Universität Potsdam
Institut für Informatik
Sommersemester 2005
Prof. Dr. K. Rebensburg
Dipl. Inf. T. J. Wilke

Seminar

Trust Management und Security Policy Enforcement

Autoren: Stefan Bär, Bettina Buchholz, Andreas Erber, Robert Fiebelkorn, Tim Friese, Sebastian Fudickar, Steven Grigoleit, Sascha Jütterschenke, Björn Knuth, Benedikt Meuthrath, Stephan Müller, Tobias Nöring, Michal Olejniczak, Jan Schaumkessel, Kerstin Seidel, Maximilian Seifert, Christian Simonsky, Christian Tinnefeld, Katja Warczecha, Mario Wegner, Michael Werlitz

Datum: Potsdam, 7. August 2005

Inhaltsverzeichnis

1 eGovernment in Deutschland **1**

1.1 Abstract . . . 1
1.2 Einleitung . . . 1
1.2.1 Definition von eGovernment . . . 1
1.2.2 Wo beginnt eGovernment? . . . 1
1.3 eGovernment in Deutschland . . . 2
1.4 eGovernment im Beziehungs-geflecht . . . 3
1.4.1 Government to Citizens (G2C) . . . 3
1.4.2 Government to Business (G2B) . . . 4
1.4.3 Government to Government (G2G) . . . 5
1.4.4 Erwartungen aus Sicht der Bürger . . . 5
1.5 Elektronische Signatur . . . 6
1.5.1 Basis der elektronischen Signatur . . . 6
1.6 Datenschutz und Datensicherheit . . . 8
1.6.1 Datenschutz . . . 8
1.7 Standards . . . 10
1.8 Anforderungen an eGovernment . . . 11
1.8.1 Authentifizierung . . . 12
1.8.2 Verifikation des Clients . . . 13
1.8.3 Nutzerzentriertes Design . . . 13
1.8.4 Datenschutz . . . 13
1.9 Fazit . . . 14
1.10 Ausblick . . . 14

2 Digitale Karten **16**

2.1 Abstract . . . 16
2.2 Einleitung . . . 16
2.3 Historische Entwicklung digitaler Karten . . . 17
2.4 Aufgaben digitaler Karten . . . 18
2.4.1 Identifikation und Informationssicherheit . . . 18
2.4.2 Anforderungen und Realität . . . 19
2.5 Technologien digitaler Karten . . . 20
2.5.1 Hochgeprägte Karten . . . 20
2.5.2 Magnetstreifenkarten . . . 21

2.5.3 Chipkarten . . . 22
2.5.4 Optische Speicherkarten . . . 25
2.6 Angriffe auf Chipkarten . . . 25
2.6.1 Time Attack . . . 26
2.6.2 Bellcore-Angriff . . . 26
2.6.3 Differentielle Fehler-Analyse . . . 26
2.6.4 Direkte Angriffstechniken gegen Chipkarten . . . 26
2.6.5 Stromverbrauchsanalyse . . . 27
2.7 Kategorisierung digitaler Karten . . . 27
2.7.1 Single-Vendor-Single-Application . . . 27
2.7.2 Single-Vendor-Multi-Applications . . . 28
2.7.3 Multi-Vendor-Single-Application . . . 28
2.7.4 Multi-Vendor-Multi-Applications . . . 28
2.8 Beispiele digitaler Karten . . . 29
2.9 Zusammenfassung . . . 30

3 eHealth: Gesundheitskarte, elektronische Rezepte 33
3.1 Abstract . . . 33
3.2 Einleitung . . . 33
3.3 Status heute . . . 34
3.4 Internationaler Vergleich . . . 34
3.5 Konzept Gesundheitskarte . . . 36
3.5.1 Gesetzgebung . . . 36
3.5.2 Erwartungen (qualitative und ökonomische Gesichtspunkte) . . . 36
3.5.3 Zielsetzung der Telematik . . . 37
3.6 Sicherheit und Schutzmechanismen . . . 38
3.6.1 Technische Sicherheitsmechanismen . . . 38
3.6.2 Umsetzung von eHealth . . . 40
3.6.3 Performanz und Verfügbarkeit . . . 41
3.7 Kritik . . . 42
3.8 Fazit . . . 43

4 ELSTER - die elektronische Steuererklärung 49
4.1 Abstract . . . 49
4.2 Einleitung - Was ist ELSTER? . . . 50
4.2.1 Was ist ELSTER? . . . 50
4.2.2 Zeitliche Entwicklung . . . 50
4.2.3 Ziele . . . 51
4.2.4 Möglichkeiten/Fähigkeiten . . . 52
4.3 Architektur . . . 52
4.4 Sicherheitskonzept . . . 56
4.4.1 Eingesetzte Sicherheitsmechanismen . . . 56
4.4.2 Technische Schwachstellen . . . 58
4.5 Gesellschaftliche Aspekte . . . 59

4.5.1 Rechtliche Grundlagen . . . 59
4.5.2 Bekanntmachung des Systems . . . 60
4.5.3 Annahme durch die Bevölkerung . . . 61
4.5.4 Andere Staaten . . . 61
4.6 Fazit . . . 62

5 e-Banking - Technische Systeme, Handhabungspraxis, Verträge 66
5.1 Abstract . . . 66
5.2 Motivation . . . 66
5.3 Electronic Banking - ein Überblick . . . 67
5.3.1 Definition e-Banking . . . 67
5.3.2 Bereiche . . . 67
5.3.3 Merkmale . . . 69
5.4 Technische Systeme . . . 69
5.4.1 Überblick . . . 69
5.4.2 Sicherheitskonzepte . . . 69
5.4.3 Verschlüsselungssysteme . . . 74
5.5 Handhabungspraxis . . . 75
5.5.1 Marktsituation . . . 75
5.5.2 Allgemeine Sicherheitsrisiken . . . 77
5.6 Rechtliche Aspekte . . . 80
5.6.1 Verträge . . . 81
5.6.2 Bankenaufsicht . . . 82
5.6.3 Rechtsrahmen . . . 83
5.7 Fazit und Ausblick . . . 83
5.8 Glossar . . . 85

6 Online-Auktionen: Technische Systeme, vertragliche Situation 88
6.1 Einleitung . . . 88
6.2 Technische Systeme . . . 89
6.2.1 Vorstellung der Auktionsplattformen . . . 89
6.2.2 Passwörter . . . 90
6.2.3 Phishing / Passwortklau . . . 91
6.2.4 Identitätsfeststellung . . . 93
6.2.5 Bewertungssysteme . . . 95
6.2.6 Sicherheitsverbindung . . . 95
6.2.7 Fazit . . . 96
6.3 Vertragliche Situation . . . 97
6.3.1 Online-Auktionen vs. Klassische Auktionen . . . 98
6.3.2 Vertragsverhältnisse bei Online-Auktionen . . . 98
6.3.3 Bewertungen bei Online-Auktionen . . . 101
6.3.4 Beweislast bei Vertragsschluss . . . 102
6.3.5 Fazit . . . 103
6.4 Zusammenfassung . . . 104

7 Elektronisches Publizieren **107**
7.1 Einleitung . . . 107
7.2 Elektronisches Publizieren . . . 107
7.2.1 Microsoft Word . . . 107
7.2.2 Adobe FrameMaker . . . 108
7.2.3 XSL-FO (XSL Formatting Objects) . . . 108
7.3 Elektronische Presse . . . 109
7.3.1 Rhein Main Presse . . . 110
7.3.2 Füssener Internet Zeitung . . . 110
7.4 Großbaustelle Urheberrecht . . . 110
7.4.1 „Erster Korb“ . . . 111
7.4.2 „Zweiter Korb“ . . . 112
7.5 Gefährdete Werte und Nutzungsrechte . . . 113
7.6 DRM-Referenzmodell . . . 115
7.7 DRM-Hardwareumsetzung (TPM/TCG/TCPA) . . . 116
7.7.1 Kritik . . . 117
7.7.2 Next Generation Secure Computing Base (NGSCB) . . . 117
7.8 DRM-Softwareumsetzung . . . 118
7.8.1 Microsoft Windows Media digital rights management . . . 118

