How könnten Personen in die lokalen Netzwerke der Unternehmen eindringen und so erhebliche Schäden anrichten.

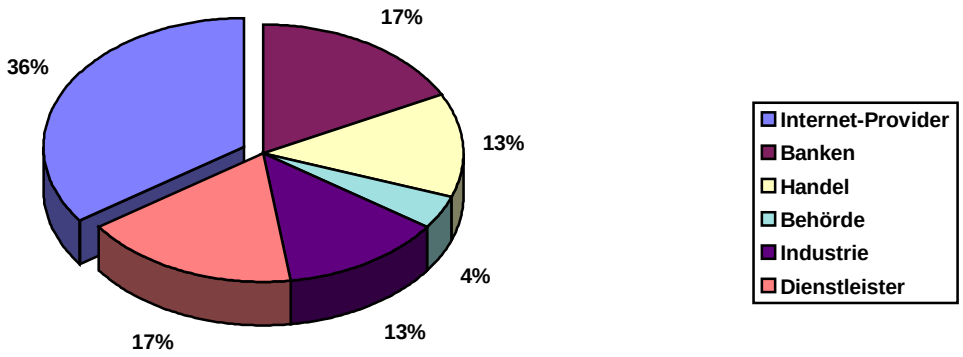
1..2 Zielsetzung und Vorgehensweise

Diese Arbeit soll die theoretischen Aspekte des Themas Sicherheit im Inter- und Intranet genauer erläutern. Weiters soll sie auch eine Momentaufnahme der Handhabung des Themas Sicherheit einiger ausgesuchter österreichischer Unternehmen, die Internetdienste anbieten, darstellen.

In Summe haben wir 24 österreichische Unternehmen befragt, von denen wir aufgrund unserer Recherchen wußten, daß sie über einen Internetanschluß verfügen, Internetdienste anbieten oder Erfahrung im Bereich des Intranets haben. Von den Internet-Service-Providern haben wir die größten ausgewählt und auch einige ihrer bekannten Kunden miteinbezogen.

[1] Meyers großes Taschenlexikon Band 20, 1987

Die Unternehmen sind in folgenden Branchen tätig:



Unsere Gesprächspartner waren die Geschäftsführer bzw. Vorstandsmitglieder oder Personen aus der EDV-Abteilung. Bei den Interviews haben wir uns an einen einheitlichen Gesprächsleitfaden gehalten, trotzdem sind die Gespräche durchwegs unterschiedlich verlaufen und wir haben je nach Spezialwissen und Interessensgebiet unserer Interviewpartner verschieden viel Information zu den einzelnen Punkten bekommen.

Wir haben versucht, alle Interviewtermine zu zweit wahrzunehmen und haben die Interviews sofort protokolliert und an alle Mitglieder unserer Seminargruppe per email verteilt.

Einige unserer Interviewpartner haben größten Wert auf die vertrauliche Behandlung der Daten gelegt und uns gebeten, sie nicht in der Arbeit zu erwähnen. Aus diesem Grund verwenden wir in unserer Seminararbeit weder Firmennamen noch die Namen unserer Interviewpartner.

Bei der Themenauswahl haben wir überlegt, mit welchen Problemen ein Unternehmen konfrontiert wird, wenn es im Internet tätig ist. Dabei haben sich die folgenden drei Schwerpunkte herauskristallisiert.

- Recht

  „Recht gibt Sicherheit„. Dieser Bereich soll die rechtlichen Aspekte des Seminarthemas genauer erläutern, da dieser in Zukunft durch die Verwendung von z.B. elektronischen Zahlungsmitteln , etc. stark an Bedeutung gewinnen wird.

  - Privatrechtliche Bestimmungen
  - Datenschutz
  - Strafrechtliche Bestimmungen

- Organisation

  Sicherheit muß organisiert sein, um effektiv gegen „Hacker„ und andere Eindringlinge Schutz zu bieten.

  - Organigramm
  - Organisation der EDV (Thematik Outsourcing)
  - Abgrenzung Inter- und Intranet
  - Kosten/Nutzen der Sicherheit

- Technik

  Auf der Technik basiert die gesamte Sicherheitsstruktur eines Unternehmens

  - Art der Anbindung des Unternehmens ans Internet
  - Eingesetzte Hardware und Software (PGP, Firewalls)
  - Elektronische Zahlungsmittel,

2. Rechtliche Aspekte der Sicherheit

2..1 Einleitung

Bei einem Brainstorming, welches wir zu Beginn dieser Seminararbeit machten, stellte sich heraus, daß es auch im rechtlichen Bereich zahlreiche Problembereiche im Bezug auf Sicherheit gibt. Dies reicht einerseits von der Unsicherheit der Unternehmen wann ein Vertrag als abgeschlossen gilt, über datenschutzrechtliche Probleme bis hin zu den Problemen die sich daraus ergeben, welches Rechtsvorschriften eigentlich anzuwenden sind. Daher haben wir diesen Abschnitt in drei Teile gegliedert:

- privatrechtlichen Bestimmungen
- Strafrecht
- Datenschutz

Im ersten Teil sollen die Problembereiche die den Vertragsanschluß und den Konsumentenschutz betreffen aufgezeigt und behandelt werden. Der zweite und der dritte Teil behandelt datenschutzrechtliche Probleme, dabei seien Logfiles, Cookies erwähnt und die damit zusammenhängenden strafrechtlichen Bestimmungen, welche im besonderen für die Provider gelten. Im Anschluß an jeden Teil werden die Meinungen der Interviewpartner, aus den verschiedensten Branchen wiedergegeben.

2..2 Privatrechtliche Bestimmungen

In diesem Abschnitt soll die Frage behandelt werden, inwieweit die bestehenden privatrechtlichen Gesetze im Internet angewandt werden können. In der Praxis begegneten wir sehr

unterschiedlichen Meinungen. Im folgenden sollen nun diese angerissen werden und die derzeitigen Lösungswege dargestellt werden.

Vertragsabschluß

Da immer mehr Unternehmer Waren oder Dienstleistungen über das Internet anbieten, werden auch zahlreiche rechtliche Probleme aufgeworfen, vor allem betreffend die Gültigkeit von Verträgen und die Möglichkeit eines Rücktrittsrechtes. Zugang zum Internet kann sich grundsätzlich jeder verschaffen, es sind keinen besonderen Voraussetzungen nötig. In Österreich genügt es einfach an einer Universität inskribiert zu sein, um eine Internet-Adresse zu bekommen. Es entstehen daher schon Probleme mit der Feststellung der Identität sowohl des Anbieters als auch des Bestellers.

Um einen Vertrag auch gültig abzuschließen, muß eine übereinstimmende Willenserklärung zwischen den Vertragspartnern gem. § 861 ABGB geben sein

> § 861
>
> Wer sich erklärt, daß er jemandem sein Recht übertragen, das heißt, daß er ihm etwas gestatten, etwas geben, daß er für ihn etwas tun, oder seinetwegen etwas unterlassen wolle, mache ein Versprechen; nimmt aber der andere das Versprechen gültig an, so kommt durch den übereinstimmenden Willen beider Teile ein Vertrag zustande. Solange die Unterhandlungen dauern, und das Versprechen noch nicht gemacht, oder weder zum voraus, noch nachher angenommen ist, entsteht kein Vertrag.

Die einleitende Willenserklärung bezeichnet man auch als Anbot und hat zur Folge, daß es den Anbieter bindet. Es obliegt nun dem Empfänger des Anbots, ob der das Angebot annimmt oder nicht. Damit das Angebot jedoch verbindlich ist, müssen zwei Voraussetzungen erfüllt sein: erstens muß der Vertragsinhalt ausreichend bestimmt sein und es muß ein eindeutiger Bindungswille des Anbieters erkennbar sein. Daher ist das Übersenden von Katalogen, Preislisten und dgl. nicht als Angebot zu sehen.

Bietet nun ein Unternehmer Waren über Internet an, so sind die Informationen über seine Produkte, die auf der Homepage zu finden sind, rechtlich als ein Offert an einen unbestimmten

Personenkreis (vergleichbar mit dem Automatenverkauf) oder die Aufforderung zur Stellung von Anboten (z.B. Annoncen, Schaufenster ...) zu sehen. Die herrschende Lehre geht davon aus, daß es sich eher um eine Aufforderung zur Stellung von Anboten handelt, da z.B. bei einem Automatenverkauf der Käufer typischerweise durch Einwurf des Kaufpreises seine Leistung sofort erbringt, während im Internet der Anbieter vorleistet bzw. die Ware gegen Nachnahme liefert. Für den Anbieter ist es auch ratsam auf seiner Homepage darauf hinzuweisen, daß er sich eine Ablehnung der Bestellung vorbehält, und somit fehlt ihm der für ein Offert erforderliche Bindungswille.[2]

Im Internet stellt somit der Käufer das Anbot, indem er via Internet eine Nachricht in die Mailbox des Anbieters sendet. Die Mailbox ist rechtlich wie ein Briefkasten zu sehen, wo nun die Regeln der Zugangstheorie gem. § 862a ABGB anzuwenden sind.

> § 862a
>
> Als rechtzeitig gilt die Annahme, wenn die Erklärung innerhalb der Annahmefrist dem Antragsteller zugekommen ist. Trotz ihrer Verspätung kommt jedoch der Vertrag zustande, wenn der Antragsteller erkennen mußte, daß die Annahmeerklärung rechtzeitig abgesendet wurde, und gleichwohl seinen Rücktritt dem andern nicht unverzüglich anzeigt.

Somit beginnt die Bindungswirkung mit dem Eingang der Nachricht in der Mailbox, soweit dieser nicht zu einer Zeit erfolgt, zu der mit einer Kenntnisnahme nicht gerechnet werden kann (z.B. an Wochenenden oder Feiertagen oder während der Nacht). Das Anbot kann bis zur tatsächlichen Kenntnisnahme durch den Anbotsempfänger widerrufen werden. Dies erfolgt durch eine weitere Nachricht in der Mailbox, aber es kann auch telefonisch oder persönlich erfolgen.

2..2.1 **Allgemeine Geschäftsbedingungen**

Gemäß § 864a ABGB muß der Verwender von AGBs darauf hinweisen bzw. der Kunde muß die Möglichkeit zur Kenntnisnahme dieser haben.

[2] Madl, ecolex 1996, 79

§ 864a

Bestimmungen ungewöhnlichen Inhaltes in Allgemeinen Geschäftsbedingungen oder Vertragsformblättern, die ein Vertragsteil verwendet hat, werden nicht Vertragsbestandteil, wenn sie dem anderen Teil nachteilig sind und er mit ihnen auch nach den Umständen, vor allem nach dem äußeren Erscheinungsbild der Urkunde, nicht zu rechnen brauchte; es sei denn, der eine Vertragsteil hat den anderen besonders darauf hingewiesen.

Im Internet müssen daher laut diesen Bestimmungen auch die allgemeinen Geschäftsbedingungen auf der selben Seite wie die Informationen über die Produkte zu finden sein. Es ist sicherlich auch ausreichend, wenn sich die AGBs auf einer auffallenden Seite befinden, die vom Kunden vor der Bestellung gesehen werden muß. Daher wird die Kenntnisnahme der AGB nur dann anzunehmen sein, wenn diese auch über Internet abrufbar sind oder zumindest ein deutlicher Hinweis aufscheint, daß die AGB auf Wunsch zur Verfügung gestellt werden.

2..2.2 **Konsumentenschutz**

Gemäß § 3 KSchG steht dem Konsumenten grundsätzlich das Recht zum Vertragsrücktritt bei Haustürgeschäften zu.

§ 3 KSchG

(1) Hat der Verbraucher seine Vertragserklärung weder in den vom Unternehmer für seine geschäftlichen Zwecke dauernd benützen Räumen noch bei einem von diesem dafür auf einer Messe oder einem Markt benützen Stand abgegeben, so kann er von seinem Vertragsantrag oder vom Vertrag zurücktreten.

Allerdings ist dieses Rücktrittsrecht dann ausgeschlossen, wenn der Verbraucher selbst die geschäftliche Verbindung angebahnt hat oder wenn dem Vertragsabschluß keine Besprechungen vorausgegangen sind.

§ 3 KSchG

> (3) Das Rücktrittsrecht steht dem Verbraucher nicht zu,
>
> 1. wenn der selbst die geschäftliche Verbindung mit dem Unternehmer oder dessen Beauftragten zwecks Schließung dieses Vertrages angebahnt hat,
>
> 2. wenn dem Zustandekommen des Vertrages keine Besprechungen zwischen den Beteiligten oder ihren Beauftragten vorangegangen sind .

Wendet man nun diese Regelungen auf Geschäfte über Internet an, so stellt man fest, daß regelmäßig beide Ausnahmetatbestände erfüllt sind. Eine Anbahnung durch den Verbraucher wird ja schon dann angenommen, wenn der Verbraucher auf ein Inserat des Unternehmers reagiert oder eine vorgedruckte Karte absendet, die er durch die Postwurfsendung erhalten hat. Die auf einer Homepage enthaltenen Informationen sind mit vom Unternehmer geschalteten Inseraten oder Postwurfsendung zu vergleichen. Aber auch die Ausnahmeregelung der fehlenden Besprechungen, die gerade auf den Versandhandel abstellt, ist auf Bestellungen im Internet anwendbar. Dem Besteller steht daher nach der derzeitigen Rechtslage kein Rücktrittsrecht zu. Diese Regelung ist daher für den Konsumenten sehr unbefriedigend, denn das Problem besteht hier darin, daß die geschickte Präsentation von Produkten am Bildschirm oft zu unüberlegten Vertragsabschlüssen führt. Außerdem hat der Konsument im Regelfall nicht die Möglichkeit, sich einen objektiven Eindruck über das angebotene Produkt zu verschafften, weil die Präsentation am PC besonders die positiven Eigenschaften herausstreicht und die negativen Eigenschaften zu verbergen versucht. Innerhalb der Europäischen Union ist man sich dieses Problembereiches bewußt und es sind derzeit Bestrebungen im Gange, die versuchen einen Lösungsweg zu finden. Die sogenannte Fernabsatz-Richtlinie, die eine Lösung bietet, soll nun im folgenden genauer beleuchtet werden.

2..2.3 **Fernabsatz-Richtlinie**

Der Rat der Europäischen Union hat einen Entwurf einer Richtlinie über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz ausgearbeitet, der derzeit beim Vermittlungsausschuß Rat - Parlament zur Behandlung liegt. Dieser Entwurf würde eine Anpassung des österreichischen KSchG und insbesondere des Rücktrittsrechts gem. § 3 KSchG erforderlich machen.

Diese Richtlinie gilt nicht nur für Geschäfte im Internet sondern insbesondere auch für den Versandhandel, Teleshopping, Zusendung von Drucksachen etc.. Voraussetzung für die Anwendung ist, daß der Unternehmer für den Vertrag bis hin zu dessen Abschluß ausschließlich eine oder mehrere Fernkommunikationstechniken verwendet. Wird über Internet jedoch ein Kontakt angebahnt und kommt es anschließend zu einem Besuch durch einen Verteter oder einen Vertragsabschluß im Geschäft des Unternehmers, so findet diese Richtlinie keine Anwendung sondern es greift in diesen Fällen § 3 KSchG. Die Richtlinie soll nur einen Mindeststandard schaffen, so daß strengere Vorschriften zugunsten der Verbraucher in den einzelnen Mitgliedstaaten beibehalten bzw. neu eingeführt werden können. Der Unternehmer muß den Verbraucher klar und verständlich vor Vertragsabschluß über die für die Entscheidung des Verbrauchers wichtigen Punkte informieren. Dazu zählen

- Identität des Unternehmers (Name, Rechtsform, Adresse)
- wesentliche Eigenschaften des Produktes
- Preise inkl. Steuern
- Lieferkosten
- Zahlungs- und Liefermodalitäten
- Belehrung über das Rücktrittsrecht

Ein Hinweis auf Art 6 der Richtlinie wird nicht ausreichend sein, sondern es sollte zumindest der Text von Art 6 zitiert werden. Weiters müssen auch die Kosten der Fernkommunikation, sofern sie über dem Grundtarif liegen, und die Gültigkeitsdauer des Preises oder Angebots angegeben werden. Diese Informationen müssen dem Verbraucher bis zur Erfüllung des Vertrages, spätestens bis zur Lieferung auch schriftlich erteilt werden.

Vergleicht man die Regelungen des Art 6 mit den derzeit geltenden Bestimmungen des § 3 KSchG, so steht jedenfalls ein Rücktrittsrecht zu. Ausnahmen finden sich unter Art 6 (3) der Richtlinie und zwar dann, wenn bei einem Rücktritt für den Unternehmer die Gefahr besteht, daß der Verbraucher sich zwar der Leistung zuwendet aber keine Gegenleistung zu erbringen hat, oder die Leistung für den Unternehmer bei der Rückabwicklung nicht mehr brauchbar ist. En Rücktrittsrecht steht auch dann nicht zu, wenn bei Dienstleistungen die Erfüllung durch den Unternehmer mit Zustimmung des Verbrauchers vor Ablauf der Rücktrittsfrist von sieben Tagen

begonnen wird. Dem Verbraucher steht somit das Rücktrittsrecht innerhalb von sieben Tagen nach Vertragsabschluß bei Dienstleistungen oder nach Erhalt der Waren zu.

Die geplante Richtlinie erweitert bei Konsumentengeschäften die Möglichkeit des Rücktrittsrechts und schreibt Mindestinformationen vor, die in dauerhafter Form dem Verbraucher zur Verfügung gestellt werden müssen. Die Chancen, daß diese Richtlinie auch umgesetzt wird ist sehr groß, zwar wird es noch in dem einen oder anderen Bereich zu Abänderungen kommen, doch grundsätzlich findet sie große Zustimmung innerhalb der einzelnen Mitgliedsstaaten. Nach der geltenden Rechtslage jedoch steht dem Verbraucher noch kein Rücktritts recht nach § 3 KSchG zu.

2..3 Forschungs- und Arbeitsgruppen im Bereich „Recht im Internet„

Sowohl auf internationaler als auch auf nationaler Ebene befassen sich zur Zeit zahlreiche Arbeitsgruppen mit den rechtlichen Problemen, die durch das Internet hervorgerufen wurden. Im folgenden sollen nur die wichtigsten erwähnt sein.

International

OECD

Die bei der OECD eingerichtete Arbeitsgruppe befaßt sich mit den bedeutsamen Fragen die sich durch den Einsatz von Verschlüsselungstechniken, der Zulassung und Vergabe von Schlüsseln und der Einrichtung von Zertifizierungen. Sie sollen vorallem die daraus entstehenden rechtlichen Probleme versuchen zu lösen. Leider sind von dieser Gruppe noch keine Ergebnisse bekannt, da sie noch hinter verschlossenen Mauern arbeiten.

UNICITRAL

Die UN-Kommission für internationales Handelsrecht arbeitet an einem Modellgesetz über den elektronischen Handel. Der dabei ausgearbeitete Entwurf wurde von der Kommission angenommen und liegt zur Zeit bei der Generalversammlung auf. Dieses Modellgesetz enthält Bedingungen für das elektronische Äquivalent eines Schriftstücks, einer Unterschrift und eines Originals, es befaßt sich mit der Zulässigkeit und dem Beweiswert von Datenbotschaften in behördlichen Verfahren, der Risikoverteilung bei Übermittlungsfehlern und mit der Bedeutung einer elektronischen Empfangsbestätigung. Dieses Gesetz beruht auf der Tatsache, daß die geltenden vertrags- und handelsrechtlichen regeln grundsätzlich auch für den Vertragsabschluß mittels

Computer zu schaffen, dies wurde jedoch abgewehrt. Denn man ist der Meinung, daß versucht werden soll, mit den bestehenden Regeln auszukommen und nur dort wo die Eigenart der verwendeten Technologie es erforderlich macht, notwendige Ergänzungen zu den bestehenden Gesetzen anzubringen.[3]

Europäische Union
Hierbei sei die vorhin bereits erwähnte und behandelte Fernabsatzrichtline zu erwähnen.

National
Auch die österreichische Bundesregierung hat eine Arbeitsgruppe „Österreichs Weg in die Informationsgesellschaft eingerichtet. Hier soll untersucht werden, inwieweit die bestehenden gesetzlichen Regeln auch Anwendung im Internet finden. Laut Auskunft eines Mitgliedes dieser Projektgruppe aus dem Jusitzministerium sucht Österreich internationale Lösungen und versucht auch in den jeweiligen Arbeitsgruppen sowohl bei der Europäischen Union als auch bei den Vereinten Nationen aktiv mitzuarbeiten. Bis nun die einzelnen Projektgruppen zu einer Lösung kommen, versucht man mit den bestehenden Regeln auszukommen.

2..3.1 Case-Study

Bei den Befragungen der Unternehmen sind wir unter anderem speziell auf folgende Fragen eingegangen.

Frage:
Wann ist für Sie der Vertrag gültig zustande gekommen?

Antworten:
Ein Anbieter von Kleinanzeigen, der auch über Internet seine Dienste anbietet, erklärte, daß der Vertrag erst dann zustande gekommen ist, wenn der Käufer die Kreditkartenabrechnung akzeptiert bzw. bezahlt. Sie orientieren sich dabei an die Auskünfte ihres Rechtsberaters.

Anbieter von Waren über das Internet folgen der herrschenden Lehre, die im bereits ausführlich beschrieben wurde.

[3] Johannes Stabentheiner, ecolex 1996, 748

Die zahlreichen Provider die wir dazu befragten konnten uns dazu keinerlei Auskunft geben, da sich die Interviewpartner mit dieser Problematik zuwenig oder noch gar nicht auseinandergesetzt haben.

Frage:
Sind die AGBs bereits in Ihrer Homepage zu finden?

Antworten:
Vorallem die Banken sind daran interessiert auch ihre allgemeinen Geschäftsbedingungen in ihre Homepage aufzunehmen, da diese ein wichtiger Bestandteil ihrer Geschäfte darstellen. Bis jetzt sind die AGBs noch auf keiner Homepage zu finden, jedoch sollte dies zu Beginn dieses Jahres erfolgen, so die Antwort der Interviewpartner.

Auch der Anbieter von Kleinanzeigen möchte ordnungshalber die AGBs in seiner Homepage aufnehmen, obwohl dies nicht gesetzlich vorgeschrieben ist. Als Veröffentlichungstermin wurde uns Beginn 1997 genannt.

Unternehmen die Waren über das Internet anbieten wollen auch die AGBs in ihre Homepage aufnehmen, doch sind diese Seiten erst in Arbeit.

Das Justitzministerium gab uns zur Antwort, daß die AGBs auch auf den Hompages zu finden sein müssen, da dies auch gesetzlich vorgeschrieben ist.

Frage:
Inwieweit sind die bestehenden Gesetze auch auf das Internet anwendbar?

Antworten:
Das Justitzministerium gab uns die Anwort, daß die bestehende Lösung eine Notlösung sei, und daß man bestrebt ist neue Gesetze zu schaffen. Bis konkrete Ergebnisse vorliegen hat man versucht die bestehenden Regeln auch auf Geschäfte im Internet anzuwenden.

Frage:
Besteht die Möglichkeit nach Abschluß eines Geschäftes über Internet problemlos vom Vertrag zurückzutreten?

Antwort:

Der Anbieter von Kleinanzeigen ist der Meinung, daß es sehr leicht ist vom Vertrag zurückzutreten, denn man braucht nur bei der Kreditkartenfirma gegen die fragwürdige Position Einspruch erheben.

Auch die Anbieter Waren folgen der Meinung dieses Kleinanzeigenunternehmens.

Im Gegensatz dazu vertritt das Justitzministerium die Meinung, daß kein Rücktritt vom Vertrag möglich ist. Es gibt zwar die Möglichkeit Einspruch bei der Kreditkartenfirma zu erheben, jedoch liegt die Beweislast beim Kunden und eine einfache Erklärung „Ich war das nicht„ reicht nicht aus.

2..4 Strafrecht

Im Bereich des Strafrechtes interessierte uns vor allem, wie sich Provider hinsichtlich eines möglichen Netzmißbrauches ihrer Kunden verhalten. Können sie bereits heute durch Gesetz dazu angehalten werden Mailboxen, Newsgroups und dergleichen zu kontrollieren, bzw. führen sie freiwillige Selbstkontrollen durch. Haften Provider für eine mißbräuchliche Verwendung des Internets durch ihre Kunden? Unter mißbräuchlicher Verwendung sei speziell die Verbreitung von Kinderpornographie, rechtsradikaler Propaganda und Raubkopien verstanden. Deweiteren interessierte uns, inwieweit heute bereits eine laufende Überwachunge eines Internetanschlußes durchgeführt werden kann.

Prinzipiell lassen sich gemäß derzeit herrschender österreichischer Rechtsauffassung „strafrechtsrelevante (Mailbox- oder Netz-)Inhalte in der Regel unter die herkömmlichen Strafrechtstatbestände subsumieren, so daß allein durch die Verwendung neuer Technologien zum Zwecke des Transports und der Verbreitung strafrechtswidriger Inhalte keine nennenswerten Strafbarkeitslücken entstehen.„ [4]

2..4.1 Providerhaftung

§16 FernmeldeG verlangt, daß Netzbetreiber „alle geeigneten Maßnahmen treffen, die eine mißbräuchliche Verwendung der (Fernmelde)Anlage ausschließen.„ Als mißbräuchlich definiert Abs 2 „jede Nachrichtenübermittlung, welche die öffentliche Sicherheit und Ordnung, oder

[4] Stabentheiner, ecolex 1996, 750

Sittlichkeit gefährdet, oder welche gegen die Gesetze verstößt„ (Z1) und andererseits „jede Verletzung der nach diesem Gesetz und den internationalen Verträgen bestehenden Geheimhaltungspflichten.„ (Z3)

Auf den ersten Blick ergibt sich hier für den Provider ein Dilemma: Kontrolliert er die Inhalte von Mailboxen, Newsgroups, oder den Inhalt abgerufener URLs, so trifft ihn zwar keine Haftung nach Z1, aber möglicherweise drohen ihm Konsequenzen aufgrund einer Verletzung von Geheimhaltungspflichten gem. Z3. Unterläßt er eine solche Überwachung, so haftet er nach Z1. Ganz egal was er auch macht, er handelt offensichtlich immer gesetzeswidrig. Laut herrschender Rechtsmeinung tritt keine Haftung bei bloßer Email-Kommunikation ein.[4a] In diesem Falle gehen Geheimhaltungspflichten der Inhaltskontrolle vor. Es wäre auch technisch und wirtschaftlich kaum realisierbar, den gesamten Email-Verkehr zu überwachen (Kapazitätsengpässe und Zeitverlust). Stellt der Provider jedoch seinen Kunden mehr als die bloßen Leitungen zur Verfügung, z.B. in der Form von moderierten Newsforen, so treten die Geheimhaltungspflichten in den Hintergrund und der Provider ist gezwungen, die Inhalte zu überwachen, soweit dies verhältnismäßig ist. Die Geheimhaltungspflicht ist hier zweitrangig, da es ja gerade die Absicht ist, Beiträge in Newsforen einer möglichst breiten Masse zur Verfügung zu stellen, i.G. zu Emails.

Die Haftung des Providers ist auch damit zu begründen, daß ja er es war, der eine bestimmte Newsgroup in die Welt gesetzt hat und er damit mögliche mißbräuchliche Verwendungen initiierte. „Verhältnismäßigkeit„ bedeutet in diesem Zusammenhang, daß er nur jene Newsgroups zu überwachen hat, von denen man annehmen kann (z.B. durch eindeutige Namen), daß dort fragwürdige Inhalte verbreitet werden. Lt. Brandl und Schönberger[4b] trifft den Provider aufgrund der Verhältnismäßigkeit bei unmoderierten Diskussionsforen nicht dieselbe Intensität der Überwachungspflicht wie bei moderierten. Der Provider wird jedoch die Diskussionsteilnehmer durch Textbotschaften ausdrücklich vor mißbräuchlichen Verwendungen zu warnen haben - ein Hinweis in den AGB ist zu wenig. Die selbe Regelung gilt auch für Anbieter von Online-Diensten, die im Rahmen ihres Gesamtpaketes auch einen Internetzugang anbieten. In diesem Fall kann man nicht mehr von einem reinen „Access-Provider„ sprechen. Auch hier kann man vom Provider aufgrund des Grundsatzes der Verhältnismäßigkeit nicht verlangen, sämtliche Aktivitäten eines Benutzers hinsichtlich strafgesetzwidriger Inhalte zu kontrollieren. Jedoch muß eine Warnung erfolgen, bevor ein Benutzer das Internet „betritt„. Abschließend ergibt sich: Reine Infrastrukturanbieter - sog. „Access-Provider„ sind zur Geheimhaltung nach §16 Abs2 Z3 FernmeldeG verpflichtet. „Content-Provider„ haften nach §16 Abs2 Z1 FernmeldeG für Dienstleistungen, die offenbar aufgrund ihres Charakters keiner Geheimhaltungspflicht unterliegen, verhältnismäßig.

In der folgenden Tabelle ist die Überwachungspflicht des Providers bei den verschiedenen Internetdiensten nochmals kurz zusammengefaßt:

[4a] Brandl und Schönberger, ecolex96, 131

Email	Geheimhaltungspflicht gem §16 Abs2 Z3
Newsforen - moderiert	Inhaltliche Überwachungspflicht §16 Abs2 Z1
Newsforen - unmoderiert	Abgeschwächte Überwachungspflicht, zumindest Warnung
Reiner Internetzugang	Geheimhaltungspflicht gem §16 Abs2 Z3
Internetzugang im Rahmen eines umfassenden Online-Dienstes	Abgeschwächte Überwachungspflicht, zumindest Warnung

Analog zur Überwachung eines Telefonanschlusses. schließen §§149a ff StPO prinzipiell die Möglichkeit zur Überwachung eines Internetanschlusses mit ein. Jedoch müssen wie bei der Telefonüberwachung ein dringender Tatverdacht sowie eine richterliche Anordnung vorliegen.[5]

2..4.2 Case-Study

Folgende Fragen stellten wir im Rahmen unserer case-study den Providern, um ihre Rechtsauffassung bzw. konkrete Vorgangsweise bezüglich strafgesetzwidriger Verwendungen des Internets bzw. hinsichtlich einer möglichen Überwachung ausfindig zu machen. Frage 1 und 2 beziehen sich auf die mißbräuchliche Verwendung des Internets duch Kunden, während Frage 3 sich auf die laufende Überwachung eines Anschlußes (analog zur Telefonüberwachung) bezieht.

[4b] Brandl und Schönberger, ecolex96, 131
[5] Stabentheiner,ecolex96, 752

Frage:

Aufgrund §16 FernmeldeG sind Provider verpflichtet gegen mißbräuchliche Verwendungen von Netzen (Kinderpornographie, Neo-Nazistische Umtriebe) vorzugehen, andererseits verlangt jedoch derselbe Paragraph, Geheimhaltungspflichten nicht zu verletzen. Wie verhalten Sie sich in diesem Dilemma?

Antworten:

Nur einer der befragten Provider erklärte er führe eine aktive Kontrolle von Newsgroups durch und zwar von jenen, die schon aufgrund ihres Wortlautes bzw. aus Erfahrung her verdächtigt erscheinen. Werden dort tatsächlich gesetzeswidrige Inhalte gefunden, so werden diese umgehend gesperrt.

Ein weiterer Provider war jedoch der Meinung, daß kein aktives Ermitteln von Nöten wäre. Er meinte, daß erst reagiert wird, wenn er von mißbräuchlichen Inhalten in Kenntnis gesetzt wird. Geschieht dies, so wird der betreffende Teilnehmer zuerst verwarnt und gegebenenfalls der betreffende Inhalt gelöscht. Ein dritter Provider war überhaupt der Meinung, daß es bezweifelt werden muß, ob Internet-Dienste überhaupt unter das FernmeldeG fallen, sondern soweit es Inhalte anbelangt, es sich um elektronische Onlinedienste handelt, die vielmehr unter das Mediengesetz fallen würden, hätte der Gesetzgeber es nicht verabsäumt dieses rechtzeitig anzupassen. Desweiteren träfe bezüglich §16 die Post die selbe Verantwortung wie den Provider, da sie es ja ist, welche die Fernmeldeeinrichtungen zur Verfügung stellt. „Falls die Post meint sie könne die Verantwortung vertraglich mittels AGB, oder Gesetzen auf ihre Kunden (Provider) abwälzen, so muß dem entgegengehalten werden, daß *wir* selbstverständlich auch die Einhaltung von Internet-internen Standards vertraglich an die Benutzer übertragen haben...„ Desweiteren wird von diesem Provider keine Vorabkontrolle durchgeführt, da er sich außerstande sieht den strafgesetzwidrigen Inhalt von transportierten mails oder Newsgroups klar zu erkennen. Zum Beispiel sieht er die Grenze zwischen Kunst und Pornographie als fließend an. Solche Beurteilungen überläßt er lieber den Behörden. Nur wenn ein österreichisches Gericht konkret die Daten benennen kann (nicht bloß einzelne Wörter, oder Konzepte), würde dieser Provider bei Rechtskraft des Urteils diese entfernen. Ein weiterer Provider hatte angeblich noch keine Probleme mit Internet-Mißbrauch, falls solche auftreten, würde er dies mit seinem Rechtsanwalt besprechen.

Bei einem anderen befragten Internet-Provider sind die Erstellung von erotischen homepages untersagt. Der Grund: Leitungsüberlastung. Nur wenn der Betreffende einen Mehrtarif in Kauf nimmt, darf er diese erstellen. Ein anderer Provider nimmt eine Klausel in seine AGB mit hinein, in denen der Kunde einer Überprüfung zustimmt.

Frage:
Wie wird bei einer solchen Kontrolle (hinsichtlich strafgesetzwidriger Inhalte) konkret vorgegangen, was und wie wird kontrolliert? Gibt es gemeinsame Initiativen solche Mißbräuche zu bekämpfen?

Antworten:
Diese Frage zu stellen, hätten wir uns sparen können, da sie keine brauchbaren Ergebnisse lieferte. Bis auf einen Provider führt, wie schon oben erwähnt, niemand eine aktive Überprüfung der Anschlüsse durch. Auf diese Frage bekamen wir daher zur Antwort, daß nicht aktiv kontrolliert wird. Jener Provider, der kontrolliert, äußerte sich nicht zu dieser Frage. Die Unterfrage hinsichtlich der gemeinsamen Initiativen von Providern gg. Internet-Mißbrauch wurde von allen Befragten verneint.

Frage:
Ist eine laufende Überwachung eines Internetanschlusses heute bereits erlaubt wenn ein dringender Tatverdacht gegeben ist und eine richterliche Anordnung vorliegt (analog zur telefonischen Überwachung)? Wie sieht eine Überwachung konkret aus? Was passiert, wenn der Teilnehmer Verschlüsselungsalgorithmen verwendet? Ist der Provider in diesem Falle verpflichtet den Schlüssel (falls er ihn kennt) herauszugeben?

Antworten:
Technisch sei laut Auskunft eines Providers eine derartige Überwachung so ziemlich das simpelste, was es im Internet gibt. Falls der Kunde Verschlüsselungssoftware einsetzt, ist dieser Provider in der „glücklichen„ Lage den privaten Schlüssel des Kunden nicht zu kennen (er verwendet ein auf PGP-basierendes Verschlüsselungssystem). Desweiteren würde er die Kenntnisnahme derartiger Information verweigern. Ein anderer Provider warf in diesem Zusammenhang die Kostenfrage einer solchen Überwachung auf. Diese sei nirgends geregelt. Wer sollte sie in so einem Fall tragen - der Provider, der Staat, der Überwachte? Ein weiterer Provider meinte er beschäftige sich damit erst, wenn das Problem konkret auftritt und übergebe es dann seinem Rechtsanwalt. Die übrigen Provider gaben zu dieser Frage keine Stellungnahme ab.

2..5 Datenschutzgesetz

Das Internet bietet eine Fülle von Informationen, die auf Knopfdruck abrufbar und auch kombinierbar sind. Die Suche nach Informationen ist jedoch nicht nur auf Sachgebiete beschränkt, sondern erfaßt auch User, bzw. User-Gruppen. Jedesmal wenn ein Benutzer im Netz „surft„

hinterläßt sein Client Informationen, welche vom Server der aufgerufenen homepage erfaßt, bzw. verarbeitet werden. Desweiteren bleiben bei jeder Internet-session Verbindungsdaten beim Internet-Provider „hängen„. Es besteht daher prinzipiell die Möglichkeit solche Daten auszuwerten und einer genaueren Analyse zu unterziehen. Desweiteren bedienen sich Firmen spezieller Log-Techniken um ein Mehr an Information über ihre homepage-Besucher zu erhalten. Bedenklich wird es, sobald Unternehmen personenbezogene Daten miteinander verknüpfen, um dann auf Knopfdruck über die Interessenslage von Usern Bescheid wissen. Von Schlagwörtern wie „invasion of privacy„ oder „der gläserne Mensch„ war in letzter Zeit des öfteren zu hören. Uns interessierte im Rahmen unserer Case-study inwieweit spezielle Logtechniken von österreichischen Firmen und Providern eingesetzt werden und inwieweit diese gegen schutzwürdige Interessen, wie sie im österreichischen Datenschutzgesetz normiert werden, verstoßen. Wir wollten auch die prinzipielle Einstellung von Providern und deren Kunden hinsichtlich Logtechniken ausfindig machen.

Prinzipiell sind Internet und Datenschutz vereinbar. Sämtliche im Internet-Betrieb vorkommenden Datenermittlungen, -verarbeitungen und -übermittlungen können unter das österr. Datenschutzrecht subsumiert werden.[6] Zu beachten ist, daß das Datenschutzgesetz (DSG) primär auf Provider-Kunden anzuwenden ist, während für Provider hauptsächlich die Bestimmungen des FernmeldeG gelten, da diese als leges speciales dem DSG vorgehen.

2..5.1 Vermittlungsdaten

Folgende Daten werden standardmäßig von einem bestimmten Client-Rechner bei Aufrufen eines URL (=Uniform Resource Locator) preisgegeben. Übermittelt werden *normalerweise*:

- IP-Adresse
- IP-Nummer
- Name der Maschine
- Betriebssystem
- Art des Browsers

Die IP-Adresse, sowie -number (die laufend neu vergeben wird) sind conditio sine qua non für die Datenübermittlung. Ohne ihre Angabe wäre ein Datentransfer gar nicht möglich. Deren providerseitige Erfassung ist daher nicht nur völlig legal, sondern auch unbedingt notwendig. Jedoch bestimmt §29 FernmeldeG, daß „Vermittlungsdaten„ nur für die Zwecke der Besorgung eines Fernmeldedienstes ermittelt, verarbeitet oder übermittelt werden dürfen, andernfalls ist die

Zustimmung des Betroffenen erforderlich. Vermittlungsdaten sind jene personenbezogenen Daten, die für den Aufbau einer Verbindung, oder für die Verrechnung von Entgelten oder Gebühren erforderlich sind. Unter personenbezogenen Daten versteht man gem. §3 Z1 DSG „die auf einem Datenträger festgehaltenen Angaben über bestimmte, oder mit hoher Wahrscheinlichkeit bestimmbare Betroffene.„ Da Providerunternehmen über die Stammdaten von Personen verfügen und diese zwecks Verrechnung auf Vermittlungsdaten exakt zuordnen können, wäre eine Speicherung letzterer über die Dauer einer Verbindung hinaus ohne Zustimmung des Betroffenen ein Verstoß gegen §29 FernmeldeG.

Wie verhält es sich jedoch, wenn ein Provider-Kunde die Zugriffe auf seinen eigenen Server mitverfolgt ? In diesem Fall kommt das FernmeldeG nicht zur Anwendung, da dieses auf die Betreiber von Fernmeldeanlagen abstellt. Bleibt daher nur noch zu prüfen übrig, ob vielleicht das DSG anwendbar ist. Dieses bezieht sich jedoch auf *personenbezogene* Daten. Die Frage ist, ob durch Kenntnis der Domain (die sich aus der IP-Adresse ergibt) eine konkrete Person schon bestimmbar ist. Dies wird in der Mehrheit der Fälle zu verneinen sein. Die IP-Adresse ist unserer Ansicht nach weniger *personenbezogen*, als viel mehr *domainbezogen* und gewährleistet dadurch im Regelfall noch ausreichende Anonymität. Das DSG kommt daher nicht zur Anwendung. Das bloße Mitloggen der IP-Adresse erscheint daher sowohl für den Provider (für den es unerläßlich für den Betrieb ist), also auch für seine Kunden unbedenklich.
Da die Aussagekraft der oben genannten Informationen für Firmen eher beschränkt ist, bedienen sie sich anderer Techniken um ein Mehr an Information zu erhalten. Als Beispiel seien hier sog. http-cookies näher ausgeführt.

[6] Brandl und Schönberger,ecolex96, 134

2..5.2 Http-Cookies

Wie gefährlich sind Cookies und sind sie datenschutzrechtlich bedenklich?
Zum einen muß man sagen, daß sich der Einzelne ausreichend gegen Cookies „schützen„ kann, indem er einfach nach jeder Sitzung das Cookie-file von seiner Festplatte entfernt. Weiters bietet Netscape die Möglichkeit an, über das Network Preferences Menü jedesmal einen Alarm auszulösen, wenn ein Cookie gesetzt werden soll. Der Benutzer wird dann gefragt, ob er es akzeptiert[10]. Wie sieht die „Cookie-Problematik„ aus datenschutzrechtlicher (österr.) Sicht nun aus? Hier gilt ähnliches wie für die schon zuvor erwähnten standardmäßig übermittelten Browserdaten: Mittels Cookie kann man keine Person identifizieren, sondern nur den Client-Rechner. Damit aber das DSG zur Anwendung käme, müßten gem. §3 Z1 und Z5 *personenbezogene* Daten verarbeitet werden. Im konkreten Fall liegen aber unserer Ansicht nach nur *clientspezifische* Informationen vor und dies alleine ist zu wenig, um eine Person zu konkretisieren bzw. mit hoher Wahrscheinlichkeit zu bestimmen. Desweiteren kann das Cookie immer nur für eine ganz konkrete Domain gesetzt werden und auch nur von einem Server innerhalb dieser wieder abgerufen werden. D.h. es ist nicht möglich Cookies, die von verschiedenen Domains bezüglich der Merkmale eines Clients gesetzt wurden miteinander zu vergleichen. Auch ein Ausspionieren von Konkurrenzfirmen ist dadurch ausgeschlossen.
Cookies für sich alleine genommen dürften also kein datenschutzrelevantes Problem darstellen, jedoch können sie Partner haben. Mittels JavaScripts, welche im html-code einer Homepage „versteckt„ sind, soll es möglich sein auf die Email-Kennung eines Users zu greifen und diese in ein Cookie zu verpacken, jedoch nur wenn Netscape so konfiguriert ist, daß Mails empfangen und abgesandt werden können. Desweiteren eröffneten ältere Netscape Versionen die Möglichkeit direkt mittels JavaScripts auf das Mail-Modul zuzugreifen und die Email-Kennung zu erlangen. Netscape hat ab Version 2.01 diese Sicherheitslücke geschlossen, aber es ist denkbar, daß noch weitere unentdeckte Risiken bestehen[11] . Desweiteren soll auch ActiveX zum selben Ergebnis wie JavaScripts führen.
Wer sich solcher Techniken bedient, begeht unserer Ansicht nach mehrere Vergehen:
Zum Ersten wäre es denkbar, daß man eine solche Vorgangsweise bereits unter Computerkriminalität subsumieren kann, vor allem dann, wenn die Information nicht auf der Festplatte des Clients zwecks späterer Verarbeitung (z.B. persönliche Begrüßung) verbleibt, sondern ohne Zustimmung und Wissen des Betroffenen auf den Server geladen wird.
Desweiteren ist hier unserer Ansicht nach bereits eine Verarbeitung von personenbezogenen Daten gegeben, da mittels Email-Kennung eine eindeutige Zuordnung in der virtuellen Welt

[10] http://www.illuminatus.com/cookie-fcgi
[11] http://www.macworld.com/netsmart

möglich ist. Der Name und die Anschrift in der realen Welt entsprechen der Emailadresse in der virtuellen. Mit dieser Identität bewegt sich jemand in der Cyberwelt: er kauft z.B. Dinge ein, er tut seine Meinung in Newsgroups kund. Desweiteren ist ein bloßes Speichern od. Verknüpfen von Daten gem §3 Z7 DSG bereits als Verarbeiten von Daten zu betrachten. Unserer Meinung nach kommt in diesem Fall das DSG zur Anwendung, welches in §§ 22 und 23 die Registrierung der Datenverarbeitung fordert und welches die Übertragung gem §18 DSG an die ausdrückliche schriftliche Zustimmung des Betroffenen bindet (was wohl nur mittels elektronischer Unterschrift gewährleistet scheint). Das folgende Horrorszenario wäre durch die Verwendung von JavaScripts durchaus denkbar:
Ein österr. Staatsbürger besucht eine lokale Elektronische Shopping Mall und stößt beim Surfen auf eine Ankündigung für einen AIDS-Kongreß im Ort X (vielleicht eine Ankündigung eines Arzneimittelherstellers der in der Mall ebenfalls Verkäufe tätigt). Über diese Ankündigung führt auch ein Link zu einem AIDS-Server, der eine genaue Beschreibung der Konferenz enthält. Der Benutzer verläßt kurzfristig die Mall und folgt diesem Link. Der Server der Shopping Mall notiert diesen Ausstieg samt Email-Kennung dieses Users in einem Cookie-file. Der Benutzer entschließt sich diesen Kongreß zu besuchen und kehrt in den Homeshop-Server zurück, da dort auch ein günstiges Reisebüro anbietet. Schließlich bucht er eine Reise zum Ort des AIDS-Kongresses. Die Zentrale der Shopping Mall führt diese 2 Informationen zusammen (AIDS-Kongreß in X und Buchen einer Reise nach X) und verkauft diese Information an ein Versicherungsunternehmen, bei dem diese Person krankenversichert ist und welches ebenfalls über deren Email-Kennung verfügt. Die Folgen einer solchen Vorgangsweise wären nicht auszudenken. Nicht nur, daß die Methode der Datenerhebung fragwürdig ist, dieser Homeshop-Betreiber verletzt auch die Registrierungspflicht d. Datenverarbeitung gem §§22 und 23 DSG, sowie die Pflicht zur Einholung der Zustimmung des Betroffenen bei Übermittlung von Daten gem. §18 DSG. Benutzt der Shopping-Mall-Betreiber diese Email-Kennung nicht zum Verkauf, sondern für eigene Direct Mail Aktivitäten, so verstößt er möglicherweise gg. §1 UWG, da in der Regel bei Emails noch kein Filtermechanismus besteht, aufgr. dessen man wichtige Mails von Werbungen trennen kann. Die darauf verwendete Zeit und Mühe wirkt geschäftsstörend und ist daher als sittenwidrig zu beurteilen.

Sieht man nun in die Durchführung oben angeführter Praktiken als Verstoß gegen datenschutzrechtliche bzw. strafrechtliche Bestimmungen, so müßte auch der Provider gem. §16 Abs2 Z1 haften, welcher „jede Nachrichtenübermittlung, die die öffentliche Sicherheit und Ordnung gefährdet, *oder welche gegen die Gesetze verstößt*„ zu unterbinden hat. Hier ist wiederum die Interessensabwägung zwischen Z1 (mißbräuchliche Verwendung) und Z3 (Geheimhaltungspflichten) vorzunehmen. Bei Anbieten einer Homepage im WWW geht es gerade darum möglichst viele Interessenten zu erreichen, daher treten analog zu Newsgroups Geheimhaltungspflichten (Z3) in den Hintergrund. Es wird also hier der Provider gefordert sein,

solche tracking-Techniken unter dem Gesichtspunkt der Verhältnismäßigkeit zu unterbinden. Daher sollte zumindest eine Warnung an die Kunden erfolgen, durch die auf eine eventuelle Gesetzeswidrigkeit solcher Praktiken hingewiesen wird (wie bei unmoderierten Newsgroups). Wenn ein Kunde, der diese Techniken anwendet, sich einen Platz am Server des Providers anmietet, also dessen Server benutzt, so ist fraglich, ob §29 FernmeldeG, welches normiert, daß Vermittlungsdaten ohne Zustimmung des Betroffenen nicht über die Dauer einer Verbindung gespeichert werden dürfen, nicht auch den Kunden miterfaßt; man also die Aktivitäten des Kunden der Sphäre des Providers zuordnen kann. Unserer Meinung nach wird dies zu verneinen sein, da das FernmeldeG eindeutig die Nachrichtenübertragung für Dritte im Auge hat und Vermittlungsdaten als *„Daten, die für den Aufbau einer Verbindung, oder für die Verrechnung von Entgelten erforderlich sind*„ definiert sind. Daher ist §29 FernmeldeG unserer Meinung nach ausschließlich auf Provider anzuwenden.