8 Elektronischer Vertragsabschluss **121**
8.1 Zusammenfassung . . . 121
8.2 Allgemeiner Vertragsabschluss . . . 121
8.3 Technische Grundlagen . . . 123
8.3.1 Public-Key-Verfahren . . . 123
8.3.2 Algorithmen und Standards . . . 126
8.3.3 Elektronische Signatur . . . 127
8.4 Signaturgesetz . . . 129
8.4.1 Begriffsbestimmungen . . . 129
8.5 Elektronischer Vertragsabschluss . . . 131
8.5.1 Elektronischer Vertragsabschluss ohne Signatur . . . 133
8.5.2 Elektronischer Vertragsabschluss mit Signatur . . . 134
8.6 Probleme der Elektronischen Signatur . . . 134
8.6.1 Aufwand . . . 135
8.6.2 Gültigkeit einer Signatur – Nachsignierung . . . 135
8.6.3 Sicherheit der elektronischen Signatur . . . 135
8.6.4 Rechtliche Fragestellungen . . . 135
8.6.5 Allgemeine Akzeptanz . . . 136
8.7 Fazit . . . 137

9 Social Engineering **139**
9.1 Einleitung . . . 139
9.1.1 Risikofaktor Mensch - psychologische Grundlagen . . . 139
9.2 Social Engineering . . . 141

9.2.1 Phasen des Social Engineering . . . 141
9.2.2 Kombination von Social Engineering und Technologie . . . 144
9.2.3 Covert Channel . . . 145
9.3 Abwehr von Social Engineering . . . 146
9.3.1 Warnzeichen für einen Social Engineering Angriff . . . 146
9.3.2 Gegenmaßnahmen . . . 146
9.3.3 Evaluierung von Gegenmaßnahmen . . . 148
9.4 Zusammenfassung . . . 149

10 Kombinierte Angriffe **152**
10.1 Abstract . . . 152
10.2 Einleitung . . . 152
10.3 Ursachen der Bedrohungen von IT-Infrastukturen . . . 154
10.3.1 Motivation der Angreifer . . . 154
10.3.2 Technische und Organisatorische Schwachstellen heutiger IT-Systeme . . . 154
10.4 Klassen von Schadenssoftware (Malware) . . . 157
10.5 Gegenmaßnahmen zur Gefahrenabwehr . . . 158
10.5.1 Reaktive Maßnahmen . . . 159
10.5.2 Proaktive Maßnahmen . . . 160
10.6 Beispielhafte Blended Threats . . . 162
10.6.1 Nimda . . . 162
10.6.2 JS Scob . . . 163
10.6.3 Lovgate . . . 164
10.7 Social Engineering . . . 165
10.7.1 Computer Based Social Engineering . . . 165
10.7.2 Human Based Social Engineering . . . 166
10.7.3 Reverse Based Social Engineering . . . 166
10.8 Phishing . . . 166
10.8.1 Übertragung der Phishingangriffe . . . 167
10.8.2 Täuschungsmanöver der Angreifer . . . 169
10.8.3 Abwehrmechanismen . . . 170
10.9 Zusammenfassung und Ausblick . . . 171

11 Staatliche und öffentliche Einrichtungen: BSI, CERT, ENISA **175**
11.1 Management Summary . . . 175
11.2 Das BSI . . . 176
11.2.1 Aufgabenspektrum des BSI . . . 177
11.2.2 Die Köpfe / das Management des BSI . . . 178
11.2.3 Die wichtigsten Anwendungsbereiche des BSI . . . 179
11.3 ENISA . . . 180
11.3.1 Ziele . . . 180
11.3.2 Aufgaben . . . 180
11.3.3 Organisation . . . 181

11.3.4 Überprüfungsklausel 182
11.3.5 Zusammenfassung 182
11.4 CERT 183
11.4.1 Analyse der Sicherheitslücken und Reaktion auf Vorfälle 183
11.4.2 Survivable Enterprise Management 184
11.4.3 Ausbildung und Training 184
11.4.4 Überlebensfähige Netzwerktechnologien 184
11.4.5 Zusammenfassung 185

1 eGovernment in Deutschland

B.Sc. Sebastian Fudickar, Stefan Bär

1.1 Abstract

Dieses Paper soll eine Einführung in das eGovernment in Deutschland geben. Dazu soll nach einer kurzen Einleitung in Kapitel 10.2 der Entwicklungsprozess von eGovernment Anwendungen näher betrachtet werden. Kapitel 1.3 beschreibt die Kommunikationsbeziehungen der verschiedenen Nutzergruppen von eGovernment-Anwendungen. In den folgenden Kapiteln werden entscheidende Techniken und Aspekte von eGovernment Anwendungen näher veranschaulicht. So werden in Kapitel 1.5 digitalen Signaturen vorgestellt. Kapitel 1.6 befasst sich mit dem Datenschutz. Daraufhin wird in Kapitel 1.7 SAGA vorgestellt, eine im Zuge von bundOnline2005 konzipierte Referenz, zum Aufbau von eGovernment-Anwendungen. Abschließend werden in Kapitel 6.3.5 und Kapitel 1.10 Gefahrenstellen bezüglich der Datensicherheit und Nutzbarkeit bisheriger eGovernment-Realisierungen aufgezeigt.

1.2 Einleitung

1.2.1 Definition von eGovernment

Unter Elektronik-Government welches im Allgemeinen auch als eGovernment bezeichnet wird, versteht man die Abwicklung geschäftlicher Prozesse im Zusammenhang mit der Regierung bzw. Verwaltung (Government [1]) eines Staates mit Hilfe elektronischer Medien. In Deutschland bezieht sich dies auf Verwaltungen auf kommunaler-, Bundes- und Landesebene.

1.2.2 Wo beginnt eGovernment?

Als eGovernment wird meist schon das allgemeine Vorhandensein einer Website mit Informationen zu Anträgen die Öffnungszeiten einzelner Behörden gesehen. Allerdings

[1] Government engl. für Regierung bzw. Staat

beginnt richtiges eGovernment im Sinne der Definition erst mit der tatsächlichen Abbildung von behördenbezogenen Geschäftsprozessen, wie Antragsstellungen in elektronischer Form. Dabei ist es keinesfalls ausreichend Antragsformulare zum handschriftlichen Ausfüllen online zur Verfügung zu stellen. Zum eGovernment gehört die vollständige elektronische Antragstellung, Bearbeitung und Bescheiderteilung.

1.3 eGovernment in Deutschland

In Deutschland starteten erste Initiativen zum e-Government bereits 1998 in einem durch die Bundesregierung geförderten Projekt mit dem Namen "Media@Komm". Dabei wurden über 300 praktischen eGovernment-Lösungen zur Schaffung virtueller Rathäuser und Verwaltungen in unterschiedlichen Regionen Deutschland umgesetzt. Diese wurden im Rahmen einer begleitenden Studie dokumentiert und ausgewertet.

Nr	**Dienstleistungstyp**	**vor 2002**	**2002**	**2003**	**2004**	**2005**	**gesamt**
1	Erfassen, Aufbereiten und Bereitstellen von Information	21	112	43	27	6	209
2	Beratung durchführen	1	4	1	5	0	11
3	Vorbereiten von politischen Entscheidungen bzw. Gesetzesvorhaben	0	1	1	0	0	2
4	Zusammenarbeit mit Behörden	2	6	13	15	1	37
5	Allgemeine Antragsverfahren	2	8	8	17	4	39
6	Förderungen abwickeln	1	1	4	3	0	9
7	Beschaffungsvorhaben durchführen	3	3	9	8	0	23
8	Durchführung von Aufsichtsmaßnahmen	0	3	5	3	1	12
9	Sonstige Dienstleistungen	1	0	4	3	1	9
	Dienstleistungen insgesamt	31	138	88	81	13	351

Tabelle 1.1: Realisierte Dienstleistungen auf Bundesebene

Die Hansestadt Bremen zeichnete sich dabei durch eine sehr erfolgreiche Umsetzung aus. Bremen verfügt heute über ein umfangreiches Portfolio an kommunalen Online-Dienstleistungen. Inspiriert durch solche Erfolge startete die Bundesregierung im Jahr 2000 eine eigene Initiative welche den Namen "BundOnline 2005"trägt. Ziel dieser Initiative ist es alle 451 internetfähigen Dienstleistungen des Bundes bis zum Jahr 2005 online verfügbar zu machen. Der aktuelle Stand ist in der Tabelle auf der vorherigen Seite zu entnehmen.