2..5.3 Newsgroups

Unter http://dejaNews.com/forms/authprof.html ist es möglich durch Eingabe einer Email-Kennung sämtliche Newsgroups ausfindig zu machen, in denen ein User subskribiert hat. Auch mittels dieser Einrichtung scheint es möglich, Interessenslagen von individuell konkretisierbaren Personen ausfindig zu machen. Unserer Meinung nach ist aber nicht das öst. DSG anzuwenden, da sich die Newsgroups in der Regel auf amerikanischen Servern befinden, die dann lokal heruntergeladen werden Jedoch könnte man sich ein Szenario vorstellen, bei dem dieses Service lokal angeboten wird und nur österr. Newsgroups übertragen werden. Unserer Ansicht nach treten bei Publizieren in Newsgroups Geheimhaltungspflichten stark in den Hintergrund, da es dem Autor gerade darum geht, in der Öffentlichkeit seine Meinung kundzutun. Jedoch muß man damit rechnen, daß über die Email-Kennung auf Newsgroups zugegriffen wird? Es gab vor mehreren Jahren nach Auskunft des Justizministeriums einen Fall von datenschutzrechtlicher Relevanz, bei dem jemand ein österreichisches Telefonbuch elektronisch erfaßte und danach über Straßennamen auf Personen zugriff. Diese Praktik wurde damals als bedenklich eingestuft, da hier durch die Zugriffsmöglichkeit über Straßennamen eine neue Qualität geschaffen wurde, die nicht mehr mit den ursprünglichen Möglichkeiten eines normalen Telefonbuches übereinstimmte. Derjenige, der auf eine Geheimnummer verzichtet und sich ins öffentliche Telefonbuch eintragen ließ, mußte nicht davon ausgehen, daß er über einen Straßennamen ausfindig zu machen sei. Heute ist beim elektronischen Telefonbuch ein Zugriff über Straßennamen und Eingabe des Anfangsbuchstabens d. Familiennamens durchaus möglich, daher muß heute jeder, der sich neu ins Telefonbuch eintragen läßt auf andere Zugriffsmöglichkeiten gefaßt sein. Dasselbe gilt unserer Meinung nach auch für Newsgroups (und Abfrage mittels Email-Kennung) im Internet: Der Autor, der freiwillig seinen Artikel und Email-Kennung der Öffentlichkeit bekannt gibt, muß mit anderen Zugriffsmöglichkeiten (als über das Sachgebiet) rechnen. Das DSG ist unserer Meinung nach nicht

anwendbar, da dieses auf schutzwürdige Interessen von Beteiligten abzielt, was in §17(1) zum Ausdruck kommt. Beim Publizieren in Newsgroups ist dieses Schutzinteresse wohl nicht mehr gegeben, darüberhinaus muß mit der Möglichkeit einer anderen Zugriffsart als über das Sachgebiet bei dem heutigen technischen Entwicklungsstand gerechnet werden.

2..5.4 Case-Study

Folgende Fragen richteten wir im Rahmen unserer Case-study hinsichtlich datenschutzrechtlicher Problembereiche an Provider und deren Kunden. Fragen 1, 4 und 5 wurden ausschließlich an Provider gestellt, während Fragen 2 und 3 entsprechend umformuliert auch an Providerkunden gestellt wurden.

Frage:
§29 FernmeldeG bestimmt, daß Vermittlungsdaten nur für die Dauer einer Verbindung gespeichert werden dürfen. Bezieht sich dieses Gesetz ausschließlich auf Provider, oder sind auch Ihre Kunden hiervon erfaßt, wenn sie Vermittlungsdaten speichern (z.B. mittels Browser-Cookies, oder sonst irgendwie mitloggen)? Ist der Provider für seine Kunden haftbar, die sich mittels besonderer Techniken personenbezogene Daten von Homepage-Besuchern besorgen und diese dann auswerten bzw. unerlaubt weitergeben?

Antworten:
Zwei der von uns befragten Provider zeigten kein besonderes Interesse an dieser Fragestellung. Der eine meinte man beschäftige sich mit diesem Problem erst, wenn es auftritt und dann wird der Rechtsanwalt kontaktiert. Der andere schloß eine Haftung des Providers für seine Kunden prinzipiell aus, ohne dies begründen zu können, oder zu wollen. Ein dritter Provider betonte vor allem die Vorteile von Logtechniken bzw. Cookies für den Kunden. Er konnte überhaupt keine datenschutzrechtliche Relevanz erkennen und entgegnete unseren juristischen Fragen eher mit technischen Antworten. Zum Beispiel werden keine personenbezogenen Daten erfaßt, weil dies für den Provider aufgr. Kapazitätsverlusten technisch und wirtschaftlich nicht sinnvoll sei (nicht etwa weil er einen Verstoß gg. das DSG befürchte). Da solche Techniken für ihn unproblematisch erschienen, verneinte er natürlich auch eine providerseitige Haftung für Kunden, welche auf dem Server des Providers mitloggen. „Auf dem eigenen Server ist es unproblematisch mitzuloggen, wenn dies auf dem Server des Providers geschieht, dann soll dies strafbar sein?„ Ein weiterer Provider sah die Problematik etwas differenzierter: Er war der Auffassung, daß Daten die mittels Cookies erfaßt und übertragen werden sehr wohl der Zustimmung des Betroffenen bedürfen. Er geht davon aus, daß dies in 99 % der Fälle nicht der Fall sei und daß damit ein echtes DSG-Problem besteht. Eine Haftung des Providers für seine Kunden konnte er jedoch nur dort erkennen, wo Provider solche Techniken als Serviceleistung ihren Kunden anbieten. Soweit

Kunden ihren eingeräumten Platz dazu „mißbrauchen„ kann er keine Haftung des Providers erkennen. Seine Argumentationsweise entsprach jener, der weiter oben beschriebenen Haftung als reiner „Access Provider„. Desweiteren werden Kunden angeblich in regelmäßigen Abständen über die Problematik derartiger Log-Techniken informiert. Abrechnungsrelevante Daten - das sind die Modem-Einwahlzeiten (Beginn, Dauer, Ende der Verbindung) - bleiben bis zum Ende des Kundenvertrages gespeichert, da noch nicht klar ist, wie lange realistischerweise mit Einsprüchen zu rechnen ist.

Frage:
Inwieweit empfinden sie oben erwähnte „tracking„-Techniken als datenschutzrechtlich bedenklich und bieten sie solche Möglichkeiten Ihren Kunden an?

Antworten::
Bis auf einen Provider, der das Problem zur Gänze ignorierte und der bereits unter Frage 1 beschrieben wurde, erkannten alle von uns befragten Provider eine prinzipielle datenschutzrechtliche Problematik von Log-Techniken. Zwei der befragten Provider bieten solche Techniken überhaupt nicht für ihre Kunden an. Einer dieser zwei Provider hält diese Techniken insofern für bedenklich, als der Internetbenutzer davon in Kenntnis zu setzen sei und er Möglichkeiten erhalten sollte, sich wirksam auf Wunsch dagegen zu schützen. Die übrigen Provider bieten solche Services jedoch ihren Kunden an. Ein Provider betonte jedoch ausdrücklich, daß dies nur in anonymisierter Form geschehe. Ein anderer erklärte Auswertungen würden nur in aggregierter Form vorgenommen werden und nur insoweit, als nicht gegen das DSG vorstoßen wird. Angeblich mußten sogar schon einzelne Anfragen abgewiesen werden. Sämtliche von uns auf diese Frage angesprochenen Firmen gaben zu, Logfiles über ihre Kunden angelegt zu haben. Jedoch wurde mit diesen Firmen keine datenschutzrechtliche Diskussion geführt, da oft unsere Ansprechpartner oftmals über juristische Belange wenig Ahnung hatten, bzw. Sicherheitsfragen ihren Providern überlassen.

Frage:
Welche Internet-Browser werden von Ihren Kunden verwendet und welche Daten geben diese standardmäßig bei Aufrufen einer Homepage preis?

Antworten:
Nach Auskunft eines Providers werden folgende Daten standardmäßig vom Browser abgegeben (wie schon weiter oben erwähnt):

- IP-Adresse
- IP-Nummer

- Name der Maschine
- Betriebssystem
- Art des Browsers

Die IP-Adresse und IP-Nummer (welche jedesmal neu vergeben wird) seien unbedingt notwendig für den Datentransfer. Die übrigen Daten *können* eingetragen werden.
Zwei weitere Provider gaben an, nur die IP-Adresse mitzuloggen. Ein dritter Provider meinte es interessiere ihn nicht, es sei auch nicht sein Geschäft. Hinsichtlich der Frage nach den verwendeten Internet-Browsern wurden uns hier providerseitig nur vage Angaben gemacht: z.B. „Unsere Kunden verwenden irgendwelche Browser„, oder „wir stellen einige übliche Browser als Kopie auf unserem ftp-Server zur Verfügung„. Bezüglich der verwendeten Browser von Providerkunden möchten wir auf den technischen Teil unserer Arbeit verweisen.

Frage:
Gerüchten zufolge soll es die Möglichkeit geben, in der html einer Homepage java-scripts einzubauen, die dann vom jeweiligen Netscape-Browser mitverarbeitet werden und die bewirken, daß auf die Emailadresse eines Surfenden zugegriffen werden kann, wenn Netscape so konfiguriert ist, daß Emails empfangen und gesendet werden können. Dem zweiten Gerücht zufolge soll der Internet-Explorer von Microsoft automatisch die Email-Kennung auf WWW-Server hinterlassen. Inwieweit können sie mir diese Gerüchte bestätigen oder dementieren?

Antworten::
Ein Provider konnte mir diese beiden Gerüchte definitiv bestätigen. Ein anderer meinte nur, daß er schon davon gehört habe. Die übrigen konnten zu dieser Frage keine Auskunft geben. Jedoch sei es prinzipiell, nach Aussagen von 2 Providern, technisch überhaupt kein Problem die Email-Adresse eines Users zu ermitteln und diese zu verarbeiten. Ein weiterer Provider gab jedoch zu bedenken, daß im Regelfall ein user nicht über eine, sondern durchschnittlich über drei Email-Kennungen verfüge und dadurch eine eindeutige Zuordnung von Daten zu einer konkreten Person nicht mehr so einfach wäre.

Frage:
Über http://dejaNews.com/forms/authprof.html ist es möglich sämtliche Newsgroups ausfindig zu machen, in denen ein bestimmter User subskribiert ist. Gibt es bei Ihnen ebenfalls diese Möglichkeit und wie würden sie diese datenschutzrechtlich bewerten?

Anworten:
Ein befragter Provider stuft diese Problematik nicht als dramatisch ein, da viele Autoren mittels Nicknames schreiben, die sich laufend ändern lassen. Desweiteren würden die Newsgroups zu

einem großen Teil für den Austausch von Pornographie und Raubkopien (z.B. die ersten 30 Tage bei AOL) mißbraucht und es ließe sich daher kein detailliertes Persönlichkeitsprofil von einer konkreten Person ausfindig machen. Ein anderer Provider war der Ansicht, daß man die oben skizzierte Problematik weniger mit einer Bibliothek vergleichen soll, bei der man über einen Namen sämtliche Bücher ausfindig machen kann, die sich Jemand ausgeborgt hat, sondern eher mit einer Liste aller Werke eines bestimmten Autors. Ein dritter Provider war der Ansicht, daß ein solches Programm in Österreich nur zulässig wäre, wenn

- die eigene Adresse abgefragt wird, oder
- der Betroffene eingewilligt hat, oder
- gesetzliche Bestimmungen einen derartigen Abruf erlauben würden, oder
- dies für die Erreichung bestimmter gesetzlicher Aufgaben unbedingt notwendig wäre (z.B. Strafverfolgung, oder Sicherheit des Landes)

Ein weiterer Provider meinte, daß diese Möglichkeit bei ihm nicht angeboten werde, er aber diese Möglichkeit als nicht sehr schlimm einstufe, da es sich bei Newsgroups um öffentliche postings handle.

2..5.5 Zusammenfassung

Im Rahmen unserer Case-study begegneten wir einer permanenten Rechtsunsicherheit unter den befragten Firmen, wie auch unter den Providern. Die Hauptprobleme sind:

1) Anwendung und Auslegung bestehender Gesetze auf das Internet

Aufgrund fehlender OGH-Entscheidungen betreffend „neuer Medien„ sind Unternehmer gezwungen, selbst juristisch tätig zu werden und bestehende Gesetze anzuwenden bzw. auszulegen. Oft ist dies jedoch mit erheblichen Schwierigkeiten verbunden, da man beim Gesetzesentwurf diese Medien und deren spezifische Auswirkungen nicht als regelungsbedürftig ansah. Ein Beispiel hierfür ist das Fernmeldegesetz, welches ua. für die Haftung von Providern bei Übertragung strafrechtlich bedenklicher Inhalte anzuwenden ist. Das Problem hierbei ist, daß sich dieses Gesetz in seinem Wortlaut und Formulierungen in erster Linie auf die Betreiber von Telefonanlagen bezieht. Für Provider ergeben sich dadurch erhebliche Auslegungsschwierigkeiten. Zum einem waren sich bei unserer Befragung viele Provider gar nicht sicher, ob das FernmeldeG sie überhaupt erfaßt, zum anderen gibt es Auslegungsschwierigkeiten von bestimmten Begriffen. z.B. „was gilt als Pornographie?„ Hierzu soll es jetzt innerhalb der EU Bestrebungen geben, solche Begriffe genau festzulegen.

2) Internationalität des Internets versus nationaler Gesetzgebung

Weitere Schwierigkeiten ergeben sich aus der Tatsache, daß nationale Gesetze auf ein globales Netzwerk angewendet werden sollen. Welches Gesetz soll gelten, wenn überregionale Vereinbarungen und int. Standards fehlen ?

3) Rechtliche Durchsetzbarkeit

Selbst wenn man erkennt, daß ein Internet-spezifisches Problem geregelt ist und welches nationale Gesetz zur Anwendung kommt, ergibt sich immer noch das Problem der internationalen Rechtsdurchsetzbarkeit. Obwohl die Frage der Anwendbarkeit nationaler Gesetze und deren int. Durchsetzbarkeit auch außerhalb des Internets problematisch ist, so tritt es innerhalb des Netzes, bedingt durch seine globale Struktur, besonders kraß auf.

Im Laufe unserer Interviews gewannen wir den Eindruck, daß zwar versucht wird, auf bestehende Gesetze im Zusammenhang mit Internet Rücksicht zu nehmen, die praktische Umsetzung sich jedoch sehr schwierig gestaltet. Jede Firma macht im Prinzip das, was der hauseigene Jurist für richtig hält und dies variiert von Unternehmen zu Unternehmen. Gemeinsamkeiten ergeben sich nur bezüglich des Wartens auf internationale Standards und der Scheu größere Geschäfte übers Netz abzuwickeln. Der letzte Punkt kann als Indikator für die herrschende Unsicherheit gesehen werden.

Bei den Interviews, die wir führten, hörten wir auch die Meinung, daß das Internet ein rechtsleerer Raum sei, oder, daß im Gegenteil sämtliche Möglichkeiten als legal befunden wurden, da jeder der sich ins Internet begibt sich seiner Gefahren und der technischen Möglichkeiten bewußt sein muß. Wir gewannen auch den Eindruck, daß die konkrete Ausgestaltung des Internets weniger durch gesellschaftliche Wertvorstellungen und Normen, als vielmehr durch die technische Machbarkeit bzw. Sinnhaftigkeit geformt wird. z.B. ergibt sich die Tatsache, daß Provider Vermittlungsdaten so bald wie möglich löschen nicht aus §29 FernmeldeG, sondern aufgrund von Kapazitätsengpässen bei einer etwaigen Speicherung.

3. Organisation der Sicherheit

3..1 Einleitung

Mit zunehmender Unternehmendgröße, steigender Sensibilität der gespeicherten Daten und vorallem mit der Vernetzung steigt das Sicherheitsrisiko in Unternehmen.

Laut einer Untersuchung die im Mai 1995 von der National Computer Security Association in den USA durchgeführt wurde 4, sind Unternehmen mit Internet-Anschluß im Vergleich zu nicht vernetzten Unternehmen einem achtmal höheren Angriffsrisiko ausgesetzt.

Durch ein Eindringen von nichtautorisierten Personen in das Unternehmensnetzwerk kann bedeutender finanzieller Schaden durch einen Verlust an Daten und an vertraulicher Information oder durch Einschleppen von Viren entstehen.

Um diesem Sicherheitsrisiko effizient begegnen zu können, ist es nötig, ein unternehmensweites Sicherheitskonzept zu erstellen. In diesem Sicherheitskonzept sollten für alle Mitarbeiter Richtlinien für die ordnungsgemäße Benützung der EDV-Systeme und des Netzwerkes beschrieben werden. Weiters sollen die Aufgaben und Kompetenzen der zu ernennenden Sicherheitsbeauftragten und Systemadministraroren klar festgelegt werden.[5]

Sinnvollerweise wird die Erstellung des Sicherheitskonzeptes von Mitarbeitern der EDV-Abteilung und vom Management übernommen. Die EDV-Mitarbeiter haben den Überblick über die technischen Möglichkeiten und Gefahren, die im Unternehmen derzeit gegeben sind. Das Management ist hauptsächlich dafür verantwortlich, daß sie im gesamten Unternehmen ein Klima des Sicherheits- und Problembewußtseins schaffen. Weiters muß das Management dafür sorgen, daß die Sicherheitsrichtlinien allgemein akzeptiert und eingehalten werden.

Die Aufklärung der Mitarbeiter in Sicherheitsbelangen ist von zentraler Bedeutung, da die „Menschlichkeit“ ein erhebliches Sicherheitsrisiko darstellt. Laut Untersuchungen von Ernst & Young, die 1271 Unternehmen in den USA befragt haben[6], gehen cirka zwei Drittel der Fälle in denen Unternehmen finanzielle Verluste aus einem Problem der Informationssysteme tragen mußte, auf das Konto der Mitarbeiter. In der Hälfte aller Fälle geschehen diese Attacken unabsichtlich bzw. aus mangelnder Fachkenntnis, die andere Hälfte der Fälle wird Racheakten zugeschrieben.

[4] Kyas, Sicherheit im Internet, S 20 f

Dies verdeutlicht nochmals wie wichtig es für ein Unternehmen ist, ein einheitliches Sicherheitskonzeptes zu formulieren und es in alle Bereiche des Unternehmens einzubinden.

3..2 Risikoanalyse

3..2.1 Allgemein

Mit Hilfe von Risikoanalysen kann quantifziert werden, in welchem Ausmaß das Internet eine Gefährdung für ein Unternehmen darstellen kann.
Sie können allgemein in die Phase 1 „Beschreibung das Analysebereichs„, in die Phase 2 „Erfassung des Risikos„, in die Phase 3 „Bewertung des Risikos„ und in die letzte Phase „Auswertung der Ergebnisse„ eingeteilt werden.[7]
Um zu einer ersten Abschätzung der Folgen von Sicherheitsvorfällen bedingt durch einen Internet-Zugang zu gelangen, können die Kosten für die Beeinträchtigung des Netzwerkbetriebs sowie von Datenintegritätsverlusten herangezogen werden. Netzausfälle sind mit Kosten verbunden, und so konnte während der vergangenen zehn Jahre ein stetiger Anstieg der resultierenden Kosten beobachtet werden.
„Obwohl die durchschnittliche Anzahl der Ausfallstunden für Datennetze aufgrund von stabileren Bestriebssystemen und höherwertiger Hardware pro Jahr auf etwa ein Zehntel des Wertes von vor zehn Jahren zurückgingen, stiegen die damit verbundenen Kosten deutlich an. Grund dafür ist die heute weitaus größere Abstützung der Unternehmen auf die Technologien der Datenkommunikation. Betrugen die durchschnittlichen Kosten für einen Netzwerkausfall 1989 lediglich etwa 3.500 $/Stunde, so stieg dieser Wert bis 1993 bereits auf mehr als 52.000 $/Stunde an.„[8]

3..2.2 Case-Study

Fragen:

---

[5] Kyas, Sicherheit im Internet, S122f
[6] Kyas, Sicherheit im Internet, S 19
[7] Theoretische Erläuterungen zu diesen Phasen entnehmen sie aus: Kyas, S. 22 ff
[8] http://www.cs.rpi.edu/ifip, 22. Nov. 1996

Wegen dieser oben angeführten enormen Kostensteigerung bei Netzwerkausfällen und der Tatsache, daß heute bereits jeder zweite Firmen-PC an ein Netzwerk angeschlossen ist[9], wollten wir von den Unternehmen wissen, ob und wenn ja, wie eine Risikoanalyse vor einer Netzanbindung durchgeführt wird. Um die Kosten von Netzwerkausfällen abschätzen zu können, erschienen uns zusätzlich die Fragen nach der Ausfallsrate der EDV-Anlage und nach der Aufdeckungsquote von Hacker-Attacken wichtig.

Antworten:
Unsere Umfrage bei den Firmen ergab, daß fast alle EDV-Abteilungen eine solche Risikoanalyse vor dem Internetzugang angeblich durchgeführt haben, jedoch die Daten dem Betriebsgeheimnis unterliegen würden. Wahrscheinlicher erscheint uns, daß diese Risikoanalyse ebenfalls dem Provider übertragen wurde bzw. wird.
Konkret wird von EUNET ein sogenanntes „Security Consulting„ angeboten, deren Aufgabe es ist, die Sicherheitsanforderungen des Kunden festzustellen. Nicht nur von Experten des Providers, sondern im Team mit Netzwerktechniker und/oder Sicherheitsadministratoren des Kunden werden solche Anforderungsprofile erstellt und ein Lasten/Pflichtenheft erarbeitet. Danach wird entschieden, welches Sicherheitssystem (Hardware und Software) umgesetzt wird. Lesen Sie mehr über „Security Consulting„ in dem Kapitel TECHNIK unter dem Punkt *Case-Study* .

Konfrontiert mit der Frage nach Hackern, herrschte bei den befragten Unternehmen der Grundton, daß eine Firewall ausreichend Schutz bietet. Lediglich ein Unternehmen formulierte es folgendermaßen: „Wenn ein Hacker es darauf anlegt reinzukommen, dann wird er es auch schaffen! Eine 100%-ige Sicherheit gibt es nicht!“

Die befragten Unternehmen reagierten unterschiedlich auf die Frage, ob sie Angriffe bemerkten. Ein Unternehmen sprach von 60-80 Tausend Angriffen, alle anderen sahen sich jedoch davon verschont oder sprachen von lediglich 1 oder 2 erfolglosen Versuchen. Vor allem im Bankensektor war man versucht, Hacker ins Reich der Mythen einzuordnen und „es wäre ja ohnedies sinnlos, da die verwendeten Onlinesysteme sicher seien“. Dagegen spricht jedoch eine Studie des Magazins „Konsument“ , welche 8 Bankinstitute und ihr Onlinekonto auf Schwachstellen testete. Bei 6 Bankinstituten gelang es, unauthorisiert Abbuchungen zu tätigen. Fairerhalber sei aber erwähnt, daß die beiden von uns befragten Banken, welche ein Online-Banking anbieten, den Test bestanden haben.
Lediglich eine befragte Bank ließ sich durch eine externe Organisation einem Test unterziehen und bestand diesen Test.

[9] Kyas, S. 25

Ein Bankinstitut sprach davon, daß absolute Sicherheit um jeden Preis vorhanden sein müsse. Sollten Zweifel bestehen, verzichte man lieber auf eine Internetpräsenz. Seit kurzem (Januar 1997) bietet diese Bank ebenfalls ein Online-Banking an. Nur 2 Wochen nach unserem Gespräch.

Bei den Providern herrschte der Grundton, daß ihre Sicherheitssysteme (z.B. Firewall, VPN) höchstmögliche Sicherheit bieten. Speziell bei VPNs wird eine hundertprozentige Sicherheit versprochen. Weiters war festzustellen, daß sich die Provider selbst im höchsten Maße mit Sicherheitseinrichtungen, sei es technischer oder organisatorischer Natur, einigeln. Angriffe wurden registriert, blieben jedoch stets erfolglos. Daher ist vielleicht auch das beinahe blinde Vertrauen der Kunden in den Provider („Pfarrer und Arzt in einer Person„) verständlich. Vielleicht auch, weil man die Gefahr vor allem im eigenen Unternehmen sucht und nicht beim Provider.

3..2.3 Zusammenfassung

Wenn Sicherheit ein Verkaufsargument ist, spricht man nicht gerne über Angriffe, da das Unternehmen befürchtet, an Image zu verlieren. So mag zu erklären sein, daß das Unternehmen, welches von einer großen Zahl von Angriffen sprach, nicht im Kundengeschäft tätig ist.

3..3 Verantwortlichkeit für die Umsetzung

Wie bereits in der Einleitung zur Organisation verdeutlicht, spielt die EDV-Abteilung bei der Überwachung und Implementierung des Sicherheitskonzeptes eine wichtige Rolle.

3..3.1 Case-Study

Frage:

Wir wollten deshalb mehr über die Organisation der EDV im Unternehmen und die Eingliederung in die Unternehmenshierarchie herausfinden. Darüberhinaus wollten wir genaueres über die Kompetenzen und Zuständigkeiten der EDV-Abteilungen erfahren.

Antworten:

In allen großen untersuchten Unternehmen, seien es Banken oder Dienstleistungsunternehmen, ist die EDV eine eigene Abteilung, die direkt dem Vorstand bzw. der Geschäftsleitung unterstellt ist.

Lediglich bei einem Ministerium, einem Second-Hand-Anbieter und einem virtuellen Geschäft war keinen klare Struktur erkennbar.

Bei den Providern wird die Arbeit in Form von Projektgruppen durchgeführt, in denen gemeinsam mit dem Kunden ein geeignetes Sicherheitskonzept erarbeitet wird. Im Ministerium ist die EDV als Stabstelle organisiert, die langsam gewachsen ist. Die Aufgaben der EDV reichen von der strategischen Planung, der Entwicklung eigener Applikationen, Hard- und Softwarebeschaffung über Wartung und Service bis zur Schulung der Mitarbeiter.

Ganz ausgeprägt ist die EDV-Struktur bei einem großen Unternehmen der Kommunikationsbranche. In diesem Unternehmen gibt es eine EDV-Abteilung, die für Finanz und Rechnungswesen zuständig ist und eine ADV-Abteilung (Allgemeine Datenverarbeitung) mit 50 Mitarbeitern, die sich wieder in zwei Unterbereiche gegliedert: Forschung & Entwicklung und „technischer support„. Im Rahmen der „support-Gruppe„ gibt es unter anderem eine Netzwerkabteilung für das interne Netz und eine Internetabteilung, in der fünf Mitarbeiter beschäftigt sind. Zusätzlich existiert eine Internet-Projektgruppe, in der sowohl ADV- als auch Marketingspezialisten mitarbeiten.