1.4 eGovernment im Beziehungs-geflecht

Die Beziehungen im eGovernment lassen sich am besten in Form einer Tabelle darstellen.

eGovernment	**Bürger**	**Staat/Verwaltung**	**Wirtschaft**	**NPO/NGO**
Bürger	C2C	C2G	C2B	C2N
Staat/Verwaltung	G2C	G2G	G2B	G2N
Wirtschaft	B2C	B2G	B2B	B2N
NPO/NGO	N2C	N2G	N2B	N2N

Tabelle 1.2: eGovernment in X2Y Beziehungen

Wie in Tabelle 1.2 gut abbilden, deckt das eGovernment sieben der sechzehn möglichen Felder des Beziehungsgeflechtes ab. Dabei werden folgende Beziehungen hervorgehoben:

- Beziehungen innerhalb der öffentlichen Hand (G2G)
- Beziehungen zwischen der Verwaltung und der Bevölkerung (C2G und G2C)
- Beziehungen zwischen der Veraltung und der Wirtschaft (B2G und G2B)
- Beziehungen zwischen der Verwaltung und den Non-Profit bzw. Non-Government Organisationen (N2G und G2N)

1.4.1 Government to Citizens (G2C)

Besonders Öffentlichkeitswirksam sind die Entwicklungen und Erfolge die das eGovernment auf der Ebene zwischen Verwaltung und Bürger erzielt. Hier sind die alltäglichen Belange eines jeden Bürgerns betroffen. eGovernment-Angebote haben hier ihre größte Wirkung im Bezug auf die Öffentlichkeit.
Der Bürger selbst tritt hierbei in zwei unterschiedlichen Rollen gegenüber der Verwaltung auf.

- der Bürger als Entscheidungsakteur
- der Bürger als Entscheidungsempfänger

Fälle, in denen der Bürger die Rolle als Entschei-dungsakteur einnimmt, sind z.B. in die Funktionen als Wähler oder Parlamentarier. Dies betrifft Bereiche des eGovernment welches als eDemocracy und ePolitics bezeichnet werden, aber wir hier nicht weiter betrachtet werden.
Bei den zurzeit laufenden Entwicklungen im eGovernment steht der Bürger in der Rolle des Entscheidungsempfängers im Vordergrund. Hierbei kann er in seiner Beziehung zur Verwaltung die Funktion des Antragsteller, Bescheidempfänger, Informationsnachfrager, Gebührenzahler, Bauherr, Kfz-Halter, Stellenbewerber oder Steuerzahler einnehmen.

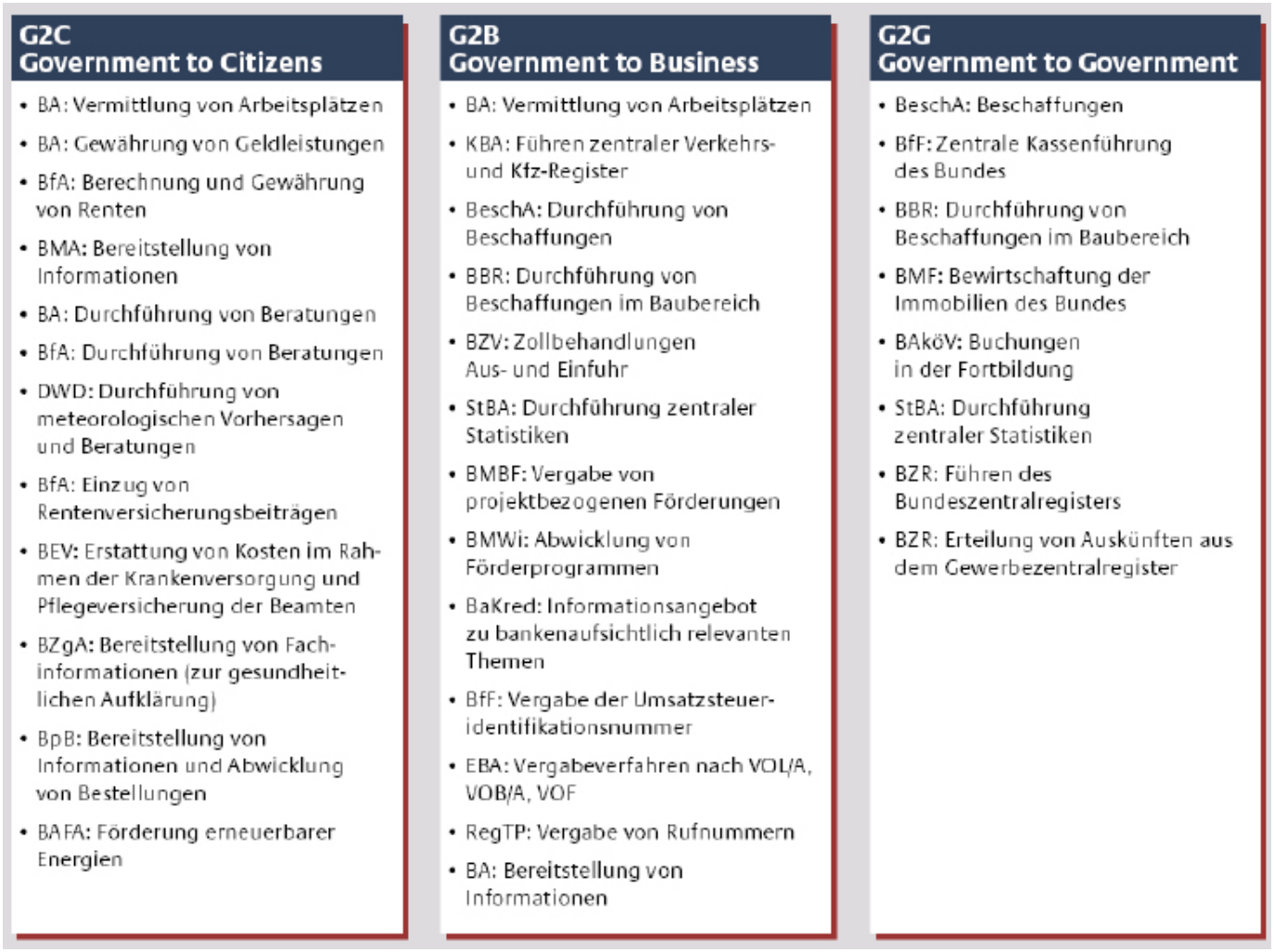


Abbildung 1.1: Attraktive Dienstleistungen von BundOnline 2005 aus Nutzensicht

1.4.2 Government to Business (G2B)

"Government to Businessöder G2B betrachtet die Beziehungen zwischen Verwaltung und Wirtschaft. Zur Wirtschaft zählen oft auch Verbände, Nicht-Regierungsorganisationen und Non-Profit-Organisationen (NPO/NGO) welche im Beziehungsgeflecht eigentlich eine eigene Beziehung darstellen würden aber nicht gesondert betrachtet werden das die Anforderungen der NPOs/NGOs durch die Beziehungen Wirtschaft zur Verwaltung abgedeckt werden.
Die Dienstsleistungen um G2B sind sehr vielfältig, aber sie erreichen nicht den Umfang der Dienstleistungen im G2C. Das größte Interesse auf dem Gebiet des G2B liegt im eProcurement. Das eProcurement stellt die Einkaufs- bzw. Beschaffungsaktivitäten der öffentlichen Verwaltung dar. Ein besonderes Projekt Seitens der öffentlichen Hand wurde vom Beschaffungsamt des Bundesministeriums des Innern realisiert . Dabei liegt das

Hauptinteresse auf den großen Einsparpotentialen die mit dem Einstieg ins eProcurement erwartet werden.