Bei einer österreichischen Großbank, in der die EDV auch direkt dem Vorstand unterstellt ist, sind starke Tendenzen in Richtung Outsourcing auf Tochterunternehmen erkennbar. Die Mitarbeiterzahl schrumpfte von 80 auf 40 Personen. Die EDV Abteilung ist für alle EDV-bezogenen Wünsche und Anfragen der Fachabteilungen zuständig. Sie liefert den Fachabteilungen ein detailliertes Kosten /Nutzen Profil aufgrund dessen die Fachabteilungen dann über die Realisierung entscheiden. Die Kosten setzen sich zusammen aus benötigter Hardware, Software

und den sich daraus ergebenden laufenden Wartungskosten. Die gesamten Kosten müssen von den jeweiligen Fachabteilungen getragen werden.

Die Internetseiten für alle Abteilungen werden von der Marketingabteilung erstellt und gewartet. Die EDV Abteilung sorgt nur für den File Transfer zum Server des Providers. Die Funktion des Internetproviders wird von einem Tochterunternehmen wahrgenommen, allerdings soll ein eigener Server im Haus installiert werden.

Bei einer anderen Bank untersteht die EDV dem stellvertretenden Generaldirektor, umfaßt 85 Mitarbeiter und ist für den problemlosen Betrieb der Informationssysteme und für die Entwicklung zuständig. Es wird auch ein Logbuch geführt und es gibt eine Stelle, bei der ungewöhnliche Vorfälle die EDV betreffend gemeldet werden.

Bei einem österreichische Kozern gibt es eine zentrale EDV-Einheit, die für die Administration der gesamten EDV zuständig ist und auch für das Inter- und Intranet verantwortlich ist. Besonderes Augenmerk wird auch auf einen einheitlichen Aufbau und eine gemeinsame Grundstruktur der angebotenen Inhalte gelegt. Abteilungsübergreifende Arbeitskreise sorgen zusätzlich für die Koordination der Informationen im Netzwerk.

Frage:

Da sich für das Unternehmen mit der Anbindung ans Internet bezüglich Sicherheit viele Änderungen ergeben, haben wir auch untersucht, wer im Unternehmen mit der Internetanbindung zu tun hat und wie die Anbindung vor sich ging.

Antworten:

Die Initiative für eine Präsenz im Internet geht laut Aussagen der Provider, die auch von uns bestätigt werden konnten, meist entweder vom Vorstand oder von der Marketingabteilung aus. Die Marketingabteilungen sehen das Internet zunehmend als innovatives Medium für Werbung, Information,Verkauf, PR und Kundenservice. Man erwartet sich die Erschließung eines neuen Marktes, neue Zielgruppen, standortunabhängige Präsenz für den Kunden, einen Dialog mit den Kunden und dadurch auch Information über den Kunden, Imagevorteile gegenüber der Konkurrenz und vieles mehr.[10] Aus diesem Grund haben die Marketingabteilungen auch das stärkste Interesse an einer Internetanbindung.

Geht die Initiative hauptsächlich von der Unternehmensleitung aus, dann beteiligt sich diese laut Provideraussagen auch sehr stark am ganzen Projekt der Einbindung um die dadurch ausgelösten Auswirkungen auf das ganze Unternehmen bestmöglich verstehen zu können.

[10] Hansen, Wien 1996, 120

Die EDV-Abteilung initiiert eine Internetpräsenz eigentlich nie. Ein Grund dafür dürfte wohl die große Belastung sein, der diese Abteilung in den meisten Unternehmen sowieso schon ausgesetzt ist. In einem Unternehmen haben wir allerdings die Information bekommen, daß die Initiative für ein Intranet, in weiterer Folge auch für das Internet, von der EDV Abteilung ausgegangen ist.

Hat sich das Unternehmen für einen Internet-Zugang entschieden, wird meistens eine Projektgruppe zusammengestellt. Diese Gruppe besteht, wie bei der vorigen Frage schon beschrieben, immer aus Mitarbeitern der EDV und der Marketingabteilung, zum Teil sind auch noch Vertriebsfachleute miteinbezogen. In Kooperation mit der Marketingabteilung plaziert die Projektgruppe die Angebote im Netz und versucht auch auszuloten, welche sichere Transaktionsmöglichkeiten genützt werden können.

Bei einer österreichischen Fluglinie zum Beispiel stellt die Marketingabteilung nur die aktuellen Inhalte und Daten zur Verfügung. Eine EDV Beauftragte aus der Projektgruppe hat die Aufgabe der Umsetzung und der täglichen Wartung der Internetseiten. In letzter Zeit wird auch damit begonnen, Daten von anderen Abteilungen außer der Marketingabteilung in die Präsentation miteinzubeziehen.

In einer untersuchten Bank wird nur der File Transfer auf den Server von der EDV-Abteilung durchgeführt. Die Erstellung und die Wartung der Seiten wird von der Marketingabteilung übernommen, von der auch der Wunsch nach einer Präsenz im Internet ausging. Diesem Wunsch haben sich dann Abteilungen, die externe Kundenbetreuung durchführen, angeschlossen.

Frage:

Gibt es im Unternehmen ein einheitliches Sicherheitskonzept und wer war für die Erarbeitung der Sicherheitsstandards verantwortlich?

Antworten:

Bezüglich der Sicherheitsstandards haben wir beobachtet, daß gänzlich verschiedene Konzepte umgesetzt werden. Die Bandbreite reicht von praktisch keinem Sicherheitsbewußtsein bis zur Sicherheit, die über alles gestellt wird und ist abhängig von Unternehmensgegenstand, Unternehmensgröße, dem Grad der internen Vernetzung und der Sensibilität der Daten.

Bei einem Anbieter von Second-hand Waren und einer virtuellen Shopping Mall ist das Thema Sicherheit absolut zweitrangig und man findet, daß der Sicherheit zu große Bedeutung beigemessen wird, jedenfalls im eigenen Bereich. Man überlegt derzeit gerade, ob man die Kreditkartennummern der Kunden verschlüsseln sollte, bzw im letztgenannten Unternehmen „denkt man über Sicherheit nicht einmal nach„.

In einem Bereich der öffentlichen Verwaltung kommt man derzeit noch mit Passwortvergabe und einer Firewall aus, die in der Abteilung selbst betrieben wird. Allerdings sieht man für die Zukunft ganz klaren Handlungsbedarf bezüglich eines guten Sicherheitskonzeptes

Ein Flugunternehmen verläßt sich bei den Sicherheitsfragen sehr auf den Provider, der das gesamte Handling übernimmt und bei dem man sich auch über die neuesten Entwicklungen auf diesem Gebiet informiert.

In einem Lebensmittel-Handelsunternehmen gibt es ein allgemeines Sicherheitsbewußtsein, Risikoanalysen werden permanent durchgeführt, das Netz wird durch eine Firewall abgesichert, Zugriffsberechtigungen werden von Funktionsvorgesetzten vergeben und von der EDV Abteilung kontrolliert. Einige Internet-Dienste (z.B. WWW) sind nur mit eigener Genehmigung verfügbar.

Bei den international agierenden Computer- und Softwarekonzernen und den Banken wird ausnahmslos auf konzernübergreifende Sicherheitsstandards, die von eigenen Sicherheitsgruppen und Arbeitsgemeinsschaften ausgearbeitet werden und ständig aktualisiert werden, zurückgegriffen. Teilweise gibt es Basisrichtlinien, an die sich der ganze Konzern halten muß, die aber dann bei verschiedenen Projekten je nach Projektanforderung noch verschärft werden. Verstöße gegen diese Richtlinien werden speziell in einem Unternehmen rigide bestraft. Die Verstöße werden aus Gründen der Abschreckung und Prävention im Unternehmen veröffentlicht.

3..3.2 Zusammenfassung

Das sehr unterschiedliche Bild, das uns bei der Befragung in diesem Bereich auf den ersten Blick bot, wird einheitlicher, wenn man die Unternehmen nach Kriterien wie Unternehmensgröße, Unternehmensgegenstand oder Art der Daten zusammenfaßt. Die Forderung eines Industrieunternehmens, daß jeder nur in dem Ausmaß für Sicherheit sorgen solle, wie es für das Unternehmen sinnvoll sei, scheint sich mit unseren Befragungen zu decken.
Dieses sinnvolle Maß festzulegen dürfte aber für die Unternehmen sehr schwer sein, da die wenigsten von ihnen die drohenden Gefahren richtig einschätzen können (vergleiche mit dem Punkt *Risikoanalyse* zu Beginn des Kapitels). Daher muß eher bezweifelt werden, daß die Unternehmen über genügend Sicherheitsvorkehrungen verfügen.

3..4 Outsourcing vs. interne Abwicklung

3..4.1 Allgemein

Mögliche Bereiche, die Unternehmen auslagern können sind folgende:

der Betrieb und die Implementation einer Firewall, die Web-Administration, und der Betrieb von Mail-Servern und File-Servern.

Unternehmen, die ein Outsourcing übernehmen haben wir gemäß dem allgemeinen Sprachgebrauch in Internet-Service-Provider und Content-Provider unterteilt, wobei aber häufig eine Überschneidung der Aufgaben zu bemerken war. Die Internet-Service Provider stellen den Internetanschluß an sich bereit, während die Content-Provider für die inhaltliche Gestaltung der Seiten und auch für das allgemeine Sicherheitskonzept sorgen.

3..4.2 Case Study:

Frage:

Welche Vorteile und Gefahren sind aus Sicht der Unternehmen mit dem Outsouring der Internetanbindung und der Sicherheitkonzepte verbunden, welche Bereiche werden outgesourct und welche Dienstleistungen bieten die Provider an ?

Antworten:

Vorallem für mittlere und kleinere Betriebe und Unternehmen ohne starke EDV-Ausrichtung ist das Outsourcing von Vorteil:

es müssen keine zusätzlichen Spezialisten eingestellt werden,denn meistens verfügen die Unternehmen nicht über genügend Wissen auf dem relevanten Gebiet, dadurch ist auch eine Konzentration auf das Kerngeschäft möglich. Der Outsourcer verfügt über einen besseren Wissensstand und neuere Technik.und somit kann größere Effizienz im Unternehmen erzielt werden.[11]

Diese Thesen decken sich auch mit den Ergebnissen, die wir durch unsere Befragungen herausgefunden haben:

[11] vgl. Bauknecht,Zürich 1994,S 220

Eine österreichissche Fluglinie verläßt sich sehr stark auf ihren Provider. Mit ihm zusammen wurde ein Kriterienkatalog für die Sicherheitsanforderungen erstellt, auch alle Information bezüglich neuer Sicherheitstrends kommt vom Provider, die Aktualisierungen der Daten und das Passwortmanagement nimmt das Unternehmen allerdings selbst vor.

Auch im Bereich der Schulen wird hauptsächlich auf Outsourcing zurückgegriffen. Ein Provider, der hauptsächlich die Schulen ans Netz anbindet, macht die Erfahrung, daß nur die wenigsten Schulen die Sicherheit selbst in die Hand nehmen wollen.

Im Bereich der öffentlichen Verwaltung ist ein Outsourcing wegen rechtlichen Vorgaben eher problematisch und wird deshalb nicht angestrebt.

Bei sehr vielen Unternehmen befindet sich der Server beim Provider, der Großteil der Unternehmen plant allerdings, ihn in Zukunft ins Haus zu holen

Die Internet-Provider sind bemüht, dem Kunden ein „sicheres„ Gesamtpaket zu garantieren, sodaß das Unternehmen mit den technischen Details oftmals nicht in Berührung kommt. Sie bieten verschiedene Pakete für Unternehmen an, die vom reinen Internetzugang über die Gestaltung der WWW-Seiten bis zum Erstellen von ganzen Sicherheitskonzepten reichen.

Hierbei arbeiten Provider-Mitarbeiter mit den Netzwerktechnikern und/oder Sicherheitsadministratoren und manchmal auch mit der Geschäftsleitung zusammen um die „Security Policy„ zu erstellen. Auf Basis dieser wird dann entschieden, welche Hard- und Software den Anforderungen des Unternehmens am besten entspricht. Es gibt auch manchmal die Möglichkeit, die Konfiguration oder ein Screening von einem anderen Unternehmen durchführen zu lassen. Durch diese gegenseitige Überprüfung erhöht sich die Sicherheit nochmals.

Ein Provider bietet zusätzlich die Übernahme der Helpdesk-Funktion, eigene Software zur Analyse der WWW Seiten und die Überwachung der Logfiles an. Ein anderer großer Provider findet die externe Überwachung der Logfiles nicht sinnvoll, da es ja darauf ankommt, daß Unregelmäßigkeiten bei der Benützung auffallen. Und diese Unregelmäßigkeiten können einem unternehmensinternen Mitarbeiter am besten auffallen.

Ein großer Vorteil für den Kunden bei Inanspruchnahme dieser Dienste soll hier die Produktunabhängigkeit und der Marktüberblick des Providers sein, die ein Garant für die beste Lösung für den Kunden sein sollen.

Die großen Provider rühmen sich auch damit, daß alle Mitarbeiter bezüglich gesetzlicher Vorschriften streng geschult werden, dem Fernmeldegesetz verpflichtet sind und zum Teil sogar ein Leumundszeugnis bei der Bewerbung vorweisen müssen. Somit wird ein ausgeprägtes Sicherheitsbewußtsein seitens der Mitarbeiter garantiert. Die Provider sehen es auch als ihre Aufgabe, den Kunden über mögliche Sicherheitsprobleme, die mit einer Internetanbindung entstehen können, aufzuklären.

Aus diesen Gründen herrscht seitens der Unternehmen sehr großes Vertrauen zum Provider und die Kunden empfinden das Outsourcing nicht als Risiko.

Geht es um große Projekte und umfangreiche Systemimplementationen so wenden sich die Unternehmen verstärkt an Softwarehäuser oder Content-Provider, die auf den jeweiligen Bereich spezialisiert sind. Hier zählt vorallem die Erfahrung, die eine optimale Unterstützung bei einem Großprojekt bietet.

Ein international agierendes Softwarehaus ist besonders im Erstellen von Gesamtlösungen für Banken, Versicherungen und Behörden.erfahren. Bei einem beliebigen Projekt im Bankenbereich wird folgendermaßen vorgegangen: im Team mit Bankmitarbeitern wird der Istzustand analysiert, danach werden mögliche Alternativen bewertet, ein Pflichtenheft entsteht, anschließend folgen Implementation, Ausbildung und Nachbetreuung. Bezüglich eines Zeitlimits für die Umsetzung ist man der Meinung, daß große Projekte nicht länger als ein Jahr in Anspruch nehmen sollten.

3..4.3 Zusammenfassung

Mögliche Gefahren durch Outsourcing wie langfristige Abhängigkeit vom Outsourcer, Know-How-Verlust im Unternehmen, weniger Sicherheitsbewußtsein durch die Auslagerung und mehr Koordinationsaufwand durch längere Befehlswege dürften durch die oben genannten Vorteile weit aufgewogen werden, da der Trend klar hin zum Outsourcing geht

Die Unternehmen haben generell keinerlei Bedenken, die Sicherheitsbelange auszulagern, sondern sehen darin einen Vortei.

3..5 Paßwortverwaltung, -vergabe, Benutzerberechtigungen

Den meisten der befragten Unternehmen ist die Paßwortverwaltung und -vergabe als Schwachstelle in ihrem Sicherheitskonzept bewußt. Dabei spielt einerseits die technische Komponente, andererseits der „menschliche„ Faktor, mit Sicherheitskonzepten sorglos umzugehen eine gewichtige Rolle. Was nützt ein ausgeklügeltes Sicherheitssystem, wenn es durch Mißachtung oder Fehlbedienung durchbrochen wird.

Welche Aufgabe hat nun eine Paßwortverwaltung, wie werden Paßwortsysteme[12] sicherer?
Paßwörter dienen dazu, Computersysteme vor unbefugtem Zutritt zu sperren. Ältere Systeme, die in Unternehmen eingesetzt wurden waren nicht flexibel genug, um den Mitarbeitern jene Dateien und Programme zur Verfügung zu stellen, die sie zur Verrichtung ihrer Arbeit benötigten. Somit wurden häufig persönliche Paßwörter an Arbeitskollegen weitergereicht. Durch diesen sorglosen Umgang mit Zutrittsberechtigungen wurde die Sicherheitstruktur durchbrochen.
Bei UNIX-Betriebssystemen ist durch eine mögliche Gruppenzuordnung der Zugriff mehrerer Benutzer auf Verzeichnisstrukturen gegeben. Die Einführung von Groupware Plattformen macht den Austausch persönlicher Paßwörter unnötig, da durch eine zentrale Berechtigungsverwaltung der Zugriff auf relevante Dateien für jeden Mitarbeiter gegeben ist.
Die regelmäßige Wartung und Änderung der Paßwörter hat dabei eine zentrale Aufgabe bei der Erhaltung einer gewissen „Grundsicherheit„ und stellt nebenbei eines der kostengünstigsten Mittel zur Erhaltung der Sicherheit dar. Unter der Wartung von Paßwörtern versteht man neben der sicheren Archivierung und Verwaltung das automatische Ausloten der Benutzerpaßworte bereits auf Systemebene auf deren Stärke, wobei zu schnell entschlüsselbare Paßwörter nicht zugelassen werden.
Nahezu jedes Betriebssystem hat jedoch Schwachstellen, die, falls sie von Hackern aufgespürt werden, zu einem immensen Schaden führen können. Da Hacker bei Attacken oftmals Programme verwenden, die Wörterbücher oder Lexika verwenden, um sogenannte „schwache„ Paßwörter ausfindig zu machen, ist die Implementierung der Schwachstellensuche bei einer Paßwortmanagement-Software anzustreben.
Eine große Anzahl an Software-Unternehmen startet massive Werbekampagnen für Sicherheitslösungen im Bereich der Paßwortverwaltung. Die Stoßrichtung der einzelnen Produkte ist eindeutig in Richtung integrierte automatische Sicherheitsadministration zu sehen. Sogenannte System Security Scanner verwalten Dateibenutzerdaten, Datei- und Applikationskonfigurationen, Programmauthentizität anhand von Checksums sowie Spuren von Hackerangriffen im System.[13]
Im Bereich der Paßwortverwaltung werden auch zusehends Programme mit künstlicher Intelligenz eingesetzt, um den immer raffinierteren Hackerangriffen Paroli bieten zu können. Derartige Ansätze treten langsam aus dem Forschungsstadium ihren Weg zur Marktreife an[14].
Genannt wurde auch die Dringlichkeit der regelmäßigen Abänderung der einzelnen Paßwörter, um eventuelle Angriffe die unentdeckt bleiben, zusätzlich zu behindern. Dabei ist es von Vorteil, wenn das System die Änderungsrhythmen automatisch vorgibt und betreut und den Benutzer somit dazu zwingt, sein Paßwort regelmäßig abzuändern.
Bei den von uns befragten Unternehmen war keine klare Strukturierung der Paßwortverwaltung zu erfragen. Da das Thema Paßwort eine wichtige Rolle im Sicherheitsumfeld der Unternehmen spielt, sind konkrete Aussagen zu dem Aufbau und der Administration der Paßwortverwaltung

[12] siehe auch Glossar: Hinweise zur Wahl sicherer Paßwörter
[13] http://iss.net/prod/s3.html
[14] http://olympus.cs.ucdavis.edu/~frank/mlid.html

unterblieben. Der Wunsch nach einem integrierten Paßwortmanagement ist insbesondere bei großen Unternehmen geäußert worden, da sich mit zunehmender Mitarbeiteranzahl die manuelle Wartung zu einem erheblichen Kostenfaktor ausbildet. Auch die Wahrung der Übersichtlichkeit ist in diesem Zusammenhang erwähnt worden.
Weitere Angaben der Interviewpartner lassen sich darauf konzentrieren, daß herkömmliche Methoden der Paßwortvergabe nicht ausreichend sind, den erforderlichen Schutz zu gewährleisten. Unternehmen schlagen den Weg ein, ihre Sicherheitssysteme durch zusätzliche Hardwareimplementationen zu verbessern. Diese Ansätzte bauen darauf auf, daß Paßwörter ständig neu generiert werden und somit nur eine extrem kurze Gültigkeit aufweisen.

3..5.1 Paßwortsysteme in Netzwerken

Als Beispiel sollen hier UNIX-Betriebssysteme dienen, um die Schwachstellenproblematik zu beschreiben:

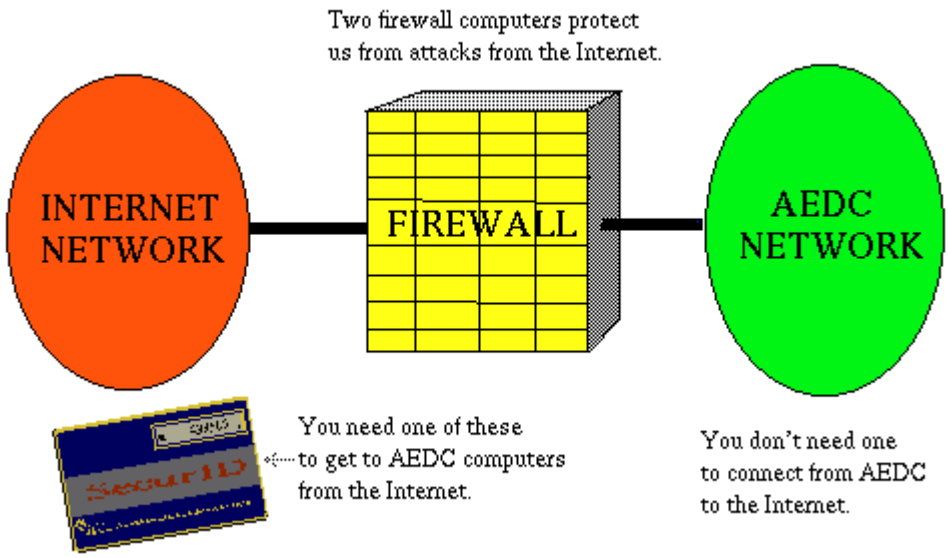
- Bei einer schlecht erfolgten Systemkonfiguration ist es möglich durch sogenannte „brute force„ Attacken ein Computersystem so lange mit verschiedenen, durch Crackprogramme generierte, Codes auszutesten, bis eine Kombination einen Zugang erlaubt.
- Telnet Sessions, die über das Internet aufgebaut werden, übertragen während des Identifikationsvorgangs Daten im Klartext. Diese Datenpakete können mitgehört werden und somit zum unbefugten Zutritt genutzt werden.
- Die Übermittlung von Zutrittsberechtigungen mittels Email kann ebenfalls abgehört werden[15].