1.4.3 Government to Government (G2G)

Weniger spektakulär als G2C und G2B verliefen bisher die Entwicklungen im G2G, d.h. der verwaltungsinternen Kommunikation auf Basis von eGovernment. Dies liegt hauptsächlich daran, dass das dies als ädministrativer Hintergrundïn der Regel weniger öffentlichkeitswirksam umgesetzt wird. Allerdings treten die laufenden Vorhaben im G2G immer dann in den Fokus der Öffentlichkeit, wenn dafür Gesetzesänderungen notwendig werden. Wie zum Beispiel bei dem "Gesetz zur Förderung des Steuerehrlichkeit"

1.4.4 Erwartungen aus Sicht der Bürger

Durch eine Befragung welche durch die Unternehmensberatung Äccenture ïn Zusammenarbeit mit der Bayerischen Staatskanzlei im Mai und Juni 2002 im Internet durchführte[2] wurde konkretere Aspekte für die Erwartungen aus Bürgersicht geliefern. Zur Zeit der Erhebung empfanden 75 Prozent der befragten Bürger die Öffnungszeiten der Behörden als sehr ungünstig und die Wartezeiten als viel zu lang. Außerdem zählten für mehr aus zwei Drittel der Befragten die schlechte Erreichbarkeit, auch über das Telefon, sowie die überaus undurchsichtigen Abläufe in der Verwaltung zu den größten Schwachstellen. Allerdings schätzen viele Bürger die persönliche Beratung und Hilfe der Verwaltungsmitarbeiter in den Ämtern und wollen auch künftig nicht auf diese traditionellen Möglichkeit verzichten Auf die Frage nach den bevorzugten Wegen für eGovernment-Services bewerteten dies etwa 90 Prozent der Befragten den Zugang per Internet als sehr wichtig oder wichtig. Etwas 50 Prozent der Befragten legte allerdings hohen Wert auf den persönlichen und telefonischen Kontakt mit den Ämtern. Daher zeigt sich das die Einführung des eGovernment keine vollständige Ablösung der bisherigen Möglichkeiten darstellen kann sondern einen Bereicherung und Ergänzung zu diesen. Anhand der Befragung konnte auch festgestellt werden dass die meisten Bürger das Internet hauptsächlich dazu verwenden um Informationen über Öffnungszeiten, Zuständigkeiten und geforderten Unterlagen bei Antragsstellung einzusehen. Allerdings wird nicht nur die Bereitstellung von Informationen sondern auch Transaktionen mit Hilfe des Internets gefordert. So werden das Ausfüllen und Einreichen von Antragen online sowie das die formlose Kommunikation per E-Mail zwischen Bürger und Verwaltungsmitarbeitern gewünscht. Auch das vollständige Antragsverfahren mit Unterschrift in Form der elektronischen Signatur wird gefordert. Besonderes Interesse Seitens des Bürgers liegt dabei in

[2] Anm.: Unter der Internetadresse www.was-will-der-buerger.de beantworteten und bewerteten über 8000Teilnehmer die ca. 60 Fragen und Thesen der ziel-gruppenspezifischen Online-Fragebögen. Es sei jedoc h darauf hingewiesen, dass die erreichte Zielgruppe zwar repräsentativ für Internetnutzer angesehen werden kann, die Interesse an Online-Verwaltungsdienstleistungen haben, allerdings nicht repräsentativ für die deutsche Bevölkerung. Ebenso sind im Vergleich zu anderen Internet-Nutzerstudien Frauen und ältere Menschenun-terrepräsentiert. (Vgl. Accenture (2002a), S. 6-7.) Den-noch sollen die in dieser Bedarfsanalyse abgegebenen Antworten und Bewertungen als allgemeine Richtlinie für die Wünsche und Erwartungen der Bürger gelten.

den Standarddienstleistungen wie An-/ und Ummeldung im Einwohnermeldeamt, Zulassen und Ummelden eines Kfz sowie die Abgabe der Steuererklärung. Bei der Umsetzung dieser Verwaltungsakte als eGovernment-Dienstleistungen versprechen sich die Bürger den größten Nutzen. Aber auch der einfache Ausdruck von Standardformularen und der Informationsbeschaffung wird eine hoher Nutzen beigemessen. Verwaltungsakte die nur sehr selten in Anspruch genommen werden, haben dagegen nur geringen Nutzen für den Bürger.

1.5 Elektronische Signatur

Da viele Kommunen bei der Umsetzung ihrer e-Government-Vorhaben bereits den Stand erreicht habe das ihre Kommunikationsbeziehungen eine hohe Komplexität aufweisen, treten sie hier auf der Stelle. Dies liegt im Besonderen daran das dabei keine rechtsverbindliche Kommunikation zustande kommt. Die Formvorschrift zur eigenhändigen Unterschrift eines Schriftstückes verhinderte die Verbreitung rechtswirksamer elektronischer Online-Erklärungen. Einerseits können Online-Dokumente nicht eigenhändig Unterschrieben werden, andererseits galten sie auch nicht als Urkunden. Außerdem fehlen der Verwaltung, den Bürgern und der Wirtschaft im Normalfall die technischen Voraussetzungen für die elektronische Signatur. Zurzeit sind hauptsächlich Pilotanwendungen mit elektronischer Signatur, wie bei der Bundesversicherungsanstalt für Angestellte (siehe Abbildung 1.2)in der die elektronische Signatur eingesetzt wird.
Auf der rechtlichen Ebene hat Deutschland eine Vorreiterrolle auf dem Gebiet der elektronischen Signatur. Als weltweit erstes Land wurde in Deutschland 1997 ein Gesetz zur elektronischen Signatur geschaffen. Das so genannte Signaturgesetzt (SigG) und die Signaturverordnung (SigV). 2001 kam noch ein Gesetz zur Anpassung der Formvorschrift an den Rechtgeschäftsverkehr hinzu. In diesem Gesetz ist geregelt das eine Unterschrift in Schriftform durch eine qualifizierte elektronische Signatur ersetzt werden kann.Dabei geht es grundsätzlich um die Schaffung der Sicherheit über die Identität des Kunden, Geschäftspartner oder Antragsstellers. Die elektronische Form der Unterschrift benötigt dabei eine qualifizierte oder akkreditierte elektronische Signatur.
Zurzeit werden hauptsächlich drei Arten von digitaler Signatur unterschieden.

- Einfache elektronische Signatur
- Qualifizierte elektronische Signatur
- Akkreditierte elektronische Signatur

Vom Bürger wird bei eGovernment-Diensten eine qualifizierte Signatur erwartet. Während von den Behörden der Orderung nach einer akkreditierten Signatur erwartet wird.