Diese drei Beispiele sollen darstellen, daß der Sicherheitsaspekt für die Betriebssicherheit eine vielschichtige technische Betrachtung erfordert. Daneben ist auch die Motivation der Hacker, sowie deren Umfeld für eine Beurteilung bedeutsam.
Personen, die Angriffe auf Computernetzwerke ausführen agieren aus unterschiedlichsten Motiven. Von den Unternehmen ist darauf hingewiesen worden, daß Angriffe auf unternehmenswichtige Daten sehr häufig von interner Seite erfolgen. Dabei geht die Motivation, dem eigenen Arbeitgeber Schaden zuzufügen häufig von verletzten Gefühlen und Rache aus[16].
Somit sind Unternehmen nicht nur gezwungen externe Einbruchversuche abzuwehren, sondern auch Angriffe aus den eigenen Reihen zu verhindern.
Die interviewten Unternehmen versuchen die ausgehenden Gefahren durch einen ganzen Mix an Ansätzen unter Kontrolle zu halten:
Um externen Gefahren begegnen zu können, wird der Weg der strikten Trennung von WWW-Servern und den internen Netzwerken beschritten. Um dennoch den Informationsaustausch mit

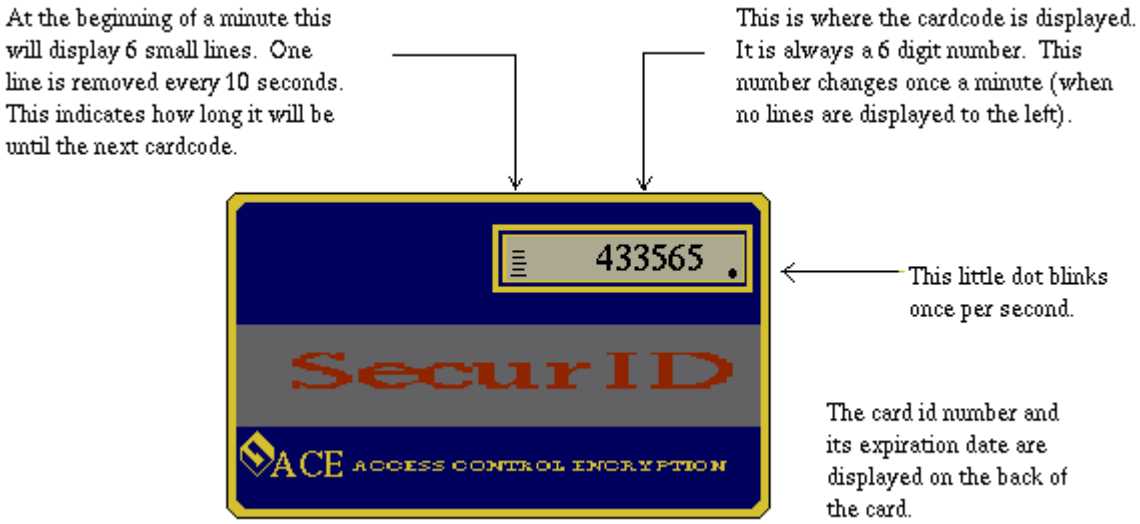
[15] Bernstein, S 38 ff.
[16] Bernstein, S 35

wichtigen, im Außendienst tätigen Mitarbeitern aufrecht zu erhalten, nutzen verschiedene Betriebe die Möglichkeit der Installation von sogenannten Callback-Modems. Der Mitarbeiter wählt dabei das Firmennetzwerk an, identifiziert sich und wird in weiterer Folge von diesem Modem zurückgerufen. Nur eine zuvor definierte Personengruppe hat damit die Möglichkeit von externer Stelle in das Netzwerk einzuloggen.
In diesem Zusammenhang wurde auch die Notwendigkeit genannt, in regelmäßigen Abständen die Arbeitsplätze der Mitarbeiter zu kontrollieren, da es häufig vorkommt, daß einzelne Mitarbeiter sich in Eigenregie Modems installieren, um von Zuhause aus auf das Firmennetzwerk zugreifen zu können.
Ein weiterer Ansatz besteht im Sperren von Internetdiensten wie Telnet oder FTP. Somit wird eine der am häufigsten gewählten Angriffsrouten für externe Hacker gesperrt.
Mit einer derartigen Verbotspolitik schränken Unternehmen aber oftmals den Informationsfluß ein.
Interne Abwehr von Angriffen erfolgt meist durch ein konsequentes Mitloggen der einzelnen Systembenutzer. Dabei werden die erfolgten Arbeitsschritte, die im Netzwerk erfolgen, mitnotiert. Jene Firmen, die derartige Überwachungsmechanismen zur Erhaltung der Sicherheit einsetzen, beteuern aber, daß sie die Daten nur bei Störfällen auswerten, um somit an den Hacker heranzukommen. Diese „big-brother„ Methode hat aber in Vergangenheit bereits zu Fehlentscheidungen geführt, da unschuldige Mitarbeiter unter Verdacht gerieten, weil Hacker wiederum die Tatsache ausnutzen sich mit einer gestohlenen Benutzerkennung zu tarnen.
Die Hauptstoßrichtung neuer Sicherheitskonzepte führt, laut Umfrageergebnissen, in den Bereich zusätzlicher Hardware Einrichtungen, welche die Identifikation der Systembenutzer sicher machen sollen. Dabei ergeben sogenannte Smart Cards sowie Token Devices einen Lösungsansatz[17].
Bei Smart Cards handelt es sich um kreditkartengroße Plastikkarten, in denen ein Prozessor sowie ein Speicher integriert sind. Derartige Systeme dienen in Verbindung mit Lesegeräten zur Identifikation der Systembenutzer. Durch die Verwendung von Abfragealgorithmen in Kombination mit einer zusätzlichen Paßwortabfrage stellen sie eine Methode dar, um einen effektiven Schutz aufzubauen.
Token Devices arbeiten nach einem ähnlichen Prinzip, nur kommen sie ohne zusätzliche Lesehardware aus. Mittels einer LCD-Anzeige wird eine, vom integrierten Prozessor berechnete sechsstellige Zahl angezeigt. Da diese nach einem gewissen Algorithmus errechnet wird, ergibt sie mit einem, auf dem Server installierten Identifikationsprogramm, einmal pro Minute einen abgeänderten Code. Somit kann grundsätzlich von jedem vernetzten Rechner aus gearbeitet werden.
Ein derartiges System wird in Zukunft bei einem Computerunternehmen installiert und trägt den Namen Secur-ID:

[17] Bernstein, S 166



Wie diese Illustration veranschaulicht, dient das System rein zur Zutrittsberechtigung externer Stellen. Somit können zumindest Hackerangriffe, die von außen erfolgen, abgeblockt werden. Die Karte selber ist sehr simpel aufgebaut:



Durch die Vernetzung von Betrieben intern und dem gleichzeitigen Anschluß von LAN's an das Internet ergaben sich große Sicherheitsdefizite. Die Struktur des Internets ist grundsätzlich nicht für sichere Transaktionen und authentifizierte Benutzer gedacht. Nur durch technische Aufsätze mittels Software oder Hardware gelingt es den Benutzer eindeutig zu identifizieren. Diese Krücken machen aber auch den Reiz derartiger weltweiter Netzwerke zunichte, da die Anonymität, die viele Benutzer schätzen, verloren geht.

3..6 Abgrenzung Informationsinhalte für Intra-/Internet

3..6.1 Definition Intranet

„Bei einem Intranet handelt es sich um ein „privates Internet„, das sich der Standards und Protokolle des Internet bedient„[18].
Eine weitere Definition ist allgemeiner gehalten: „Bei einem Intranet handelt es sich um ein plattformübergreifendes Informationsmedium„[19].

Intranets stellen die wichtigste Entwicklungsstufe der unternehmesinternen Datenverarbeitung seit Einführung der Personal Computer dar, da sie eine Oberfläche aufbauen, die die Mitarbeiter untereinander mit der benötigten Information verbinden[20].

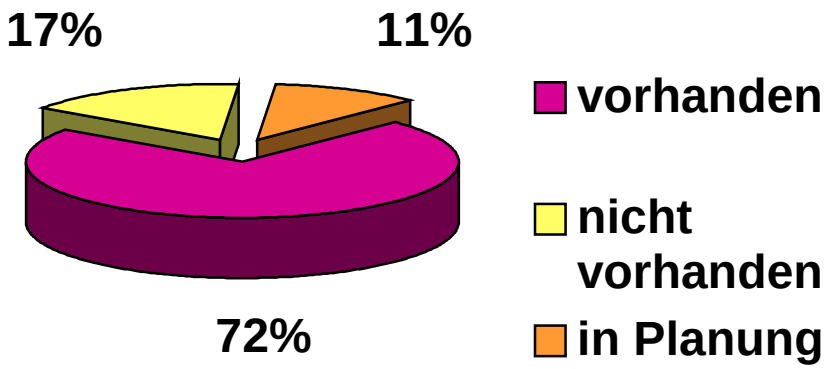
3..6.2 Worin liegen die Vorteile eines Intranets

In jüngster Zeit ist das Interesse daran, wie man Web-Technologie unternehmensintern einsetzen kann, um die Unternehmens-Kommunikation zu verbessern und die Produktivität zu steigern, enorm gestiegen. Der Begriff Intranet wird nun benutzt, um Web-Systeme zu beschreiben, deren Inhalte auf spezifische Anwenderschichten zielen - im Gegensatz zum Internet, dessen Inhalte im allgemeinen auf die breite, weltweite Anwenderschaft ausgelegt sind.
Durch den Einsatz von Web-Schnittstellen für bereits existierende Datenbanksysteme eröffnen sich für die Generierung von Daten neue, einfache Formen. Die Benutzerfreundlichkeit von Web-Oberflächen trägt sicherlich zu einer fundierteren Entscheidungshilfe bei, da Daten nicht auf umständlichen und zeitraubenden Kanälen gewonnen und transportiert werden müssen, sondern online zur Verfügung gestellt werden können.

[18] Chip 3/96 S.79
[19] Gespräch DI Theo Hoogmoed
[20] http://www.onsite.net/faq/intranet.htm

3..6.3 Abgrenzungsproblematik

Einerseits schafft ein an das Internet gekoppeltes Intranet die Möglichkeit, daß sich beispielsweise Kunden oder Interessierte in einer Art Informationsselbstbedienungsladen die gewünschte Information selbst beschaffen. Auf der anderen Seite ergeben offene Firmennetzwerke ein mit der herkömmlichen Technik kaum zu schließendes Sicherheitsloch.
Da das Intranet ein neues Schlagwort darstellt, ist der Einsatz in der Praxis noch sehr beschränkt. Zwar gaben 72% der befragten Unternehmen an, daß sie bereits ein Intranet implementiert haben, der Nutzungsumfang selber aber meist noch sehr spärlich ist.



Der Wettlauf im Intranet hat aber bereits begonnen, da der Zeitvorsprung, den ein Intranet schafft, einen beträchlichen Kostenfaktor darstellt. Die Umsetzung der einzelnen Schnittstellenmodule für die Anbindung von Datenbanken ist bei großen Unternehmen bereits in Gang gekommen. Die einzelnen Ansprechpartner sahen im Aufbau von einem Intranet eine wichtige Aufgabe um im Wettbewerb konkurrenzfähig zu bleiben.

3..7 Kosten/Nutzen der Sicherheit

Wie vor jeder Entscheidungssituation in einem Unternehmen ist die Frage der Kosten bzw. der erwartete Nutzen ein ausschlaggebendes Argument für die Realisierung.

3..7.1 Case-Study

Frage:
Uns interessierte das zur Verfügung stehende Sicherheitsbudget für die Installierung von Firewalls, für deren Wartung, für organisatorische und technische Lösungen (Sicherheitsbeauftragter). Konkret erwarteten wir uns eine Gegenüberstellung von Sicherheitskosten und dem erwarteten Nutzen, der durch eine verbesserte Kontrolle entstehen würde.

Antworten:
Generell machten Internet-Anwender folgende Aussagen:

Kosten der Beschaffung von Hardware und Software für zusätzliche Sicherheitssysteme können relativ leicht in Form einer Investitionsrechnung abgeschätzt werden. Ein Beispiel für Kostenschätzungen über Firewallmaßnahmen befindet sich im Kapitel Technik unter dem Punkt *Applikationsbasierte Firewalls*. Je größer dabei die Investitionssumme, desto genauer auch die Planung, die von den EDV-Abteilungen unserer befragten Firmen durchgeführt werden. Auffallend jedoch, daß keine der befragten Firmen bereit war, eine Kostenkalkulation vorzulegen. Begründet wurde dies des öfteren mit dem Argument des Betriebsgeheimnisses und der Unmöglichkeit das ganze Informationssystemen kostenmäßig zu erfassen.
Bei Personalkosten, dh. Kosten der laufenden Wartung, wurden wir auf die Buchhaltung verwiesen, die unserem Interesse wieder die Datenschutzbestimmungen entgegenhielten. Bei den kleineren Firmen, die wir befragten, hörten wir des öfteren die Aussage, daß die Hardware- bzw. Softwarekosten noch die Personalkosten übersteigen.
Weiters nimmt der Kostenfaktor „Weiterbildung„ einen immer größeren Stellenwert in unseren befragten Firmen ein. Bildung der internen EDV-Mitarbeiter im Bereich Sicherheitsmaßnahmen im Netz wird von allen Firmen als wichtig angesehen, jedoch macht die dafür verwendete Bildungszeit fast 50 % der gesamten Arbeitszeit mancher Mitarbeiter aus, dh. anders ausgedrückt, fast 50 % des Sicherheitsbudgets entfallen auf Weiterbildungskosten.
Der Nutzen, der durch sichere Datenbestände im Inter- und Intranet entsteht, könne laut Befragung hingegen nicht mehr quantitativ erfaßt werden. Bei vielen Firmen fehlt die Erfahrung von großen Datenverlusten bzw. Datenfälschungen, so daß der Vorteil von erhöhten Sicherheitsmaßnahmen verdeckt wird. Oft werden Sicherheitsbestimmungen als unangenehme Einschränkungen an den Arbeitnehmer empfunden. Das Verbot von manchen Diensten (z.B. FTP) stößt bei vielen Mitarbeitern in den verschiedensten Firmen auf Akzeptanzprobleme. Die durch das Internet ermöglichte Interaktion soll nicht durch Sicherheitsbestimmungen in ein reines Informationmedium umgewandelt werden. Es gilt stets die Sicherheitsüberlegungen mit dem Unternehmensfeld und Zielen der Firmen abzustimmen, denn nicht nur Einschränkungen in der

Interaktion sind die Folge, sondern jede Erhöhung an Sicherheit führt zu einer merklichen Steigerung der Kosten. In diesem Sinne ist eine Kosten/Nutzen - Analyse für den Sicherheitsaufwand in jeder Firma, die mit Inter- und Intranet in Verbindung steht, unumgänglich.

Generell wurden bei den befragten Providern zum Unterschied zu den Internet-Anwendern folgende Aussagen getroffen:

Kunden wissen kaum, welche Kosten durch die Netzanbindung auf sie zukommen. Sie sind großteils überrascht und bedenken kaum die laufenden Wartungskosten der Sicherheitssysteme. Der Provider sieht seine Aufgabe nicht nur darin, Netzanbindungen herzustellen, sondern auch auf Sicherheitsprobleme hinzuweisen. Dem Provider wird bezüglich Sicherheitsanforderungen vertraut, möglicherweise weil die Firmen sich in diesem Bereich inkompetent fühlen. Outsourcing der Sicherheitsvorkehrungen an den Provider wird bei den kleineren Kunden nicht als Sicherheitsriskio angesehen, sondern eher als Kosteneinsparungspotential.
Die befragten Provider empfehlen Kunden, die die ersten Schritte ins Netz wagen möchten, daß sie zuerst über eine Einwählverbindung, z. B. via Modem und Stand-Alone-Computer Erfahrungen sammeln und so ein Bewußtsein für Kosten/Nutzen einer Internetanbindung bzw. deren Sicherheit und Risiko schaffen. Als weiterer Schritt zur globalen Vernetzung wird die Installierung einer ISDN-Verbindung empfohlen und erst bei reichlicher Sammlung von Erfahrungswerten bezüglich Kosten und Risiken im Internet soll zu firmeninternen Netzen (Intranet) übergegangen werden.

4. Technik zur Sicherheit

4..1 Einleitung

Ausgangspunkt ist die rasante technische Entwicklung, die im letzten Jahrzehnt erst einzelne Personalcomputer, dann vernetzte Arbeitsplätze in Unternehmen, schließlich das Internet auf unseren Bildschirm gebracht hat. Somit sind viele Netze schnell gewachsen, ebenso sind die Anforderungen für die zuständigen Betreuer, Abteilungen, Unternehmen ständig gewachsen.
Der Stand der Technik in Forschung und Entwicklung hat bereits eine Vielzahl von Lösungswegen aufgezeichnet, fast täglich kommen neue Produkte sowie überarbeitete Versionen eingeführter Produkte auf den Markt.
Unternehmen haben individuelle Modi gefunden, Sicherheitsanforderungen zu definieren und die technischen Vorraussetzungen zu erfüllen.

4..2 Dimensionen der Sicherheit aus technischer Sicht

4..2.1 Voraussetzungen

Ziel der technischen Betrachtung ist die Kategorisierung der Voraussetzung und der Mittel, mit denen Unternehmen heute Sicherheitsstandards zu gewährleisten trachten.
Im Rahmen der Gesprächsreihe soll eine klare Definition des Sicherheitsbegriff an sich erarbeitet werden. Es soll der Hierarchisierung einzelner Sicherheitsbereiche ausreichend Platz eingeräumt werden . Mit den Dimensionen des Begriffs Sicherheit aus technischer Sicht ist es zwingend erforderlich auch eine Schnittstelle Mensch-Maschine unter organisatorischen Aspekten zu beachten.

4..2.2 Case-Study

Frage:
Wie definiert sich der Sicherheitsbegriff aus technischer Sicht ?

Antworten:
Nach den ersten Interviews zeigte sich, daß ein technischer Sicherheitsbegriff von den meisten Gesprächspartnern in zumeist zwei Bereiche gegliedert wird, häufig wurden die Begriffspaare Dokumentensicherheit und Verkehrssicherheit sowie Betriebssicherheit und Verkehrssicherheit genannt. Als Ursache für den allgegenwärtigen Begriff der Verkehrssicherheit vermuten wir, daß das Arbeitsumfeld der Befragten im Bereich Netzwerk und Internet liegt.

4..2.3 Dokumentensicherheit

Dokumentensicherheit betrifft jede einzelne Datei, dieser Aspekt ist im Internet bzw. Intranet besonders wichtig.
Der Browser, das Navigationstool im Internet, behandelt zum Zeitpunkt der Datenübertragung alle Files gleich. Es wird der WorldWideWeb-Server veranlaßt, das gewünschte Dokument an den Client zu schicken, ungeachtet der Tatsache, ob dies nun ein Text, ein Klang, ein Video, eine Java-Applikation oder gar ein Sicherheitszertifikat beinhaltet. Erst der Browser selbst erkennt um welche Art von Dokument es sich handelt [21], stellt dieses dann dar, oder erkundigt sich beim Benutzer, was er mit dem Dokument tun soll.
Die Abgrenzung Text, Bild, Klang, Applikation, Sicherheitszertifikat ist somit fließend, um so schwerer wird es nun, klare Aussagen über den Sicherheitsstatus der einzelnen Dokumente zu treffen.

Die Problematik der Dokumentensicherheit spielt in vielen Bereichen direkt in den Handlungs- und Entscheidungsspielraum des Benutzers hinein.

[21] Die Zuordnung dieser Dokumente erfolgt nach der Auswertung um welche Art von MIME-Type es sich handelt. MIME-Types sind defakto ein offener Standard, können vom User überarbeitet bzw. erweitert werden, und identifizieren sich anhand der File-Endung z.B. *.html, *.htm, *.au, *.wav

Der Benutzer

- ist regelmäßig Verfasser des Dokuments,
- muß die Schutzwürdigkeit des Dokuments beurteilen,
- sollte wissen mit welchen Mitteln er ein Dokument schützen kann/muß,
- neigt trotz aller Hilfestellung zu menschlichem Versagen,
- kann Information vorsätzlich veruntreuen.

Der Vorwurf der falschen Handhabung aber auch der Veruntreuung von „empfindlichen„ Dokumenten wurde in mehreren Interviews klar als schwerwiegendste Sicherheitslücke aufgezeigt. So weist ein Ansprechpartner auf die Tatsache hin, daß sich „Sicherheit vorwiegend aus der Rolle des Mitarbeiters im Unternehmen definiert, wobei die persönliche Entwicklung im Unternehmen„ eine entscheidende Determinante darstellt. Ein weiteres Statement stellt klar „70 Prozent aller Angriffe auf mehr oder weniger geheime Daten kommen von innen, also aus dem Unternehmen selbst! Um solche Risiken zu vermeiden, kommen Sie an einer gut strukturierten Sicherheitspolitik nicht vorbei„.

Es handelt sich also bei der Dokumentensicherheit um ein mehrschichtiges, oft menschliches Problem, bei dem die Rolle der Schulung im Umgang mit Technik und die Bewußtseinsbildung eine wichtige Komponente darstellen.

4..2.4 Betriebssicherheit

Sehr einprägsam definiert ein Ansprechpartner Betriebssicherheit als Kombination aus dem Zusammenspiel von Computer, Betriebssystem und Programmen.

Betriebssicherheit ist eng verbunden mit den Anforderungen zur Aufrechterhaltung des Rechnerbetriebs in einem lokalen Netzwerk oder einem Wide Area Netzwerk.
Die im Zuge der Begriffsklärung der Betriebssicherheit definierten Anforderung weisen eindeutig auf die wichtige Rolle der Netzwerkadministratoren hin. Hier überschneiden sich viele Aspekte aus der Wartung eines konventionellen Netzwerkes mit den besonderen Maßnahmen, die durch eine Anbindung an das Internet notwendig werden.

Die geführten Interviews zeigten deutlich auf, daß der Umgang mit der Sicherheit im Intranet besonders stark geprägt von den Gesichtspunkten „traditioneller„ Sicherheitsmaßnahmen in abgeschloßenen Netzwerkumgebungen ist.
Vielfach wurden wir auf die umfassenden Maßnahmen hingewiesen, die Unternehmen zur Ausfallsicherheit ergreifen. Dreifache Ausstattung durch unterbrechungsfreie Stromversorgung für wichtige Server, Triangulation der Wide Area Netzwerkverbindungen und Doppelausstattung der Router sowie Firewalls zum Internet werden hier gerne ins Treffen geführt .
Intranet-spezifischen Sicherheitsanforderungen nähert man sich sehr pragmatisch - man tut „was man kann„.

4..2.5 Verkehrssicherheit

Wir wollen eine Definition eines Ansprechpartners aus dem Bildungsbereich aufgreifen, der die Grundzüge der Verkehrssicherheit in den

- verwendeten Protokollen sowie
- der Netzwerkstrecke

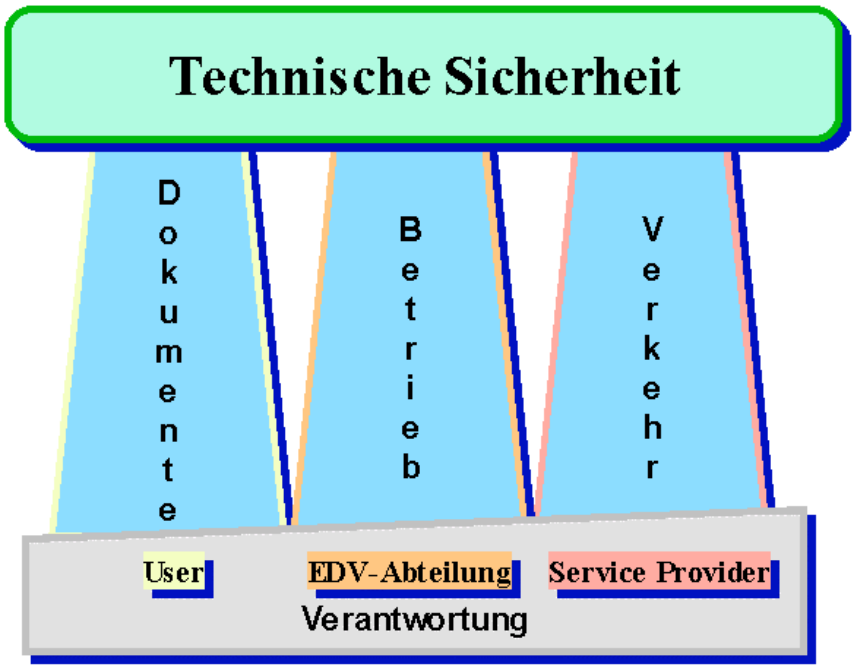
sieht.

„In Computernetzen„, wie ein Sicherheitsexperte eines internationalen Service Providers meint[22],„ wird Information von einem Computer zum nächsten gereicht. Auf jedem dieser Computer liegt die Information daher zumindest einmal kurz auf der Festplatte oder im Speicher, und wird von zumindest einem zentralen Programm weitergereicht. Das ist dann eine der Stellen, wo in Netzwerk-Kommunikation eingegriffen und Information abgefangen werden kann.„

Ein Ansprechpartner bei einem Service Provider der auch Outsourcing-Spezialist ist, meint „Verkehrssicherheit ist klar im Verantwortungsbereich des (Service) Providers angesiedelt.„
Oft stellt sich hier die Frage nach dem Outsourcing einzelner Komponenten oder Leistungen, beispielsweise die Einrichtung oder der Betrieb einer Firewall.

[22] Vgl. Homepage 05/96 S.11

Unser Versuch die Schnittstellen zwischen einzelnen Sicherheitskategorien und den Beteiligten Funktionen nachzuzeichnen hat zu folgendem Schema geführt, das mit unseren Gesprächspartnern entwickelt wurde:



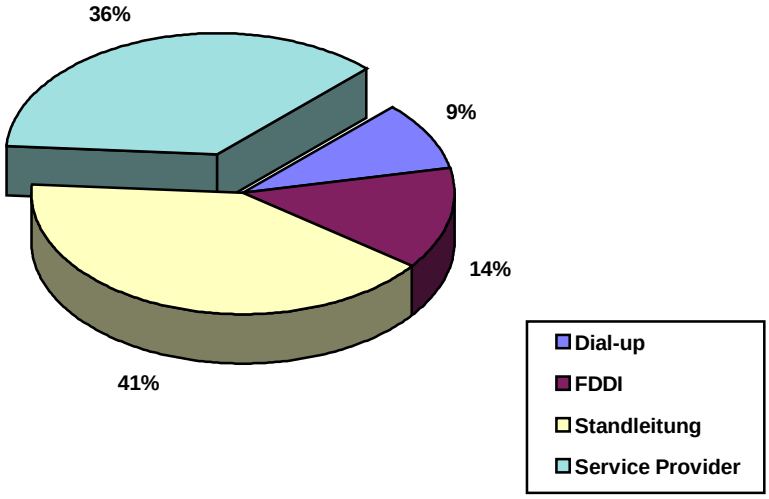
4..3 Anbindung an das Internet

Die Tatsache, daß die Kosten für Standleitungen in den letzten Jahren massiv gefallen sind[23], hat uns annehmen lassen, daß wir im Rahmen unserer Umfrage primär ISDN Anbindungen vorfinden würden. Diese Annahme hat sich weitgehend bestätigt.
Die Form der Anbindung an das Internet zeichnet auch die nachfolgenden Sicherheitsmaßnahmen in ihren Grundzügen vor.