1.5.1 Basis der elektronischen Signatur

Zur Schaffung der elektronischen Signatur werden Verschlüsselungsverfahren eingesetzt. In der Praxis sind bei der Verschlüsselung zwei Verfahren gängig:

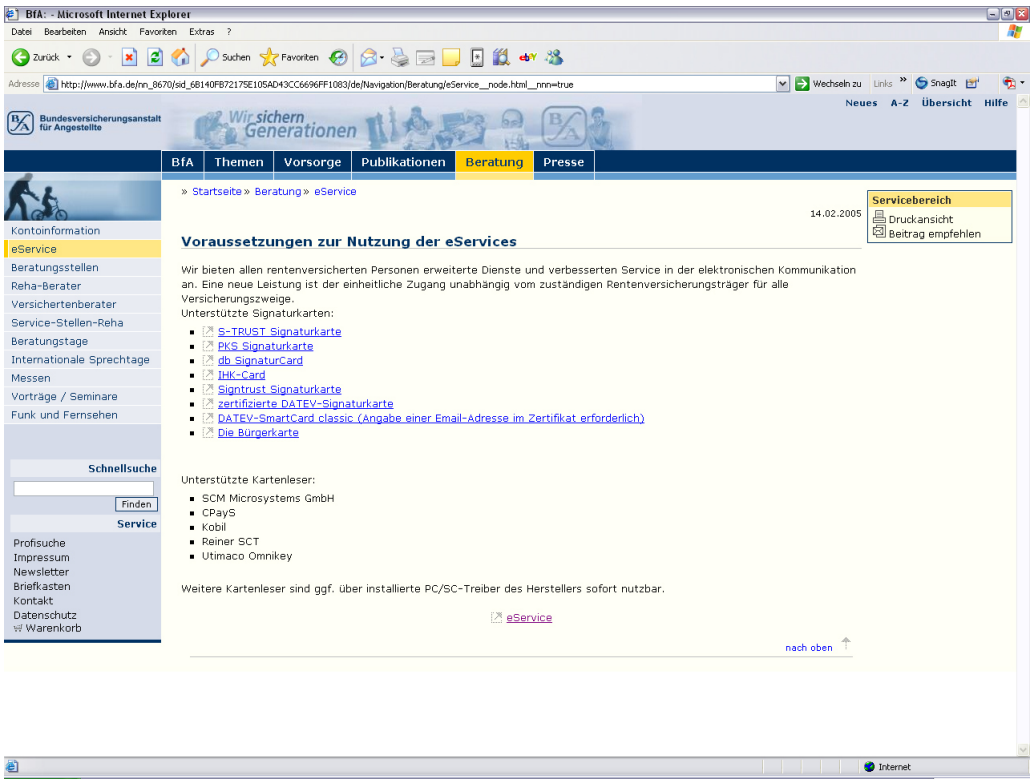


Abbildung 1.2: eService-Angebot der Bundesversicherungsanstalt für Angestellte

- die "Private Key-Verfahren", die auf symmetrischen Verschlüsselung basieren
- und die "Public Key-Verfahren“, welche auf asymmetrischer Verschlüsselung aufbauen.

Bei der elektronischen Signatur werden asymmetrische Verschlüsselungsverfahren eingesetzt, also "Public KeyVerfahren. Hensen (?? Literaturverweis??) beschreibt die digitale Unterschrift vergleichend wie folgt: Ëine digitale Signaturstellt gleichsam ein elektronisches Siegel dar. Es wird mit Hilfe eines Signaturschlüssels, der sich in der Regel zusammen mit einem digitalen Verschlüsselungsprogramm (Signieralgorithmus mit Signierprogramm) auf einer Chipkarte befindet, erzeugt. Die Funktion der Chipkarte (...) kann man dem zufolge mit einem Siegelring vergleichen, der im Siegellack einer Urkunde seinen Abdruck hinterlässt."Nach erfolgter Signatur, meist an einem PC mit Chipkartenlesegerät und Software mit Signaturfunktion, kann aufgrund des Signaturschlüsselzertifikats ßweifelsfrei"festgestellt werden, welche Person signiert hat und ob die übermittelten Daten unverändert geblieben sind. Somit dient die elektronische Signatur vor allem zwei Zwecken: der Integrität und Authentizität des Dokuments sowie dem Nachweis der Urheberschaft - zwei Bedingungen, die für fortschrittliche Verwaltungsanwendungen via Internet grundlegende Voraussetzungen sind.

1.6 Datenschutz und Datensicherheit

Der Datenschutz folgt der technischen Entwicklung, hinkt ihr allerdings auf ihrem Wege stetig hinterher. Insbesondere bei dem zunehmenden Einsatz internetbasierender Software und der damit zunehmenden Datenhaltung. Genau auf solcher internetbasierender Software bauen die eGoverment-Anwendungen auf. Die die Möglichkeit weltweit auf die Daten einer eGoverment-Anwendung Zugriff zu erlangen, insbesondere wenn dies von unbefugten geschieht muss im Datenschutz Rechnung getragen werden. Mit zunehmendem Fortschritt im eGovernment nimmt die Datensicherheit eine besondere Bedeutung an, weil der bisher auf das Amt begrenzte Zugriff der Außenwelt zugänglich gemacht wird. Die sicherheitstechnischen Vorteile der bisher eingesetzten Lösungen verlieren durch den Zugang vom Internet an Bedeutung. Daher hat die Problematik der Datensicherheit in den letzten Jahren einen wichtigen Stellenrang eingenommen. Nur durch einen hohen Stand an Datensicherheit kann ein umfassender Datenschutz realisiert werden. Die Systeme müssen einerseits durch unerlaubte Zugriffe von Außen, z.B. Hackerangriffe, und durch unbefugten Zugriff von Innen z.B. Amtsmissbrauch und Korruption geschützt werden.

1.6.1 Datenschutz

"Dem Datenschutz kommt die Aufgabe zu, die informationelle Selbstbestimmung zu gewährleisten. Dabei müssen vor allem die verfassungsrechtlich unverzichtbaren Prinzipien der Zweckbindung, der Erforderlichkeit, der Datenvermeidung und Datensparsamkeit, der Transparenz sowie die Kontroll- und Korrekturrechte der Betroffenen realisiert werden". Auf Grund der Besonderheiten des deutschen Datenschutzrechtes sind bei der Betrachtung des Datenschutzrechtes drei unterschiedliche Rechts- bzw. Regelungsbereiche für die Kommunikation mit öffentlichen Stellen zu beachten.

Inhaltsebene Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Verwaltungszwecke unterliegt dem Verwaltungsdatenschutzrecht. Das Verwaltungsdatenschutzgesetzt unterscheidet dabei nicht danach, in welcher Form und auf welchem Weg z.B. eine Verwaltungsauskunft erteilt wird. Auch für eGovernment-Anwendungen sind somit alle Anforderungen an die eine reale Auskunft zu beachten. Für die Landes- und Kommunalverwaltung gelten grundsätzlich alle Regelungen der Landesdatenschutzgesetze. Für die Bundesverwaltung gelten dagegen die Regelungen des Bundesdatenschutzgesetzes. Diese sind jedoch gegenüber bereichsspezifischen Datenschutzregelungen nur aushilfsmäßig.

Transportebene Um über das Internet Informationen zu erhalten, muss eine Telekommunikationsverbindung zwi-schen dem Anfragenden und dem Auskunftsserver aufgebaut werden. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für das Herstellen und Aufrechterhalten von Telekommunikationsverbindungen unterliegt dem Telekommunikationsdatenschutzrecht. Von dem inhaltlichen Informations- und

Kommunikationsangebot ist der technische Telekommunikationsvorgang, der das Übermitteln von Signalen ermöglicht, zu unterscheiden. Die Verwendung personenbezogener Daten, die diesem Zweck dient, ist in § 91 ff. Telekommunikationsgesetz (TKG) geregelt. Unter das Telekommunikationsrecht fällt der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern und Tönen mittels Telekommunikationsanlagen. Adressat der Regelungen ist aber nur derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt. Nicht erfasst werden vom TKG inhaltliche Aspekte der Kommunikationsbeziehungen der Nutzer der Telekommunikationstechnik. Zu den Telekommunika-tionsdiensten gehören z.B. der reine E-Mail-Transport und die Internet-Telefonie.

Personenbezogene Daten Bei der Nutzung von eGoverment-Anwendungen handelt es sich in der Kommunikation mit Dritten (außerhalb einer öffentlichen Stelle) rechtlich um die Inanspruchnahme von Telekommunikationsdiensten und Telediensten (z. B. Erteilung einer Eingangsbestätigung durch die Behörde). Dabei fallen neben den vorgangsbezogenen Daten der Bürger weitere personenbezogene Daten an, die bei der Kommunikation mit der Verwaltung und bei der Vorgangsbearbeitung zur Erledigung von Verwaltungsaufgaben entstehen. Diese personenbezogenen Daten sind im Hinblick auf den Schutzbedarf sowohl einzeln als auch im Gesamtkontext der Anwendung zu bewerten. Die Ausges-taltung der Schutzmaßnahmen muss sich daran orientieren, welche Folgen für einen Betroffenen durch die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung entstehen können und welcher potentielle Schaden für den Betreiber eintreten kann. Die Kommunikation mit Bürgern, Firmen und Verwaltungen über eine eGovernment-Anwendung erfordert besondere Vorkehrungen in Bezug auf Datenschutz und Datensicherheit. Dabei sind die folgenden rechtlichen Rahmenbedingungen, wie Zweckbindung, Datensparsamkeit und -vermeidung, Berichtigung, Speicherung, Löschung, Freiwilligkeit, Transparenz, Erforderlichkeit, Verhältnismäßigkeit sowie technisch-organisatorische Sicherungen zu beachten. Die personenbezogenen Daten werden dazu die in folgende Datentypen einteilt:

Bestandsdaten Bestandsdaten sind all die personenbezogenen An-gaben, die einem Betroffenen im Rahmen der Vertragsbeziehungen zu zugeordnet sind. Dazu zählen in erster Line die Daten, die für die Nutzung von angebotenen eGovernment-Anwendungen erforderlich sind z.B. Name, Anschrift, Adresse, Telefon- oder Telefaxnummer, Geburtsdatum, Bank-verbindung, Kreditkartennummer, öffentlicher Schlüssel, statische IP-Adressen und weitere Angaben. Welche Bestandsdaten im Einzelnen erhoben, verarbeitet oder genutzt werden dürfen, ist im Wesentlichen abhängig von der technischen Ausgestaltung der jeweiligen eGovernment-Anwendung.

Nutzungsdaten Nutzungsdaten sind gem. § 6 Abs. 1 TDDSG Da-ten, die erforderlich sind, um die Inanspruchnahme von Telediensten zu ermöglichen und diese abzurechnen. Dabei handelt es sich insbesondere um Daten zur Identifikation des Nutzers wie z.B. Angaben über Beginn und Ende als auch Umfang der einer Nutzung und Angaben über

die von den Nutzer in Anspruch genommenen Dienste.

Verkehrsdaten Bei Angeboten, die sich auf die reine Übermittlung von Daten beschränken (z.B. E-Mails), handelt es sich um Telekommunikationsdienste. Die bei der Erbringung dieser Dienste anfallenden Daten sind Verkehrsdaten im Sinne des Telekommunikationsrechts (§ 3 Nr. 30 und § 96 TKG). Verkehrsdaten bei eGoverment-Anwendungen sind insbesondere EMail-Adressen (die auch Bestandsdaten sein können), Zeitpunkte der Sendung bzw. Zustellung und Routing-Informationen.

Inhaltsdaten Die Beurteilung der Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung von Inhaltsdaten bei Telekommunikations- und Telediensten, also der eigentlichen vorgangsbezogenen personenbezogenen Daten, richtet sich nach den Vorschriften des allgemeinen Datenschutzrechts, soweit nicht spezialgesetzliche Regelungen (z.B. die Erhebung von Sozialdaten nach den Vorschriften des Sozialgesetzbuches, Auskünfte zum Meldewesen nach den Meldegesetzen etc.) einschlägig sind. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen ist zusätzlich zu beachten.

1.7 Standards

Bei der Entwicklung von eGovernment-Lösungen ähneln sich viele Teil-Workflows. So sind z.B. Arbeitsabläufe wie das Abwicklung vom Zahlungsverkehr oder die Abwicklung sicherer, nachvollziehbarer und vertraulicher Kommunikation zwischen Kommunikationspartner (G2G, B2G und G2C) solcher Natur. Deshalb wurden im Zuge des Projektes BUND online 2005, aus Gründen der Kostenersparnis und Einheitlichkeit SStandards und Architekturen für eGovernment-Anwendungen"(SAGA) entwickelt. Dieses Dokument [6??], welches augenblicklich in Version 2.0 vorliegt, dient als Orientierungshilfe für die Entwicklung von eGovernment-Anwendungen, indem es den Einsatz von Basiskomponenten, wie beispielsweise der Basiskomponente ePayment oder der Basiskomponente Datensicherheit - auch als Virtuelle Poststelle (VPS) bezeichnet, beschreibt. Folgende Ziele werden mit dem Einsatz von vorgefertigten Basiskomponenten verfolgt:

- Interoperabilität: eGovernment Anwendungen müssen miteinander kommunizieren und zusammenarbeiten können.
- Wiederverwendbarkeit: eGovernment-Anwendungen sollen vorgefertigte Komponenten und Strukturen nutzen, um eine redundante Entwicklung zu verhindern.
- Offenheit der Spezifikation: Offene Spezifikationen ermöglichen die problemlose Erstellung und Integration von eGovernment Anwendungen.
- Reduktion von Kosten und Risiken: Die Wiederverwendung bereits etablierter Standards und Systeme reduziert Kosten und Risiken.

- Skalierbarkeit: Bei der Entwicklung der Basiskomponenten wurde eine zukünftige hohe Nutzerzahl berücksichtigt.

Das Dokument wird durch Architekturmodelle, Kategorisierungen von Standards und Beispielimplementierungen vervollständigt. Für alle Prozesse und Systeme, die eGovernment-Leistungen des Bundes anbieten, ist die Konformität mit SAGA dabei verpflichtend. Somit stellt SAGA einen Standard dar, der eine redundanzfreie bundinterne Kommunikation und einen ebensolchen Datenaustausch, sowie eine teilweise einheitliche Funktionalität nach innen und außen ermöglicht. In SAGA werden zu diesem Zweck die vorgestellten Standards in drei Klassen unterteilt, welche Empfehlungen zum Einsatz der Standards darstellen:

- Obligatorisch: Der Einsatz obligatorischer Standards sind verpflichtender Natur, d.h. sie sollen eingesetzt werden sofern entsprechende Technologien eingesetzt werden sollen. Dabei sind sie gegenüber den Standards aus den anderen Kategorien vorzuziehen.

- Empfohlen: Empfohlene Standards sind zwar schon Praxis erprobt, allerdings wurden sie noch nicht ausreichend für eine Einstufung als obligatorisch beobachtet und getestet.

- Unter Beobachtung: Standards, die sich noch nicht eingesetzt wurden, aber viel versprechend sind, haben den Status unter Beobachtung. Ihr Einsatz soll nur dann erfolgen, wenn in dem jeweiligen Bereich noch keine als empfohlenen oder obligatorischen eingestuften Standards vorhanden sind.

- Black List: Eine Black List listet Technologien auf, die nicht eingesetzt werden sollen. Standardisierung der Verwaltungsprozesse.

Um eine hohe Effizienz und Kostenersparnis beim eGovernment zu erreichen müssen nicht nur die technischen Faktoren vereinheitlicht werden. Darüber hinaus ist auch eine Vereinheitlichung der Arbeitsabläufe und Formulare der einzelnen Behörden notwendig, mittels derer erst die vollen Reichweite der Vorteile von eGovernment zum Tragen kommt. Somit bietet die Entwicklung von technischen Standardlösungen eine gute Grundlage für die Überarbeitung und Vereinheitlichung der Abläufe innerhalb der Behörden.

1.8 Anforderungen an eGovernment

In diesem Kapitel sollen verschiedene Anforderungen beschrieben werden, die an eGovernment Anwendungen gestellt werden sollten und bei deren Realisierung beachtet werden sollten, um die Akzeptanz durch den Bürger zu erhöhen.