[23] 64Kbit ISDN Standleitungen inklusive 100MB Datenaufkommen sind bereits ab ATS 3990.- /Monat verfügbar.

4..3.1 Case-Study

Frage:
Über welche Art der Anbindung an das Internet verfügt Ihr Unternehmen?



Antworten:
Nur noch wenige Unternehmen die das Internet ernsthaft nutzen verfügen über eine Dial-Up Verbindung zum Internet. Diese Dial-Up Verbindungen werden heute jedoch in der Regel bereits über ISDN abgewickelt.
Dominierend sind Standleitungsanbindungen mittels eines (64kBit/s) oder zwei (128kBit/s) ISDN Kanälen.
Interessant ist auch die starke Ausnutzung bestehender FDDI Strukturen in Verbindung mit ausgedehnten Corporate Networks,. Manche Unternehmen verfügen somit über eine Infrastruktur die es Ihnen gestatten, auf Internet Service Provider in ganz Europa oder Übersee zurückzugreifen. Ähnliche Strukuren finden wir bei den größeren Internet Service Providern vor.

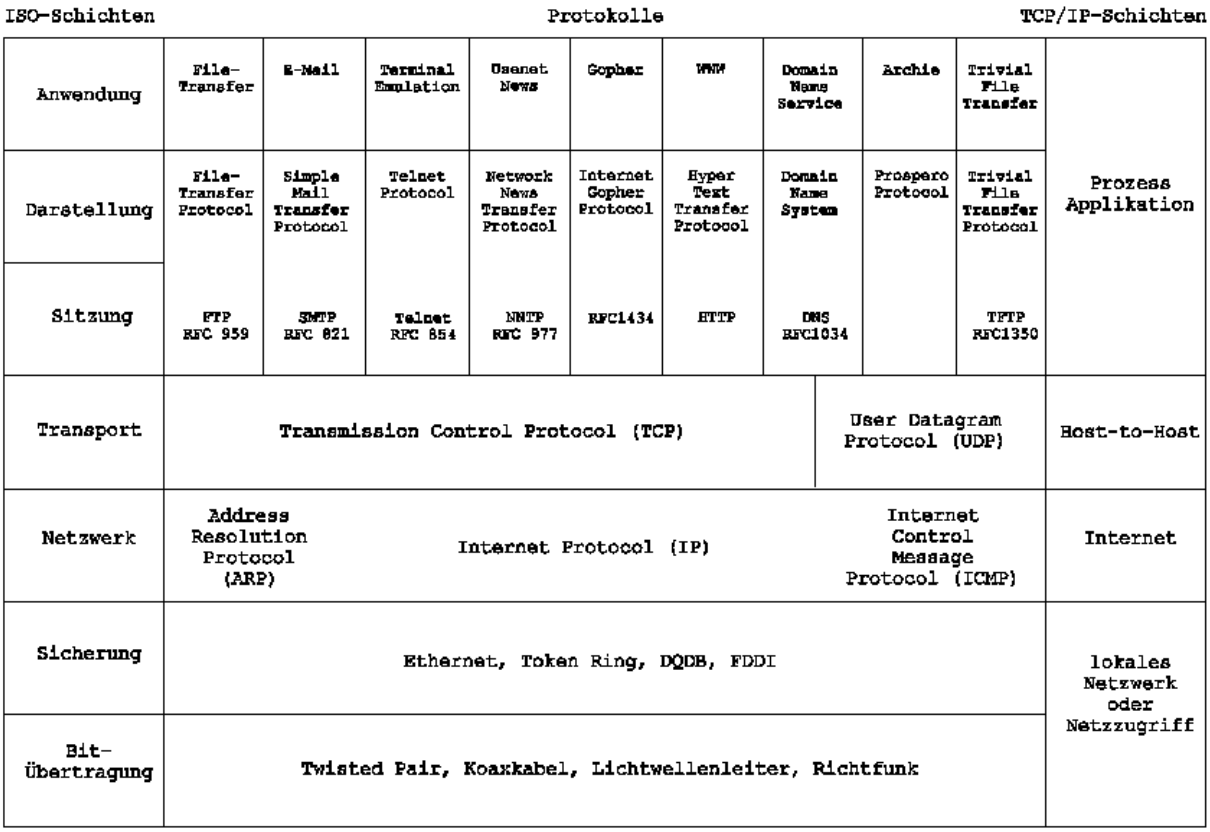
4..4 Sicherheit in Schichten

4..4.1 Protokolle und Dienste

Die Fokussierung auf Internet und Intranet-Umgebungen setzt eine Auseinandersetzung mit dem Internetprotokoll TCP/IP und dessen Grundlagen auseinander.
Anhand des ISO/OSI Referenzmodells wollen wir eine Einteilung der technischen Maßnahmen treffen.

Das ISO/OSI Schichten-Referenzmodell ist heute Basis für die Definition des Transports von Daten über jede denkbare Hard und Software.
Das ISO/OSI Modell ist ein offener Standard, der so einen möglichst großen Spielraum für die Erweiterung und Bereicherung vorhandener Techniken ermöglicht. So bleibt den Entwicklern neuer Hard- und Software ein großer Spielraum, um aufbauend auf den Stand der Technik neue Konzepte zu realisieren.

Das ISO/OSI-Modell entstand allerdings erst zu Beginn der 70er Jahre, als das Arpanet bereits einsatzfähig war. Das Arpanet beruht auf den damals gängigen 4 schichtigen DoD Modellen. Die Erfahrungen, die bei der Entwicklung des Arpanet gemacht wurden, gingen jedoch in die ISO/OSI Modellierung mit ein. Die Internet-Protokolle können aber in das Schichtenmodell von ISO/OSI, allerdings mit nur fünf Ebenen, eingeordnet werden:[24]



[24] [Scheller, S.25]

4..4.2 Case Study

Die hier wiedergegebenen Ergebnisse resultieren primär aus Interviews, die einerseits mit Service Providern, andererseits mit Unternehmen, die in Forschung und Entwicklung tätig sind, geführt wurden.

Frage:

Auf welchen Ebenen des ISO/OSI Referenzmodells setzen die von Ihnen getroffenen Sicherheitsmaßnahmen an?

Antworten:

Aus dem ISO/OSI Referenzmodell leiten sich Kategorien von Eingriffen in den Datenfluß ab, die sich einerseits den Protokollen der unteren Schichten des ISO/OSI Modells auf Netzwerkebene zurechnen lassen, andererseits an den oberen Schichten, als Softwarelösung ansetzen.
Es kommen somit auch grundsätzlich 2 verschiedene Typen von Firewalls zum Einsatz, darüber hinaus kommen weitere Protokolle auf Applikatiuonsschicht wie SSL zur Verwendung. Die eingesetzten Firewalls lassen sich anhand der Schichten im ISO/OSI Modell in folgende Kategorien einteilen:

Firewalls auf unteren Schichten

Für die Sicherheit von Relevanz ist bei den unteren ISO Schichten besonders Schicht 3 (DoD 2), die das Netzwerk definiert. Besondere Bedeutung kommt hierbei dem Weiterreichen von Paketen zu. Diese werden von Rechner zu Rechner, von Netz zu Netz weitergereicht - ein Prozeß der im allgemeinen als Routing bekannt ist. Um das automatische Routing von außen ins Intranet und vice versa zu blockieren werden Firewalls eingesetzt. Firewalls unterbinden das Weiterreichen von Paketen, abhängig davon, an welche Ports sie adressiert sind. Wir haben es also mit intelligenten Filtern zu tun, die in den Datenfluß auf der Netzwerk-Schicht des ISO/OSI Referenzmodells beeinflussen. Packet Filtering Firewalls (siehe Glossar) werden von allen befragten Service Providern angeboten.

Firewalls auf höheren Schichten

Hier setzen die Sicherheitsmaßnahmen in dem zuvor angeführten ISO/OSI Schichtenmodell auf Schichten 5, 6, 7 (DoD Schicht 4) an. Wir können Ansätze auf Prozeß/Applikationsebene in diesem Spektrum ansiedeln. Im Regelfall handelt es sich um „Applikations basierte Firewalls“, auch „Dual Homed Gatways“ (siehe Glossar). Kleiner Serviceprovider bieten hier deutlich seltener Lösungen an, diese sind jedoch häufig sehr kreativ: Besonders das Betriebssystem LINUX und dessen Fähigkeit als Firewall zu agieren wird wiederholt ins Treffen geführt. Auch SHAREWARE die über das Internet bezogen wurde kommt zum Einsatz, hier ist besonders Windows 95 und Windows NT im Visier der Hersteller.

4..5 Sicherheitskonzepte

Ein Sicherheitskonzept, häufig auch als „policy“ bezeichnet, bildet die Grundlage für die Sicherheitmaßnahmen. Wir wollten feststellen über welche Konzepte Unternehmen verfügen und wo das erforderliche Wissen erworben wurde.

4..5.1 Case-Study

Frage:
Welche Sicherheitskonzepte und Techniken kommen zum Einsatz , wie werden diese erfaßt und umgesetzt?

Antworten:
Es scheint ein Mangel an „All-in-one“ Produkten vorzuliegen, die alle Bausteine eines Sicherheitskonzepts berücksichtigen. Es fehlt aber auch die Nachfrage nach individuellen Konzepten, die besonders ein Intranet in spezifischer Weise schützen.
So erinnert man sich bei einem Softwarehaus, das zumeist Internet als Nachhut zu betriebswirtschaftlicher Standardsoftware an Kunden mit ausgedehnten Netzwerken liefert, an eine einzige Anfrage zu einem Rollenkozept in einem Intranet.
Meist wird darauf hingewiesen, daß eine Trennung der Zugriffsrechte im Intranet ausschließlich über die Form der Netzwerkanbindung beziehungsweise die IP-Adresse des Clients erzielt wird.

Die Serviceprovider warten mit einer breiten Palette an Maßnahmen auf, deren Kern sich auf drei technische Konzepte reduzieren läßt:

- Paketfilterung mittels intelligenter Router
- Applikationsbasierte Firewalls
- Virtual Private Networks

Im Rahmen von Sicherheits-Consulting und Auditing werden von den Serviceprovidern Sicherheitskonzepte an die Verhältnisse im jeweiligen Unternehmen angepaßt.
Das folgende Schema gibt uns Aufschluß über den Ablauf eines Security Consulting samt Firewall Implementierung bei einem Firmen Netzwerk[25]:

Phase 1

1 Manntag vor Ort.

- Erläuterung der Funktionsweise und Konzepte für eine Firewall.
- Definition der Sicherheitspolitik.
- Festlegung der Konfiguration.
- Abklärung der Hard- und Softwarevorraussetzungen.

Phase 2

Plattformabhängig, ca. 2 Manntage vor Ort, nach etwaiger Lieferung und Installation der Komponenten

- Installation und Konfiguration.
- Test der Endbenutzer Applikationen.
- Split-DomainNameServer-Setup.
- Realisierung von interaktivem Zugang von außen mittels One-Time Password oder Schlüssel Taschenrechner

Phase 3

½ Manntag vor Ort, ½ Manntag bei Eunet

- Verifikation von innen und außen.
- Erstellung des Protokolls, Abnahme.

Phase 4

1 - 2 Manntage vor Ort

- „Train the Trainer„-Schulung

[25] Vgl. homepage 05/96 S.11

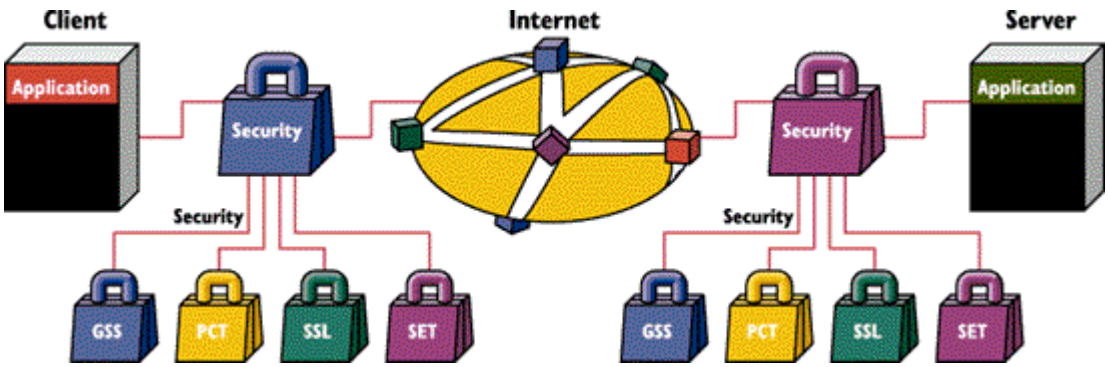
Für den oben gezeichneten Ablauf ergeben sich laut Anbieter für Phase 1-3 Kosten von rund ATS 70.000.- (exklusive Hard- und Software). Phase 4 schlägt sich mit weiteren ATS 20.000.- bis ATS 40.000.- zu Buche.
Ein Konkurrent rechnet für eine SUN-basierte Firewall (samt Installation) ATS 300.000.- (ATS 40.000.- bis ATS 50.000.-), weist jedoch daruf hin, daß der Kundenwunsch meist auf eine „shared„ Firewall beim Service Provider deutet. Diese wird dann von mehreren Kunden geteilt.
Es kann schon vorkommen, daß sich bei einer solchen geteilten Variante, über 50 Kunden in jeweils getrennten Subnetzen (meist Class-A, Class-B) eine Firewall teilen.

4..6 Sichere Protokolle für Internet-Transaktionen

In diesem Teil geht es um Protokolle, welche eine sichere Transaktion via Internet und/oder Intranet ermöglichen sollen. Unsere Frage zu diesem Thema lautete :
Sind ihnen diese Protokolle bekannt und inwieweit setzen sie diese Protokolle bereits ein ?

4..6.1 Allgemein

Die rasante technische Entwicklung und die dadurch entstandenen neuen Produktsparten (z.B. Online Shopping) stellen neue Anforderungen an bestehende Sicherheitssysteme. Es sind Protokolle gefragt, die diesem Sicherheitsbedürfnis entsprechen. Sie sollen auf Transport Layer Ebene zumindest eine Verschlüsselung ermöglichen können.
Die folgende Grafik soll veranschaulichen, wie eine sichere Datenübertragung via Internet mittels vielen verschiedenen Protokollen funktioniert. Bevor Daten über öffentliche Netze versandt werden, werden sie verschlüsselt bzw. wenn sie am Zielort ankommen, entschlüsselt.



Quelle : TradeWave Corporation, www.tradewave.com

4..6.2 Case-Study

In unserer Umfrage wurden nur zwei Protokolle genannt : SSL (Secure Sockets Layer) und SET (Secure Electronic Transaction). Ihre Funktionsweise wird kurz im Glossar beschrieben.

Da SSL von fast allen neuen Web-Browsern unterstützt wird, dürfte es sich als Standard etablieren. Dieses Protokoll findet bereits rege Verwendung bei der Verschlüsselung von Online-Banking und Online-Shopping Diensten. Bei zwei Banken und einem Handelsunternehmen wird SSL bereits verwendet. Insgesamt ist dieses Protokoll auf großes Interesse gestoßen. Ein anonymes Einkaufen ist aber, bei den von uns befragten Unternehmen, weiterhin nicht möglich. Kunden, welches dieses Angebot nützen wollen, müssen sich vorher beim Unternehmen registrieren lassen. SSL hat hier also lediglich die Funktion, Daten zu verschlüsseln.
SET wurde von den Providern positiv aufgenommen, da es sich auch hervorragend für kleinere Beträge eignet, wurde argumentiert. Aber bei keinem Unternehmen wurde bislang das Protokoll SET im Realbetrieb verwendet.

4..6.3 Zusammenfassung

Mit SSL und SET haben Unternehmen zwei leistungsstarke Protokolle zur Verfügung, auf deren Basis sichere Verkaufs- und Marketinginstrumente ansetzen können. SSL stellt eine billige und leicht zu realisierende Möglichkeit dar, Online-Geschäfte zu tätigen, auch wenn es in Österreich bisher „nur„ zur Datenverschlüsselung eingesetzt wird. SET geht weit über die Funktionen von SSL hinaus, hat jedoch den Nachteil, daß es kein Stand-Alone Produkt ist. Es benötigt Applikationen, welche auf SET aufbauen, um zu funktionieren. Es sei hier auf IBMs Net.Commerce Payment verwiesen (siehe Glossar). Weiters sei an selber Stelle auf Verifone´s Internet Commerce verwiesen, welches eine Kombination aus SSL und SET darstellt.

4..7 Software

4..7.1 Allgemein

Als Webbrowser liegt momentan Netscape weit führend voran. Eine Ursache für den Erfolg von Netscape ist die Verfügbarkeit für fast alle Plattformen. Mittlerweile sind Versionen für Linux, NT, Windows, MacIntosh und OS/2 erhältlich.
Microsoft dürfte jedoch in Zukunft an Bedeutung gewinnen, da Microsoft die Produkte (iExplorer, Frontpage,...) meist kostenlos zur Verfügung stellt.
Ebenfalls sollte in Betracht gezogen werden, welche Sicherheitsstandards (z.B. SSL) unterstützt werden und welche Erweiterungen (sog. Plug-Ins) angeboten werden. Ein weiteres Sicherheitsmerkmal liegt in der Möglichkeit, ActiveX und JavaApplets abzuschalten, da in ihnen beträchtliche Sicherheitsrisiken stecken

4..7.2 Case-Study:

Fragen:
Welche Software wird in ihrem Unternehmen genutzt ?
Nach welchen Kriterien wurden diese ausgewählt ?

Anworten:
Grundsätzlich war festzustellen, daß die verwendeten Softwarepakete vom Provider empfohlen bzw. bereitgestellt wurden. Diese wiederum wählen je nach Marktsituation aus und nach dem bevorzugten Betriebssystem des Unternehmens. Daher wurde zumeist Netscapes Navigator empfohlen.

Weiters Funktionalität, Bedienerfreundlichkeit und Wartungsfreundlichkeit sollten in Betracht gezogen werden. Ein Provider sprach davon, daß es schön und gut ist, wenn ein Programm zwar viele interessante Funktionen bietet, aber es abzulehnen ist, wenn eine Weiterentwicklung durch den Hersteller nicht gesichert sei. Man verläßt sich lieber auf Programme von großen Softwarehäusern.
Die Problematik von ActiveX und JavaScripts war allen Unternehmen bewußt und daher wurden diese Funktionen auch von vielen, mit Ausnahme aller Provider, deaktiviert. Die Provider

argumentierten damit, daß man stets auf dem neuesten technischen Stand sein will und Entwicklungen verfolgen will und muß.

Sehr verbreitet im Bereich Intranet / Web-Publishing ist Lotus Notes. Es ist eine benutzerfreundliche Lösung für die meisten Internet spezifische Anforderungen. Einige Unternehmen setzen jedoch auf exotische Browser, wie sie auch im Internet Verbreitung finden.

4..8 Pretty Good Privacy (PGP)

4..8.1 Allgemein

Pretty Good Privacy ist ein Paket, das dem Anwender gestattet, unter Verwendung assymetrischer Public Key Kryptographie, empfindliche Daten über unsichere Übertragungswege zu versenden. Haupteinsatzbereich von PGP ist der Mitteilungsaustausch über E-Mail.

4..8.2 Case-Study

Frage:
Setzen sie Pretty Good Privacy (PGP) ein?

Antworten:
PGP ist ein asymmetrisches Verschlüsselungsverfahren, das von den befragten Unternehmen nur selten zum Schutz von E-Mail eingesetzt wird. PGP gestattet die Verschlüsselung einzelner Dokumente zum Transport über unsichere Netzwerkstrecken, kann aber auch zur Verschlüsselung ganzer Festplatteninhalte eingesetzt werden, wie ein Ansprechpartner aus dem Bereich Forschung und Entwicklung aufzeigt.
Jedoch haben Versuche mit PGP in den meisten Unternehmen gezeigt, daß es die Fertigkeit und das Vorhandensein entsprechender Software bei Sender und Empfänger voraussetzt, was in der Praxis noch zu erheblichen Problemen führt.
PGP steht in Widerspruch zu lange eingeführter, „bewährter„ Software:

- Integration zumeist unmöglich
- Benutzer deutlich überfordert
- Partnerunternehmen unterstützt PGP nicht

Oft wird nun mit dem Produkt MS-Mail oder dessen Nachfolger MS-Exchange gearbeitet.
Diese Pakete sind besonders schlecht zur sanften Migration zu PGP fähigen E-mail-Clients geeignet.
Wer dennoch PGP einsetzen will, darf dies jedoch in den meisten Unternehmen. Vereinzelte Service Provider empfehlen PGP ausdrücklich, kennen jedoch die Probleme der Unternehmen.
Es wurde auch erwähnt, daß Kryptisierung von E-Mail entgegen eindeutigen EU Bestrebungen in einzelnen EU-Staaten verboten ist.

4..8.3 Zusammenfassung

Im Intranet geht der Trend in die Richtung, daß es, vom Aufbau her, vom Internet nicht zu unterscheiden ist. Mit ein und derselben Software soll auf beide Bereiche zugegriffen werden können. Das Intranet wird, wie auch die eigene Homepage, in HTML verfaßt.
Kein einziges Unternehmen hat sich über ihre Internetsoftware beklagt , wie es bei kaufmännischer Software oft vorkommt, da sie nicht für jedes Unternehmen maßgeschneidert sein kann. Das Internet scheint wohl noch dermaßen Neuland zu sein, daß man es nach der gegebenen Funktionalität der Software bewertet und nicht nach den eigentlichen technischen und wirtschaftlichen Möglichkeiten sucht. Akzeptanz geht vor Innovation.

4..9 Zahlungsabwicklung

„Für den Internet-Anwender in Österreich sind vor allem die folgenden zwei Formen der Kommunikation via Internet relevant: Erstens das „Cyberpublishing„, darunter versteht man das Anbieten von „bunten Seiten„ im World Wide Web, zweitens die Abwicklung von Geschäftsprozessen, wie der Zugriff auf Geschäftsdaten durch Einkaufen und Buchen. Mit der steigenden Bedeutung, die der Austausch von Gütern und Dienstleistungen im Internet erhält, steigt auch die Nachfrage nach Zahlungsmitteln, die diesem Medium entsprechen, rasant. Während für die Veröffentlichung diverser Informationen über das Internet traditionelle publizistische und grafische Kenntnisse im wesentlichen ausreichen, sind die Methoden und Techniken des herkömmlichen Zahlungsverkehrs im Internet beschränkt anwendbar„[26].

[26]vgl. Interview mit Dr. Thomas Kolarik, Information Service, 12. Nov. 1996

4..9.1 Übersicht über Zahlungssysteme[27]

Neue Techniken zur sicheren Übertragung von Transaktionsdaten über dieses unsichere Medium sollen hier nur demonstrativ aufgezählt und kurz erläutert werden, um den Schwerpunkt dieses Abschnittes auf unsere interviewten Firmen zu legen, die wir über ihre Einstellung und die Möglichkeit eines Einzsatzes elektronischer Zahlungsmittel befragten.

First Virtual[28] und Cyber Cash[29]

Beide Systeme übernehmen die Rolle des Kreditkartenhändlers, demgegenüber jeder Käufer über seine Kreditkarte bezahlt. Nach Erhalt des Geldes überweist der jeweilige Vermittler das Geld - nach Abzug einer gewissen Provision - an den eigentlichen Verkäufer auf traditionellem Wege, z. B. als Banküberweisung. Der Verkäufer von Waren, der das First Virtual- oder das Cyber Cash Bezahlsystem benutzt, braucht selbst also kein Kreditkartenhändler zu sein. Allerdings müssen Käufer und Verkäufer vorher Kunden bei diesen Vermittlern werden.

Die beiden Systeme unterscheiden sich lediglich in der Art der Übermittlung der Kreditkartennummern des Kunden an den Vermittler. Bei First Virtual beschränkt sich die Übermittlungssicherheit auf eine klug ausgedachte Abarbeitungsreihenfolge von E-mails und ist somit nur so vertraulich wie bestehende Internetanwendungen, während bei Cyber Cash die Übermittlung kryptographisch geschützt wird.

Beide System, First Virtual und Cyber Cash, laufen im Realbetrieb. Sie wickeln bereits seit September 1994 reale Informations- und Geldgeschäfte über das Internet ab. Über Umsatzvolumina schweigen sich die Firmen aus. Aber First Virtual behauptet eine Umsatzverdopplung alle drei Monate.[30]

Ecash[31] und CAFE[32]

Die gemeinsame Grundidee dieser beiden Zahlungssysteme ist eine bestimmte Form digitaler Geldmünzen, durch die ein Käufer anonym gegenüber Verkäufer und Bank einkaufen kann, während der Käufer von sich aus in Zusammenarbeit mit der Bank die Identität des Geldempfängers aufdecken und beweisen kann. Der wesentliche Unterschied besteht darin, daß Ecash auf Online Kommunikation im Internet basiert, während CAFE Offline mit digitalen Geldbörsen, sogenannten „Wallets„, operiert.