1.8.1 Authentifizierung

Die Authentifikation bezeichnet den Vorgang bei dem die Identität eines Nutzers ermittelt wird. Bei der Authentifikation muss sichergestellt werden, dass nur die entsprechende Person in der Lage ist sich mittels einer qualifizierten Signatur zu authentifizieren (vgl. Abbildung 1.3). Dies könnte durch mehrere Verfahren erreicht werden, auf die im Folgenden kurz eingegangen werden soll. Eine Authentifizierung durch eine Signaturkarte, die mittels eines integrierten Fingerabdruckscanners, erst nach Sicherstellung der korrekten Person als Nutzer die Signatur entschlüsselt und somit freigibt, währe die sicherste Lösung. Hierbei könnte die Signatur noch mit einem verschlüsselten Zeitstempel versehen werden, was die wiederholte Nutzung durch unautorisierte verhindert. Durch die eingesetzte Technik wird diese vermutlich in der Anschaffung sehr kostspielig sein, könnte aber, wegen der hohen Sicherheit, länger Gültigkeit behalten. Eine einfachere Authentifizierung eines eGovernment-Nutzers mittels einer Signatur, wäre nach Sicht des Autors die Kombination einer Signatur und eines Passworts oder einer TAN-Nummer. Mit dieser Methode könnte man bei einem geringeren Anschaffungspreis trotzdem eine relativ hohe Sicherheit garantieren.

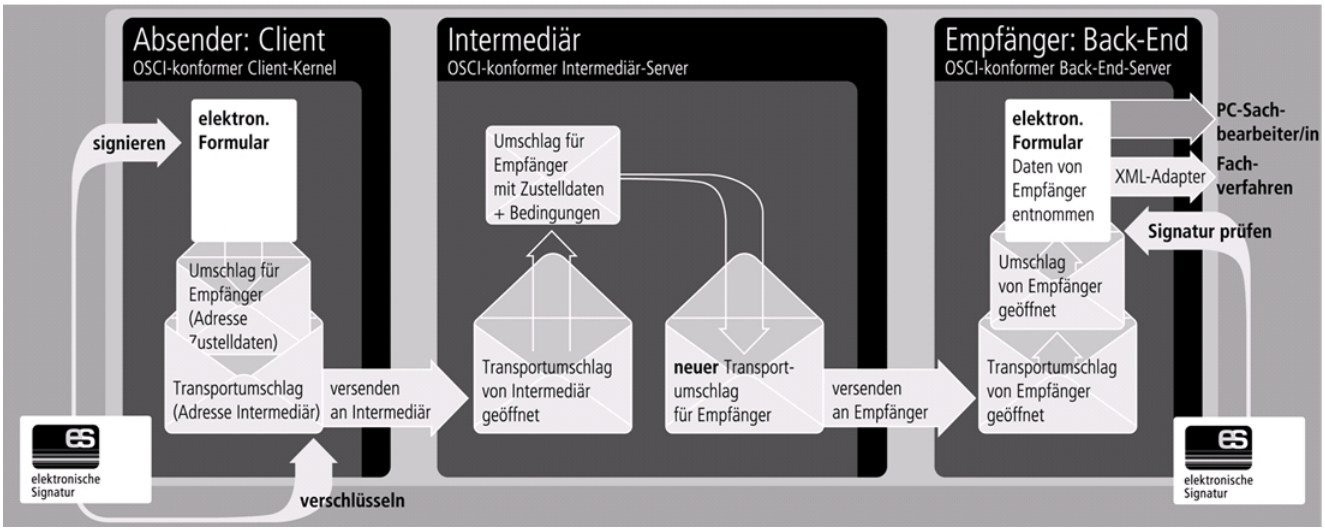


Abbildung 1.3: Signaturvorgang bei Kommunikation nach SAGA

Bisher hat es der BUND nicht geschafft eine einheitliche Signaturen Anforderung durchzusetzen. Zurzeit existieren so verschiedenste Lösungen, bei denen sich die geforderten Sicherheitslevels stark voneinander unterscheiden. Nach Ansicht des Autors wäre es zweckmäßig folgende Fortschritte zu erzielen:

- Eine zentrale bundeseigene Zertifizierungstelle sollte an jeden Bürger Zertifikate ausgeben. Hier könnte eine direkte Koppelung an das Einwohnermelderegister einen Datenabgleich und somit eine Verifikation der Bürger erleichtern, was zu einer preiswerteren Erstellung von Zertifikaten führen kann. Zurzeit sind solche Aktionen von Rentenkassen geplant.

- Eine Standardisierung der Sicherheitsniveauanforderungen für den Einsatz von Signaturen beim eGovernment könnte dazu führen, dass ein Bürger mit einer Karte alle angebotenen Dienste ausführen bzw. nutzen kann. Ein Zustand der erstrebenswert ist.

1.8.2 Verifikation des Clients

Eine weitere Gefahrenstelle könnten Sicherheitslücken in der Anwendungsoberfläche darstellen. So könnte es passieren, dass man ohne Authentisierungsprüfung Zugriff auf personenbezogene Daten anderer Nutzer erhält. Um diese Gefahren größtmöglich auszuschließen, verlangt die Bayrische Landesregierung, dass die Implementierung ihrer eGovernment Anwendungen bestimmten Sicherheitsspezifikationen entsprechend durchgeführt wird. Deshalb müssen die in Bayern eingesetzten Applets nach bestimmten Standards verifiziert werden. Dieses Verfahren bewirkt zwar Zu-satzkosten für die Behörden, jedoch wir damit eine minimale Grundsicherheit sichergestellt. Somit ist hier das Vorgehen des Bundeslandes Bayern mustergültig und sollte auch von allen anderen Anbietern von eGovernment Anwen-dungen durchgeführt werden. Allerdings ist dieses Vorgehen beim Bund nicht verpflichtend und stellt somit ein nichtverständliches Sicherheitsloch dar.

1.8.3 Nutzerzentriertes Design

Eine wesentliche Anforderung, die an eGovernment Anwendungen zu stellen ist, sind Nutzer zentrierte Designs, der Nutzeroberflächen. Denn erst wenn die Anwendungen übersichtlich und klar strukturiert sind, stellen sie für den Nutzer eine Erleichterung dar und können ihm somit eine wirkliche Alternative zum Gang zum Amt bieten. Die daraus resultierende intuitive Bedienung wird außerdem durch eine standardisierte Oberflächenstruktur verstärkt. So wird die Akzeptanz von eGovernment Lösungen nicht nur von der eingesetzten Technik abhängen, sondern auch von einer interregionalen einheitliche Strukturierung der Oberflächen. Schließlich sind die wenigsten Nutzer bereit, sich in verschiedene eGovernment Anwendungen verschiedener Städte oder Länder immer wieder neu einzuarbeiten.

1.8.4 Datenschutz

Durch die existierenden eGovernment-Lösungen werden nicht nur einfachere Nutzung von Verwaltungsaktionen für den Nutzer ermöglicht. Aus der neuen Verknüpfung von Ämtern mittels G2G-Anwendungen wird auch eine Verknüpfung von Daten möglich, die Ge-fahren für die Sicherstellung der rechtlich fixierten Informativen Selbstbestimmung des Bürgers, also dem Recht des Bürgers, über die Verbreitung der ihn beschreibende Informationen selbst zu entscheiden, darstellen kann. Längst sind Beispiele bekannt, wo dieses Recht ohne die gesetzlich geforderte Notwendigkeit übergangen wurde, so zum Beispiel. die Übertragung aller Studentendaten an das BKA zum Einsatz bei der Rasterfahndung zur Terroristenverfolgung. Kann die rechtliche Stellung des Bürgers beim Einsatz von eGovernment nicht mehr sichergestellt werden, birgt dies, nach Ansicht des

Autors, die Gefahr, dass trotz einer sonst guten Realisierung, diese Neuerung in der Bevölkerung nicht akzeptiert wird. Deshalb sollten zum einen neue Konzepte vor der Einführung öffentlich diskutiert werden und nicht, wie die biometrischen Pässe von öben herabëingeführt werden. Zum anderen müssen die Verknüpfung von Daten und der Zugriff durch Behörden für den betroffenen Bürger offen gelegt und damit nachvollziehbar werden.