---

[27]Vgl. Grimm, R; Teil 1, Ausgabe 5/96, S. 8 ff,
[28]vlg. url: http://www.fv.com/
[29]vlg. url: http://www.cybercash.com/pub/draft-cybercash-v08-00.txt
[30]vgl. Grimm, R, Teil 2, Ausgabe 2/96, S. 9,
[31]vlg. url: http://www.digicash.com/ecash/ecash-home.html

Bei Ecash von der holländischen Firma Digicash werden die digitalen Geldmünzen in einem lokalen System, z.B. einer Smartcard oder verschlüsselt auf einer Workstation, gespeichert. Käufer und Verkäufer sind über das Internet miteinander verbunden und transferieren die Geldmünzen über das Netz. Der Verkäufer prüft eine ihm angebotene Münze, bevor er sie annimmt, indem er ihre Echtheit online von der ausstellenden Bank prüfen läßt: so kann auch keine Münze mehr als einmal ausgegeben werden, da sich die Bank die Seriennummern aller ausgegebenen Münzen merkt und eine zum zweitenmal eingereichte Seriennummer als bereits verbraucht zurückweisen würde.

CAFE hingegen verwendet für dieses System entwickelte Hardware-Geräte als elektronische Geldbörsen, die über Infrarot miteinander kommunizieren. Hier ist eine Online-Prüfung der Echtheit von Münzen nicht ohne weiteres möglich. Statt dessen liefert der Käufer bei dem Bezahlvorgang eine Teilmenge seiner Identifikationskennzeichen mit, die für sich genommen keine weitere Auskunft über seine Identität geben. Aber in Kombination mit jeder anderen Teilmenge seiner Identifikationskennzeichen zu selben Seriennummer deckt sie seine Identität beweisbar auf. Die Bank könnte dann die verschiedenen Teilmengen zur echten Identität des „Betrügers„ kombinieren und z.B. den betrogenen Empfänger der doppelt ausgegebenen Geldmünze auf Kosten des Betrügers entschädigen.[33]

Ecash und CAFE verwenden aufgrund ihrer unterschiedlichen technischen Anforderungen verschiedene Algorithmen. Ecash verwendet RSA 78[34] und CAFE verwendet Schnorr-Varianten von ElGamal (ELGA 85[35]).

4..9.2 Case-study

Frage:

Mit oben angeführten Hintergrundwissen über die Funktionsweise und Arten des elektronischen Geldes fragten wir unsere ausgewählten, österreichischen Firmen, ob sie im Internet Zahlungsmöglichkeiten anbieten, bzw. wenn ja, welche Zahlungsform sie bevorzugen. Weiters interessierte uns, ob man ein Wachstumspotential in dieser Marketing - Strategie sieht und natürlich, ob die Daten des Zahlungsverkehrs im Netz verschlüsselt werden.

Antworten:

---

[32]vlg. url: http://www.cwi.nl/cwi/projects/cafe.html
[33]vgl. Grimm, Teil 2, S. 11.
[34] vgl. [Rivest, R., Shamir, A., Adleman, L. S. 120-126]]
[35]vgl. ElGamal, T,: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, Vol.IT-31, 469-472, 1985

Bei einem österreichischen Flugunternehmen werden seit Mitte November 1996 Reservierungsmöglichkeiten für Reiserestplätze im Internet angeboten. Um die Reiseveranstalter nicht zu verärgern, werden nur Restplätze angeboten, die noch am selben Tag der Internet-Ankündigung gebucht werden müssen. Die Reservierungen selbst werden per E-Mail vorgenommen, in der unverschlüsselt die Namen, die Adresse und die Kreditkartennummer von Kunden angegeben werden. Die Überprüfung der Kreditkartennummern auf ihre Gültigkeit und Deckung wird von dem Reservierungsprogramm Amadeus sofort nach Absendung der Email durchgeführt. Bei erfolgreicher Prüfung wird eine Rückbestätigung der Reservierung vom Flugunternehmen an den Kunden per Email geschickt und die Tickets werden am Flugschalter bereit gehalten. Erst bei Abholung der Tickets kommt es zur Abbuchung am Konto des Kunden.
Negative Erfahrungen über die unverschlüsselten Kreditkartennummern im Netz bzw. mit Jux-Reservierungen wurden bisher noch nicht gemacht, möglicherweise aufgrund des zu kurzen Beobachtungszeitraums. Die Thematik der „öffentlichen„ Kreditkartennummern wird nicht als internetspezifisches Problem erkannt, sondern sieht die gleichen Probleme beim Kauf in herkömmlichen Geschäften. Um den Kunden jedoch die Angst des ungeschützten Datenverkehrs zu nehmen, können bei diesem Flugunternehmen eigene Kundendaten angelegt werden, über die dann die Reservierung bzw. Abrechnung erfolgt.
Dieser Online-Dienst wurde bisher wenig beworben, um die Reiseveranstalter nicht zu verunsichern. Doch in der Tourismusbranche zeigt sich nun auch in Österreich deutlich die internationale Tendenz, die Reisebüros aus ihrer Funktion als Reisemittler zu verdrängen.
Den verschlüsselten Zahlungssystemen im Netz (E-Cash, Cyber Cash, MS Money) steht diese Fluglinie aufgeschlossen gegenüber, wartet aber noch auf Erfahrungswerte von anderen Unternehmen.

Auf gleiche Weise funktioniert das Zahlungssystem bei Inserat-Firmen im Second-Hand Bereich. Name, Adresse und Kreditkartennummer befinden sich für max. einen Tag unverschlüsselt auf dem Server beim Provider und werden danach in den internen Unternehmensbereich übertragen. Die Funktion der öffentlichen Zahlungsabwicklung wird in diesem Geschäftsbereich nur mäßig in Anspruch genommen. (3 - 4 Kreditkartennummern pro Tag). Die Beträge, die mit unverschlüsselter Kreditkartennummer überwiesen werden, sind als gering anzusehen.

Bei einer österreichischen Großbank, die zwar seit Anfang 1995 eine Homepage besitzt, aber noch keine Transaktionen übers Netz durchführt, steht der Sicherheitsaspekt der Transfers und der Datenschutz im Vordergrund. Bisher erfolgte das angebotene Electronic Banking nur mit bekannten Kunden über unverschlüsselte Leitungen nach dem Callback Prinzip. Um neue „verschlüsselte„ Transaktionen zu entwickeln bzw. bestehende Systeme zu testen, wird im Frühjahr 1997 der Transaktionsbereich aus der Bankzentrale ausgegliedert und in eine dafür gegründete Tochterfirma verlagert. Ein eigener Provider wurde bereits im März 1996 als Tochterfirma gegründet. Dieser Provider löst den bisherigen, nicht in den Konzernverbund integrierten alten Provider ab und übernimmt auf ihren Server die gesamte Internet - Bankpräsentation, sowie den Einsatz der Firewall.

Bei einer anderen österreichischen Großbank ist seit Anfang November 1997 ein vollintegriertes Internet-Telebanking im Einsatz. Ziel ist es, den Zahlungsverkehr zu automatisieren und somit Personalkosten in diesem Bereich zu senken, sowie ein bequemeres 24-Stunden Service für Bankkunden zu schaffen.
Die Grundlage für sichere Transaktionen bildet ein 64-Bit Schlüssel (SSL 64 Bit RSA), für den eine Sondergenehmigung der amerikanischen Exportkontrollbehörde erteilt wurde. Für die Authentizierung der beiden Geschäftspartner wurde eine Zertifizierungsstelle für die Bank eingerichtet, die Verfügungsnummern und ein PIN - Code an Kunden vergibt.
Voraussetzung für Online-Banking bei dieser Bank ist die Installierung des Finanzplanungsprogramms MS Money 97 bei den Bankkunden.
Zum Schutz vor dem „Nachspielen„ von Transaktionen am Internet werden pro Kunde 48 Transaktionsnummern vergeben, wobei bei jeder Transaktion eine Nummer (TAN) verbraucht wird, d.h. die Abruf eines Kontostandes und eine Überweisung benötigen 2 Nummern. Bei ca. 10 verbleibenden Nummern werden neue per Internet zugesandt.
Die befragte Bank setzt auf die elektronische Abwicklung der Zahlung, da nicht nur ein bequemeres Kundenservice ermöglicht wird, sondern enorme Rationalisierungsmaßnahmen getroffen werden und Zeiteinsparung für beide Geschäftspartner ermöglicht werden. Ab Jänner ´97 wurde bereits die erste vollelektronische Filiale (easy bank) in Österreich eingesetzt.
Auf eventuelle Sicherheitsbedenken angesprochen, entgegnete man uns, daß dieses Thema künstlich von den Medien hochgepusht wird. In dieser Bank hätte es seit der Installierung dieses Zahlungssystems noch keine sicherheitsbezogenen Vorfälle gegeben.

Bei einer in Österreich ansässigen, international agierenden Kommunikationsfirma stellen nicht die technischen Möglichkeiten die Probleme für sicheren Zahlungsverkehr dar, sondern die rechtlichen Probleme in Österreich. Dies sei angeblich auch der Grund, warum man für die relativ teuren Firmenprodukte, die auf der Homepage beworben werden, noch keinen Zahlungsverkehr im Netz

anbietet. In einer eigenen Internetabteilung werden elektronische Zahlungssysteme und elektronische Unterschriften auf ihre Sicherheit und Anwendbarkeit getestet. Desweiteren wird ein https- Server zu Testzwecken verwendet.

Die befragten österreichischen Provider beklagen die fehlenden Standards im Transaktionsbereich. Solche Standards wären unumgänglich für nationale und vor allem internationale Sicherheitsmaßnahmen.
SET (siehe GLOSSAR) könnte nach Meinung dieser Provider zu einem möglichen Standardtool im nicht anonymen Zahlungsverkehr heranreifen. Bei diesem Tool werden die Kreditkartennummern vor der Übertragung im Netz verschlüsselt und die Identität des Kunden wird mittels elektronischer Unterschrift überprüft. Die Durchsetzung von SET wird hauptsächlich von den beiden größten Kreditkartenfirmen VISA und MASTERCARD vorangetrieben. Im Bereich des anonymen Zahlungstroms wird E-Cash von den Providern empfohlen. Dieses Zahlungssystem befindet sich zur Zeit in einer sechsmonatigen Testphase bei der Deutschen Bank.[36]

4..9.3 Zusammenfassung

Allgemein kann festgestellt werden, daß sich die befragten Firmen der Sicherheitsprobleme im Transaktionsbereich durchaus bewußt sind. Abhängig von der Branche und dem Transaktionsumfang werden aber diese Sicherheitsfragen relativiert und mit dem möglichen Schadenspotential gegenübergestellt. Speziell im Bereich der Kreditkarten bestehen bereits Versicherungen, die den Schaden aus Geschäften mit falschen Kreditkartennummern absichern. Alle befragten Firmen gaben sich aufgeschlossen gegenüber den verschlüsselten Transaktionstechniken, wenngleich unterschiedliche Aussagen über deren Einsatz getroffen wurde. Man wartet die Marktentwicklung in diesem Bereich ab.

[36]vgl. url: http://www.deutsche-bank.de/

5. Ausblicke

Viele befragten Personen waren der Meinung, daß Sicherheit im Internet kein technisches Problem, sondern ein psychologisches Problem sei („Sicherheit spielt sich im Kopf der Leute ab„).

Das Internet sei genauso viel oder wenig sicher wie Briefsendungen, Telefax, etc., denn auch diese können abgefangen und verändert werden. Der einzige Unterschied zu herkömmlichen Kommunikations- und Transaktionsverfahren ist, daß das Internet ein relativ neues Medium ist. Und der Großteil der Menschen steht Neuem grundsätzlich mit Skepsis gegenüber.

Natürlich gibt es branchenspezifische Unterschiede, die den Stellenwert der Sicherheit in den verschiedenen Unternehmen betreffen.

Die Provider legen sehr viel Wert auf hohe Sicherheitsstandards. Sie versuchen auch ihren Kunden die Sicherheitsproblematik klarzumachen. Viele kleinere Unternehmen haben aber nicht mit dem Wartungsaufwand gerechnet, den ein Internetanschluß mit sich bringt. Aus diesem Grund lagern die meisten Unternehmen, die neu im Internet sind, die Sicherheitsproblematik aus. In den meisten Fällen übernimmt das der für das Unternehmen zuständige Provider.

Die größeren Unternehmen haben ihr eigenes „corporate network„ für das sie eigene, besonders hohe Sicherheitsstandards entwickelt haben.

Auf dem Bankensektor gibt es große Unterschiede das Thema Sicherheit betreffend. Einige Banken legen großen Wert auf einen hohen Sicherheitsstandard, andere wiederum haben bis 1995 Kontoauszüge etc. im Klartext, d.h. unverschlüsselt übertragen.

5..1 Trends

Ein Bereich der Zuwachsraten verzeichnet, ist jener der virtuellen Shopping Malls. Aber auch hier besteht das Problem der Authentizierung. Aus diesem Grund etablieren sich Banken, vor allem in den USA, auf diesem Sektor. Die Daten der aktuellen Bankkunden sind bekannt, die der neuen werden erfaßt und so wird ihnen automatisch der Zugang zur bankeigenen Shopping Mall ermöglicht. Ein weiterer Vorteil ist die enge Bindung des Bankkunden an das Geldinstitut.

Die größte Bedeutung wird aber dem Internet Banking zukommen. Im Moment wird das Wachstum des Internet Banking durch Sicherheitsbedenken, Konsumentenverhalten, technologische Umsetzung etc. noch beschränkt. Laut einer Studie von Booz, Allen & Hamiton [37]sollten bis Ende 1996 ca. 285 Banken im Internet vertreten sein. 1997 soll die Zahl der „Internet-Banken„ auf über 900 steigen. Dadurch werden an die Sicherheitsstrukturen der Banken noch höhere Ansprüche gestellt.

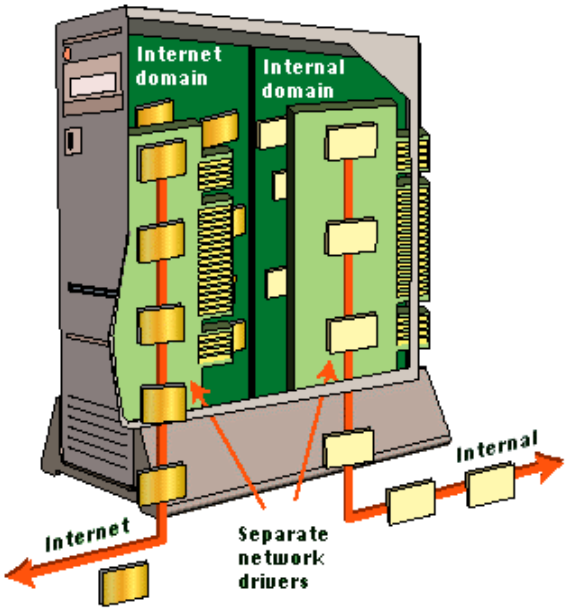
Weitere absehbare Trends betreffen das Inter- ,Intranet selbst. Die Entwicklung geht in die Richtung, daß das Intranet, vom Aufbau her, vom Internet nicht zu unterscheiden sein wird. Mit ein und derselben Software soll auf beide Bereiche zugegriffen werden können. Das Intranet wird, wie auch die eigene Homepage, in HTML verfaßt werden.

[37] Booz, Allen & Hamilton, Internet Banking Survey, 1996 zitiert in offizieller Publikation der Firma Unisys, Marktentwicklungen im Internet Banking

6. Glossar

6..1.1.11. Applikationsbasierte Firewalls

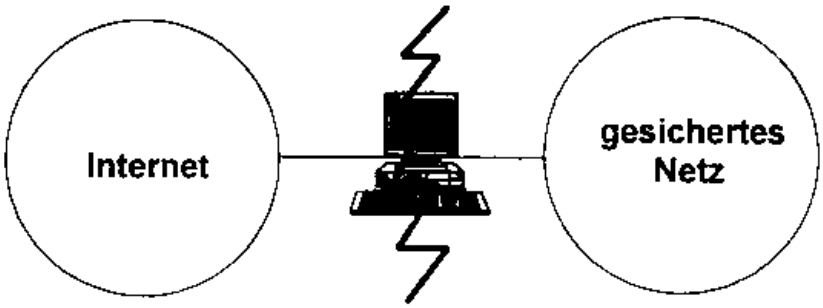
Diese Maßnahmen setzen in dem bereits angeführten ISO/OSI Schichtenmodell auf Schicht 7 (DoD Schicht 4) an.



Man spricht in diesem Zusammenhang auch von einem „Dual Homed Gateway„, was zum Ausdruck bringt, daß es sich um einen Rechner handelt, der in zwei oder mehreren Netzwerken gleichzeitig präsent ist.

Die Funktionsweise dieser Firewalls auf Applikationsebene ist von zwei weiteren wichtigen Eigenschaften geprägt:

- Der direkte Verkehr auf TCP/IP Ebene ist gänzlich blockiert
- kleine Applikationen, sogenannte Proxies kontrollieren die Kommunikation



Die Proxy Applikationen wählen nach Kriterien, die den Filterlisten der Packet Filtering Firewalls entsprechen, Pakete aus, diese „schaufeln„ sie dann vom Lokalen Netz ins Internet und, darin besteht der Unterschied zur Router-Lösung, auch vice-versa.
Das Ergebnis ist eine größere Eindringtiefe ins lokale Netz, ohne aber Sicherheitseinbußen in Kauf nehmen zu müssen.

6..1.1.12. CGI (Common Gateway Interface)[38]

[38] http://www.boku.ac.at/htmleinf/heinwas.html

CGI-Programme sind Programme oder Shell-Scripts, die auf dem WWW-Server laufen, eventuelle Dateneingaben des Clients verarbeiten und die Ergebnisse im HTML-Format an den Client-Rechner senden.

6..1.1.13. Client[39]

Clients (Kunden) sind die Benutzer, die Informationen haben wollen. Client-Programme sind die Programme, mit denen die Benutzer von ihren eigenen Rechnern (PCs) aus auf die Informationen, die auf den Servern gespeichert sind, zugreifen. WWW-Client-Programme werden auch als Web-Browser bezeichnet.

6..1.1.14. Cookies

Siehe HTTP-Cookies

6..1.1.15. Domain[40]

Verwaltungsgebiet, der ein bestimmter Internet-Rechner zugehört. Ein Beispiel hierfür wäre wu-wien.ac.at, wobei „at„ angibt, daß der Rechner sich in Österreich befindet, „ac„, daß er dem akademischen Netz zugeordnet ist, und „wu-wien„ beschreibt den Teilbereich dieses Netzes (eben die Wirtschaftsuniversität Wien).

6..1.1.16. Email (elektronische Post)[41]

Bildet die Funktionen der „Gelben Post„ in Rechnernetzen nach. Dabei werden alle Nachrichten elektronisch erstellt, versendet, empfangen und gespeichert. Dies ermöglicht den „papierlosen„ Austausch der verschiedensten Nachrichtenarten, beispielsweise von Briefen und Grafiken.

6..1.1.17. HTML (Hypertext Markup Language)[42]

HTML ist das Format, in dem die Text- und Hypertext-Informationen im WWW gespeichert und übertragen werden. Der offiziell gültige Standard ist HTML 2.0, aber neue, erweiterte Versionen HTML 3.x werden vom W3-Consortium laufend in mehreren Einzelschritten entwickelt und sind

[39] http://www.boku.ac.at/htmleinf/heinwas.html
[40] Hansen, Einführung in die Wirtschaftsinformatik I, 381
[41] Hansen, Einführung in die Wirtschaftsinformatik I, 326
[42] http://www.boku.ac.at/htmleinf/heinwas.html

bereits teilweise als De-facto-Standard verfügbar. HTML ist eine "Content-based Markup Language" mit SGML-Syntax. HTML unterstützt ein logisches Markup, bei dem die logische Bedeutung der Textteile so festgelegt wird, daß sie vom jeweiligen Web-Browser in der für den Benutzer (Client) optimalen Form dargestellt werden können. HTML-Files können mit einfachen Text-Editoren oder mit speziellen Hilfsprogrammen erstellt werden. (siehe auch Geschichte und Referenzen)

6..1.1.18. HTTP (Hypertext Transfer Protocol)[43]

HTTP ist das Protokoll, nach dem die Informationen zwischen WWW-Servern und WWW-Clients über das Internet übertragen werden.

6..1.1.19. Http-Cookies

Ein Cookie ist ein kleines Stück Information, welches von einem WWW-Server an alle Clients geschickt wird, die Informationen innerhalb eines bestimmten Zeitraums und innerhalb eines festgelegten Bereichs abrufen. Das Cookie wird gleichzeitig mit der abgerufenen Information an den Client übertragen. Typischerweise wird ein solches Cookie durch ein CGI-Skript generiert. Ein Cookie wird als ganz normales Textfile auf der Festplatte des Clients gespeichert und bleibt dort so lange erhalten bis es vom User gelöscht wird, bzw. vom Erzeuger inaktiviert wird.[44]
Wenn ein Browser nun das nächste mal einen bestimmten URL von einem http-Server aufrufen will, so vergleicht dieser zuerst die Domain und danach den URL der aufgerufenen Seite mit sämtlichen auf ihn gespeicherten Cookies. Wenn die Domain und der URL übereinstimmen, sendet der Browser den auf ihn gespeicherten Cookie zusammen mit dem http-request an den Server.

Praktische Bedeutung von Cookies

Weglassen der ID-number
Mit Hilfe von Cookies ist es nur einmal nötig sich zu identifizieren. Ab diesem Zeitpunkt erkennt der betreffende Server, daß jemand sich bereits einmal identifiziert hat und gestattet freien Zugang.
Erleichterungen beim electronic shopping
Der Warenkorb, den sich jemand in einer electronic shopping mall einmal zusammengestellt hat, geht nicht verloren, wenn der Betroffene diese vorzeitig verläßt. Beim nächsten Aufruf steht er ihm wieder zur Gänze zur Verfügung.
Site- personalization

[43] http://www.boku.ac.at/htmleinf/heinwas.html
[44] http://home.netscape.com/newsref/std/cookie_spec.html

Mittels Cookies ist es möglich jedem Besucher eines URLs eine persönliche Werbung zu präsentieren, da in Cookies Interessensgebiete des Aufrufenden abgespeichert werden können. Zum Beispiel läßt Benutzer Search.com dem Benutzer die zwanzig populärsten Suchhilfen auswählen. Bei der nächsten Benutzung dieser Site, bekommt man eine persönliche Seite präsentiert, welche eben diese vormals ausgewählten 20 links enthält[45]. Durch diese Technik ist es auch möglich gleichzeitig zwei verschiedenen Besuchern zwei völlig verschiedene Seiten zu präsentieren. z.B. könnte man jemandem, der beim letzten Besuch an Automobilen Interesse gezeigt hat, Werbung für die neuesten Modelle einspielen, während Jemand, der sich regelmäßig über Reisen informiert zur selben Zeit der neueste Billigflug offeriert wird.

Website-tracking

Es gibt eigene Firmen, die sich darauf spezialisiert haben, umfassende Analysen hinsichtlich der Interessen von Benutzern durchzuführen. Es werden hierbei Browser-Cookies kombiniert mit normalen Logfiles eingesetzt, um Besucher auf ihrem Weg innerhalb der Seiten eines bestimmten Anbieters genau zu folgen[46] .Dadurch lassen sich detaillierte Aussagen machen, welche Seiten sich Jemand angesehen hat und auch die Seiten über die Jemand „ein-„ und wieder „ausgestiegen„ ist. Vor allem die Reihenfolge der angesehenen Seiten läßt einige Aufschlüsse über die Interessenslagen einer bestimmten Person zu.

6..1.1.110. Internet[47]

Das Internet ist das umfangreichste Computer-Netzwerk der Welt. Es verbindet mehrere Millionen Computer (einschließlich PCs) und mehrere zehn Millionen Menschen. Der Name kommt von "Interconnected Networks" (verbundene Netze); das Internet ist ein Zusammenschluß von vielen lokalen, nationalen und internationalen Computer-Netzen, die alle das Protokoll TCP/IP verwenden und die jeweils lokal, nicht über eine Welt-Zentrale, verwaltet werden ("Domains"). Das Internet unterstützt viele verschiedene Services. Die wichtigsten sind: "Telnet" für den Aufruf von Programmen auf anderen Computern, "FTP" (File Transfer Protocol) für die Übertragung von Files auf andere Computer, "Electronic Mail" (elektronische Briefpost), "Usenet News" (Veröffentlichungen in Diskussionsforen) und "IRC" (Internet Relay Chat) für den Austausch von Informationen mit anderen Computerbenutzern, "WWW" und "Gopher" für den Zugriff auf Informationssysteme in aller Welt. (siehe auch Geschichte und Referenzen)

6..1.1.111. IP-Adresse[48]

[45] http://www.macworld.com/netsmart
[46] http://www.ipro.com/netline/about.html#Solutions
[47] http://www.boku.ac.at/htmleinf/heinwas.html
[48] Hansen, Einführung in die Wirtschaftsinformatik I, 380

Jeder Internet-Rechner besitzt eine IP-Adresse (Internet-Protokoll-Adresse) und kann anhand dieser eindeutig identifiziert werden. Eine IP-Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennten Zahlen. Für jede dieser Zahlen stehen daher acht Bits zur Verfügung, womit sie maximal 256 Werte annehmen können.

6..1.1.112. JavaScript[49]

JavaScript ist eine von der Firma Netscape erfundene Sprache zur Ausführung von bestimmten Aktionen innerhalb des Netscape-Browsers. Im Gegensatz zu Java ist diese Sprache weder plattformunabhängig noch mit den notwendigen Sicherheitsmechanismen ausgestattet.

6..1.1.113. Mailbox[50]

Jeder Teilnehmer hat in einem bestimmten Postamt (Server) sein elektronisches Postfach und läßt sich durch seine Email-Adresse eindeutig identifizieren. Elektronische Postsysteme unterstützen die zeitversetzte Kommunikation zwischen den Teilnehmern, wobei zusätzlich auch Leistungen wie Zwischenspeichern und Massenversand geboten werden.

6..1.1.114. Net.Commerce Payment von IBM

Dieses Produkt basiert auf dem SET Protokoll. Es schützt die Übertragung vertraulicher Informationen von Händlern und Kunden, und stellt eine Schnittstelle zwischen involvierten Bankinstituten einerseits und dem Internet andererseits dar. Die Bank erhält von den Händlern die zur Kundenidentifizierung erforderlichen Daten in verschlüsselter Form zugesandt, überprüft die Kreditwürdigkeit des Kunden und teilt dies dem Händler mit. Der Händler selbst erhält KEINE vertraulichen Kundendaten bezüglich Kreditkartennummern etc.

6..1.1.115. Newsgroups[51]

Funktionieren wie öffentliche Verteiler, die grundsätzlich allen Internet-Teilnehmern zugänglich sind und dienen der Diskussion von verschiedensten Themengebieten. Dabei deckt jeweils eine derartige Diskussionsliste oder Newsgroup mehr oder weniger spezialisiert ein Themengebiet ab.

[49] http://www.boku.ac.at/htmleinf/heinwas.html
[50] Hansen, Einführung in die Wirtschaftsinformatik I, 326
[51] Hansen, Einführung in die Wirtschaftsinformatik I, 385f

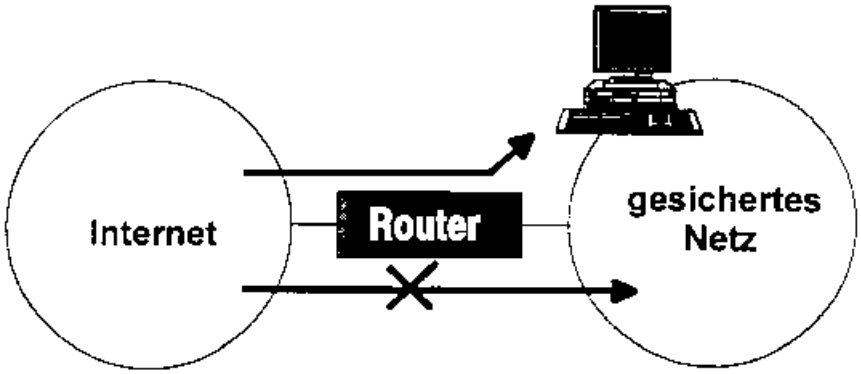
6..1.1.116. Newsforen

Siehe Newsgroups

6..1.1.117. Packet Filtering Firewalls

sind Router, die jeden Verkehr aus dem lokalen Netzwerk ins Internet zulassen, jedoch nur minimalen Paket Einlaß in das lokale Netzwerk gestatten.C
Der Router wird mit Filterlisten gefüttert, wobei die Listen Regeln über den Durchlaß von Paketen an bestimmten Ports in bestimmte Richtungen definieren.
Services wie WorldWideWeb-Server oder Telnet scheiden jedoch praktisch aus, ein Freischalten dieser Dienste führt die Installation dieser Filterlisten basierten Lösungen defacto ad absurdum. In der Regel bleiben nur E-Mail und DNS Ports geöffnet.
Als Einstiegslösung für kleinere Firmenszenarien werden häufig diese kostengünstigen intelligenten Router empfohlen.

Will man in einem solchen Szenario dennoch WorldWideWeb-Daten zur Verfügung stellen, so besteht die Möglichkeit einen „Bastion Host„ zur Verfügung zur stellen.



Der Bastion Host ist ein extrem geschützter, aber auch in seinem Leistungsspektrum extrem eingeschränkter Server, der außerhalb der Firewall plaziert ist.
Ein solcher Server bedient beispielsweise ausschließlich Port 80 und Port 443 (http und https), auf allen weiteren Ports herrscht beharrlich Schweigen. DI.Theo Hoogemoed von Siemens Österreich weis von überaus positiven Erfahrungen mit einem Bastion-Host-Konzept zu berichten, es zeigt, daß auch größere Unternehmen so effizient das Internet nutzen können. Für den unternehmensinternen Datenverkehr besteht bei Siemens seit längerem ein FDDI-Ring, Datenaustausch mit Kunden wird prinzipiell über Modem abgewickelt, die Modemzugänge werden mit Abschluß des jeweiligen Projekts wieder abgebaut.

6..1.1.118. Paßwortwahl[52]

Eigenschaften von schlechten Paßwörtern

Das Paßwort ist zu kurz. Das Paßwort wird auf einfache Art abgeleitet aus der Kennung, dem Namen des Besitzers der Kennung, Vornamen Wörtern aus natürlichen Sprachen, Namen von Orten, Zeichenfolgen, die zum persönlichen Umfeld gehören wie z.B. das Geburtsdatum oder die Hausnummer, beliebten Zeichenfolgen wie z. B. „12345678„, „xxxxxxxx„, „qwerty„ oder „qwertz„, Wörtern wie z. B. „wizard„, „guru„ oder „gandalf„.Mit „einfacher Ableitung„ sind dabei die folgenden Bildungsregeln gemeint:: der Begriff selbst, wobei nur Groß- oder nur Kleinbuchstaben verwendet werden, eine der vorhergehenden Varianten rückwärts geschrieben, eine der vorhergehenden Varianten, wobei noch zusätzlich am Anfang oder Ende eine Ziffer angefügt wird.

Das Paßwort ist so kompliziert, daß man es sich nicht merken kann und es deshalb aufschreibt. Das Paßwort ist mehreren Personen bekannt.

Eigenschaften von guten Paßwörtern.

Das Paßwort sollte die volle mögliche Zeichenkette ausnutzten. Es sollten mindestens zwei Buchstaben enthalten sein. Wenn möglich sollten dabei sowohl Groß- als auch Kleinbuchstaben verwendet werden. Im Paßwort sollten mindestens zwei Ziffern oder Sonderzeichen vorkommen. Dabei sollten diese nach Möglichkeit nicht nur am Anfang und/oder Ende stehen. Man muß sich das Paßwort leicht merken können. Das Paßwort sollte schnell eingegeben werden können. Dadurch wird der Diebstahl des Paßworts zumindest erschwert, wenn man dem Besitzer der Kennung über die Schulter schaut. Besitzt man verschiedene Kennungen (z. B. eine Kennung auf mehreren Rechnern, die nicht durch Yellow Page verwaltet werden), sollte man wenn möglich auch verschiedene Paßwörter wählen. Das Paßwort sollte in angemessenen Abständen geändert werden. Was „angemessen„ bedeutet, hängt dabei von den Sicherheitsanforderungen ab, wobei bereits auf Systemebene Wartungsprogramme eingesetzt werden sollen. Für eine normale Benutzerkennung sollte z.B. ein Intervall von zwei bis drei Monaten ausreichen. Das Paßwort darf nur dem Inhaber der Kennung bekannt sein. Aus diesem Grunde sind „Gruppenkennungen„ zu vermeiden. Dies bedeutet auch keine Funktionseinbuße, da es genügend Methoden gibt, mit denen Benutzer ohne Bequemlichkeitsverlust auf gemeinsamen Datenbeständen arbeiten können und die Gruppenkennungen überflüssig machen. Man sollte sich bei der Eingabe des Paßworts nicht über die Schulter schauen lassen.

Beispiele für mögliche Bildungsalgorithmen

Im folgenden werden zwei Bildungsregeln vorgestellt, mit denen man „gute„ Paßwörter erhält, die den vorher genannten Anforderungen genügen, und die man insbesondere sich gut merken kann:

Man wählt zwei Wörter (möglichst aus verschiedenen Sprachen) und nimmt aus ihnen jeweils drei aufeinanderfolgende Buchstaben (z. B. den Wortanfang oder das Wortende). Danach verbindet man diese beiden Zeichenfolgen mit zwei Sonderzeichen oder Ziffern. Zur weiteren Erhöhung der Sicherheit kann man noch gleichzeitig Groß- und Kleinbuchstaben verwenden. Beispiel:

[52] (http://www.wu-wien.ac.at/manuals/wu/pass)

„hau23HOU„, wenn man im „hau„s (Englisch „HOU„se) mit der Nr. „23„ wohnt. Der Benutzer wählt einen Satz und verwendet dann als Paßwort die Anfangs- und/oder Endbuchstaben der einzelnen Wörter, wobei er noch zwei Ziffern oder Sonderzeichen dazwischen einfügt. Beispiel: „DBweS&&v„ für den Anfang des letzten Satzes. Besitzt man mehrere Kennungen, so kann man sich nach dem folgenden Verfahren leicht zu merkende, unterschiedliche Paßwörter erzeugen: Man wählt eine fünf bis sieben Zeichen lange Zeichenfolge (z. B. mit einem der vorhergehenden Verfahren), die für alle Paßwörter gleich ist, und ergänzt sie um ein bis drei Zeichen, die aus dem Rechnernamen bzw. der Kennung abgeleitet werden (z. B. die ersten oder letzten zwei Zeichen des Rechnernamens bzw. der Kennung).Diese Bildungsregeln sollen jedoch nur als Anregung dienen. Es ist sehr erwünscht, daß jeder Benutzer sich Gedanken über einen eigenen Algorithmus macht oder die Vorschläge zumindest abwandelt. Dadurch wird verhindert, daß neue Generationen von Knack-Programmen, die auch auf diese schon häufig empfohlenen Bildungsregeln eingehen, erfolgreich sind. Insbesondere darf man nicht die Paßwörter „hau23HOU“ und „DBweS&&v“ verwenden.

Niederschreiben von Paßwörtern

Wie vorher schon erwähnt, sollte man Paßwörter wenn irgend möglich nicht aufschreiben. Ist dies dennoch nicht zu vermeiden (weil man z.B. viele verschiedene oder nur selten benutzte Kennungen besitzt), so sollte man wenigstens die folgenden Regeln beachten:

Ein Paßwort sollte niemals als Paßwort erkennbar sein. Man sollte nicht eine Kennung und das dazugehörige Paßwort zusammen auf dem gleichen Stück Papier niederschreiben. Man sollte den Zettel mit dem Paßwort nicht am Bildschirm, an der Tastatur, am Rechner, etc. befestigen. Wenn möglich sollte man beim Niederschreiben das Paßwort mit beliebigen Zeichen in einer leicht zu merkenden Art mischen, so daß es sich vom echten Paßwort unterscheidet. Ein Paßwort sollte niemals in ‘elektronischer’ Form aufbewahrt werden. Dies umfaßt die Speicherung in programmierbaren Tasten oder Dateien (z. B. ‘$HOME/.netrc’), die Mitteilung mittels E-Mail, etc.

6..1.1.119. Risiko[53]

Der Begriff Risiko umfaßt nach DIN, UDE Norm 31000 folgende zwei Bereiche:

- das zu erwartende Schadensausmaß bei Eintritt des Ereignisses
- die zu erwartende Häufigkeit mit der dieses gefährdende Ereignis auftritt.

6..1.1.120. Server[54]

[53] Kyas; Sicherheit im Internet; 1996

[54] http://www.boku.ac.at/htmleinf/heinwas.html

Server (Verkäufer, Bedienender) sind die Computer, auf denen die Informationen gespeichert sind. WWW-Server laufen meistens auf Unix-Rechnern und werden auch als HTTP-Dämonen bezeichnet. Es gibt mehrere solche Softwareprodukte, sowohl public domain als auch kommerziell.

6..1.1.121. SSL (Secure Sockets Layer)

Dieses von Netscape Communication Corporation entwickelte Protokoll beinhaltet eine Server Authentizierung, Datenverschlüsselung und Gewährleistung der Datenintegrität. SSL arbeitet zwischen der TCP/IP Protokollebene und den Applikationsprotokollen (HTTP, Telnet, FTP, Gopher, NNTP, etc.) auf dem Transport Layer. SSL ist somit applikationsunabhängig und erlaubt, sofern Server und Client SSL unterstützen, eine verschlüsselte und somit sichere Datenübertragung. TradeVPI von TradeWave
VPI (Virtual Private Internet) setzt auf dem Internet auf und baut ein sog. virtuelles privates Netzwerk auf. Server und/oder Clients, welche an ein VPI-System angeschlossen sind, funktionieren wie ein eigenes Netzwerk. Dieses ´private´ Netzwerk ist durch Zugangskontrolle, User Authentizierung und Datenverschlüsselung geschützt. Ein weiters Produkt, nämlich VPN (Virtual Private Networks), umfaßt dieselben Funktionen, jedoch abgestimmt auf Intranets.

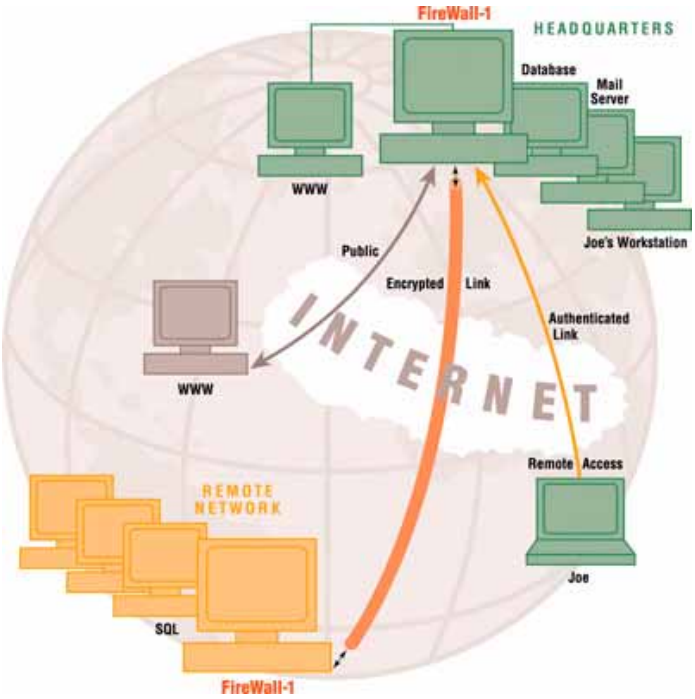
6..1.1.122. URL (Uniform Resource Locator)[55]

URL ist die "Adresse", die das Client-Programm benötigt, um eine bestimmte Information vom jeweiligen Server-Computer zu erhalten. Der URL enthält zu diesem Zweck Informationen wie die Art des Zugriffs (Protokoll), die Adresse des Server-Computers (Hostname), eventuell mit einem Username und Paßwort oder einer Port-Nummer, und das Directory und den Filenamen der Datei, in der die gewünschte Information gespeichert ist, sowie eventuell die Stelle innerhalb der Datei oder die Parameter für ein CGI-Programm oder für einen Suchvorgang.

[55] http://www.boku.ac.at/htmleinf/heinwas.html

6..1.1.123. Virtual Privat Networks (VPN)

Stellen wir uns folgendes Szenario vor: Ein österreichisches Unternehmen der möchte mit einer auf mehrere Jahre eingerichteten Außenstelle in Ostasien regen Datenaustausch betreiben. Aus Kostengründen, und zumal Internet bereits im Haus vorhanden ist, soll dieses Medium für den Datenaustausch genützt werden. Sicherheitsmaßnahmen auf Dokumentenbasis, wie der Versand PGP verschlüsselter Daten, als Attachments per E-Mail, scheidet aufgrund der zu hohen Risiken im Bereich der falschen Handhabung durch den Endbenutzer aus - was tun ?



Hier ist der richtige Einsatzbereich für Virtual Private Networks - Sicherheitseinrichtungen, wo zwischen zwei oder mehreren Firewalls, über verschlüsselte Kanäle ungestörter Datenaustausch wie wir ihn aus einem WAN kennen, abgewickelt wird.
Laut dem Sicherheitsbeauftragten eines Internationalen Service Providers bieten VPNs „optimalen Schutz„.
Wir wollen, einer Empfehlung von eines Service Providers folgend, ein VPN durch die folgende Grafik illustrieren:[56]

Von den befragten Unternehmen, die nicht als Internet-Service-Provider auftreten, unterhielt zum Zeitpunkt der Umfrage noch kein Unternehmen ein VPN, das Konzept wird jedoch bereits in einigen Unternehmen angedacht.

[56] Vgl. http://www.checkpoint.com/brochure/page3.html

6..1.1.124. VeriFone´s Internet Commerce[57]

Wie die Grafik zeigt, benötigt man als Benutzer lediglich einen SSL-fähigen Browser. Die eigentliche Implementation findet beim Händler statt. Dieses System beinhaltet eine Verschlüsselung und eine digitale Unterschrift, womit eine eindeutige Authentizierung möglich wird.

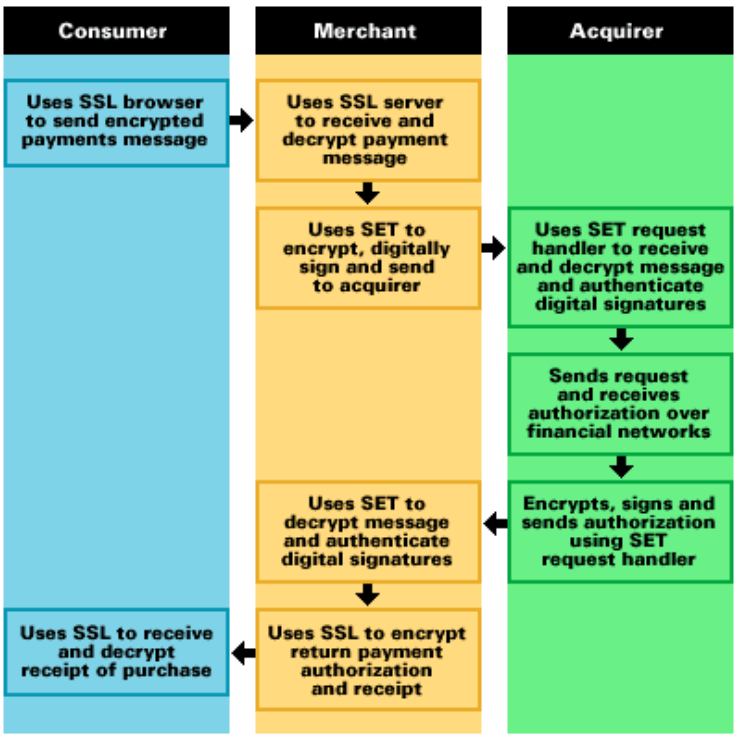


Figure 6. Message flow using VeriFone's Secure Merchant Transactions Implementation

6..1.1.125. Web-Browser[58]

Als Web-Browser bezeichnet man Client-Programme für den Zugriff auf WWW-Server. Es gibt viele verschiedene solche Programme, sowohl public domain als auch kommerziell. Manche wie z.B. Lynx unterstützen nur die Textausgabe und funktionieren in einem einfachen Zeilenmodus mit Tastatursteuerung, die meisten wie z.B. Mosaic und Netscape unterstützen auch Bilder und funktionieren nur auf einer graphischen Benutzeroberfläche mit Maus oder Touch-Screen. Spezielle Browser-Programme können die Informationen auch in Blindenschrift oder akustisch (als gesprochene Texte) oder in Form von dreidimensionalen Virtual-Reality-Szenen darstellen. Die meisten Web-Browser unterstützen nicht nur den Zugriff auf WWW-Server sondern auch auf Gopher-Server und auf andere Internet-Services wie Telnet und FTP sowie mit Einschränkungen auch Electronic Mail und Usenet News. (siehe auch Geschichte und Referenzen)

6..1.1.126. WWW (World Wide Web)[59]

WWW ist ein Informationssystem, das einen bequemen Zugriff auf Informationen, die auf vielen verschiedenen Computern gespeichert sind, in der Form von Hypertext- und Hypermedia-Links ermöglicht. Der Zugriff erfolgt nach dem Prinzip von Server und Client über das Internet mit dem Protokoll HTTP. Textinformationen werden auf den WWW-Servern in der Form von HTML-Files gespeichert. Außerdem können auch Bilder, Töne und beliebige sonstige Files über das WWW übertragen werden, und es können auch Benutzereingaben von Programmen, die auf dem WWW-

[57] http://www.verifone.com
[58] http://www.boku.ac.at/htmleinf/heinwas.html

Servern laufen, verarbeitet werden (Formulare, Suchvorgänge u.a.). WWW wurde am europäischen Kernforschungszentrum CERN in Genf entwickelt und wird vom W3-Consortium weiter entwickelt. Der Name bedeutet so etwas wie ein "weltweites Spinnennetz". (siehe auch Geschichte und Referenzen)

[59] http://www.boku.ac.at/htmleinf/heinwas.html

7. Literaturverzeichnis

7..1 Literatur:

1. Bauknecht, K.; Teufel,S.; Sicherheit in Informationssystemen, Proceedings der Fachtagung SIS '94, Verlag der Fachvereine, Zürich 1994
2. Bernstern, T.; Bhimani, A. B.; Schultz, E.; Siegel C. A.; Internet Security for Business, Wiley Computer Publishing, New York, 1996
3. Brandl und Schönberger,ecolex 96, - Die Haftung von Online-Diensten für übermittelte Inhalte
4. Grimm, R.; Zangeneh, K; Cypermoney im Internet, Teil 1, in: Ausgabe 5/96, D - Mölln, 1996
5. Grimm, R.; Zangeneh, K; Cypermoney im Internet, Teil 2, in: Ausgabe 6-7/96, D - Mölln, 1996
6. Hansen, H.R.: Wirtschaftsinformatik I, Grundlagen betrieblicher Informationsverarbeitung, 7. Auflage, Lucius & Lucius, Stuttgart 1996
7. Hansen, H.R.; Klare Sicht am Info-Highway; Orac Verlag, Wien 1996
8. Kodex, Bürgerliches Recht, Orac, Wien, Stand 1.9.1995
9. Koziol-Welser, Grundriß des bürgerlichen Rechts I, Wien 1996, 10. Auflage
10. Kyas, Othmar, Risikoanalyse - Strategien - Firewalls, Wien, 1996
11. Meyers großes Taschenlexikon Band 20, Bibliographisches Institut & F. A. Brockhaus AG, Mannheim 1987
12. Peter Madl, ecolex 1996, Vertragsabschluß im Internet, Wien, 1996
13. Rivest, R.; Shamir, A; Adleman, L.: A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Com ACM 21 (2), Washington, Feb 1978
14. Scheller, M.; Boden, K.P.;Greenen, A.; Kampermann, J.; Internet: Werkzeuge und Dienste; Springer Vlg. Berlin, Heidelberg; 1994
15. Stabentheiner, J.; ecolex 1996, - Straf- und zivillegislativer Handlungsbedarf durch Datenhighway im Internet, Wien, 1996
16. Unisys, Marktentwicklungen im Internet Banking, Wien, 1996

7..2 Zeitschriften

1. iX; N.N.; Die Bank24 im Internet; Ausg 12; H.Heise Vlg.; Hannover; 1996
2. iX; N.N.; Apache Server; Ausg 6; H.Heise Vlg.; Hannover; 1996
3. Homepage - Das Internetmagazin für professionelle Anwender; Klaus Dünser; Security; Ausg 5; Atlas-Zeitschriften Vlg.; 1996

7..3 Adressen

Recht: http://home.netscape.com/Newsref/std/cookie_spec.html
http://www.macworld.com/netsmart
http://www.ipro.com/netline/about.html#Solutions
http://www.illuminatus.com/cookie-fcgi
http://www.macworld.com/netsmart

Organisation: http://www.cert.dfn.de
http://www.cs.rpi.edu/ifip
http://www.cpsr.org
http.//www.usenix.org
http://www.nsa.gov:8080
http://www.isoc.org

Linkpage: http://strv.trans.univie.ac.at/peter/intralinks/links.html
FIREWALL: http://www.checkpoint.com/brochure/page3.html 20.12.1996
Zahlungs-
abwicklung http://www.fv.com/
http://www.cybercash.com/pub/draft-cybercash-v08-00.txt
http://www.digicash.com/ecash/ecash-home.html
http://www.cwi.nl/cwi/projects/cafe.html
http://www.deutsche-bank.de/
Paßwörter http://www.wu-wien.ac.at/manuals/wu/pass

Secure ID http://info.arnold.af.mil/hpc/card.gif

http://www.onsite.net/faq/intranet.htm

http://www.onsite.net/faq/intranet.htm

http://www.tradewave.com

http://www.verifone.com

Newsgroups zum Thema Internet-Sicherheit

alt.2600„

alt.cyberpunk

alt.cyberpunk.movement

alt.cyberpunk.tech

alt.cyberpunk.chatsubo

alt.cyberspace

alt.hackers

alt.security

comp.risks

comp.security.unix

comp.virus

misc.legal.computing