Neben der direkten Verknüpfung von Daten existieren weitere Gefahren für den Datenschutz. So muss durch geeignete Verschlüsselungsmechanismen und Sicherungen garantiert sein, dass ein Zugriff auf Bürgerdaten nur durch autorisiertes Personal möglich ist. Fälle wie in Amerika wo sich Diebe Millionen Datensätze von Kreditkartendaten angeeignet haben [siehe **??**] müssen auch im eGovernment Bereich ausgeschlossen werden können. Dabei spielt auch die kontrollierte Vernichtung von alten Datenträgern eine Rolle. Diese Beispiele zeigen, das Datenschutz, ein umfangreiches Problem ist, was weder vernachlässigt, noch unterschätzt werden darf. Es lässt sich folglich zusammenfassend feststellen, dass es ,trotz enormer Entwicklungen im Bereich eGovernment und signifikanter Fortschritte bezüglich des Einsatzes von Standarddatenmodellen und Standardkomponenten, noch einige Bereiche verbessert werden müssen. Zu diesen zählen speziell die Bereiche Datenschutz, Standardisierung von Signaturen und Nutzerzentriertes Design. Man wird sehen in wie weit diese Herausforderungen in der Zukunft bewältigt werden und eine vermehrte Akzeptanz von eGovernment durch die Bürger erreicht werden kann.

1.9 Fazit

Auf kommunaler Ebene sind bereits erhebliche Erfolge zu verzeichnen. Insbesondere in den Bundesländern Bremen und Hamburg. Auch auf Bundesebene hat man es geschafft bereits einen Großteil der möglichen Dienstleistungen umzusetzen. Dafür würden sowohl die gesetzlichen als auch die technischen Vorraussetzungen geschaffen. Mit dem Projekt "BundOnline2005"versucht man bereits die Projekte von Bund, Ländern und Kommunen zu bündeln. Hierfür wurden auch umfangreiche Standards und Richtlinien geschaffen. Allerdings stehen einer übergreifenden Umsetzung von eGovernment in Deutschland sowohl der Datenschutz als auch die föderale Struktur Deutschlands im Wege.

1.10 Ausblick

Eines der größten zurzeit bestehenden Hindernisse in der Akzeptanz von eGovernment-Angeboten liegt in der Verbreitung der elektronischen Signatur. Nur eine Minderheit, besitzt heute eine elektronische Signatur, was einfach auf die damit verbundenen Kosten zurückzuführen ist. So wird es für die Zukunft eine der größten Herausforderungen sein jedem Bürger den Zugang zur elektronischen Signatur zu erschwinglichen Kosten zu ermöglichen.

Literaturverzeichnis

[1] *Datenschutzgerechtes eGovernment, Kapitel 3 ff.* http://www.lfd.niedersachsen.de.

[2] *eGovernment aus Bürgersicht.* http://www.was-will-der-buerger.de.

[3] *eGovernment-Handbuch.*

[4] *Fünf Millionen US-Kreditkartennummern geklaut*, 2000-02-18. http://www.heise.de.

[5] A. Altingdag. *Chancen und Entwicklungen im Public Procurement.* 2000.

[6] Hensen. *Digitale Signaturen: Revolutionierung des Verwaltungshandelns und Einebnung der Aktenberge?* 2000.

[7] Stern. *Der Dieb war ein Polizist.*

2 Digitale Karten

Bettina Buchholz, Michael Werlitz

2.1 Abstract

Im Rahmen des Seminars *Trust Management und Security Policy Enforcement* wurden von Bettina Buchholz und Michael Werlitz das Thema *Digitale Karten* gewählt.
Nach einer kurzen Klärung was sich hinter dem Begriff der digitalen Karten im Sinne dieser Ausarbeitung verbirgt, wird kurz auf deren historische Entwicklung eingegangen. Danach kommt es zu einer Betrachtung der Aufgaben digitaler Karten und welche Rolle die *Informationssicherheit* und die Identität zwischen Nutzer und Karteninhaber dazu einnehmen. Darüber hinaus werden die am meisten verbreiteten Kartentechnologien betrachtet und der Versuch unternommen eine eigene Kategorisierung digitaler Karten vorzunehmen.
In der abschließenden Zusammenfassung werden die Kernaussagen der Ausarbeitung noch einmal in komprimierter Form dargestellt.
Der Anhang der Ausarbeitung enthält ein Glossar, das einige Begriffe und Abkürzungen kurz erklärend darstellt.

2.2 Einleitung

Digitale Karten sind ein Bestandteil unseres alltäglichen Lebens geworden. Niemand, der sich nicht vollständig unserer westlichen Gesellschaft entzogen hat, kommt heutzutage noch ohne digitale Karten aus. Sei es beim bargeldlosen Einkauf, wenn man zum Arzt geht, beim Telefonieren mit dem Handy, oder dem Öffnen einer elektronisch gesicherten Tür. Überall existieren Anwendungsmöglichkeiten digitaler Karten.
Sie helfen uns dabei „langwierigere“ Prozesse zu vermeiden, wie zum Beispiel das Abheben von Bargeld, und Objekte zu ersetzen, zum Beispiel einen Schlüssel oder das lästige Kleingeld.
Der Begriff der *digitalen Karte* ist sehr vieldeutig. Im Rahmen dieser Ausarbeitung werden darunter Karten verstanden, die als maschinenlesbare Repräsentation personenabhängiger (EC-Karte, Kundenkarten) oder aber personenunabhängiger Daten (Telefonkarte, Kopierkarte) dienen. In der Literatur werden diese Karten oft auch als *Identifikationskarten* bezeichnet.

Da dieses Thema einen sehr weiten Bereich umfasst, haben wir uns zuerst an den Technologien orientiert, die innerhalb der letzten 60 Jahre entwickelt wurden und die auch heute noch verbreitet sind. Darüber hinaus betrachten wir die Aufgaben der digitalen Karten und gehen kritisch auf die Gewährleistung der *Informationssicherheit* und der Identität zwischen Nutzer und Karteninhaber ein. Abschließend haben wir eine Kategorisierung vorgenommen, die sich dem rein technischen Blickwinkel entzieht und den Fokus mehr auf die Anwendungen und die Kartenbetreiber richtet.

2.3 Historische Entwicklung digitaler Karten

Möchte man eine exakte zeitliche Entwicklung der digitalen Karten darstellen, so muss man leider feststellen, dass dies nicht ohne weiteres möglich ist. Innerhalb der letzten Jahrzehnte sind so viele verschiedene Karten und Kartensysteme entwickelt worden, dass an dieser Stelle eine genaue Ausführung den Rahmen der Ausarbeitung sprengen würde. Deshalb wird die Historie im Folgenden anhand verschiedener Kartentechnologien umrissen.
Eigentlich könnte man sagen, dass die Entwicklung der digitalen Karten mit den Lochkarten begann, obwohl diese nicht als digitale Karten (im Sinne der Identifikationskarten) zu bewerten sind. Lochkarten wurden noch vor den 50er Jahren dazu verwendet um z.B. innerbetriebliche Vorgänge, wie Zeiten- oder Zugangskontrolle, zu regulieren.
In den 50er Jahren entstanden dann die ersten Hochgeprägten Karten in den USA (Beginn des Diners Club). Diese wiesen höhergestellte Zeichen auf, die mittels einer Schicht Kohlepapier erfasst und später digital verarbeitet werden konnten. Eine einfache jedoch auf keinen Fall fälschungssichere Möglichkeit der Datenerfassung war gegeben. Es gab jedoch noch einen weiteren Nachteil. Die Daten auf den Karten waren im Nachhinein nicht mehr veränderbar.
Aus der Notwendigkeit heraus, kleine Datenmengen in einer kompakten Form auf einem wieder verwendbaren Datenträger abzuspeichern, wurde in den 70er Jahren das Magnetband auch für den Computer massentauglich. In diesen Jahren kamen unter anderem Taschenrechner mit Magnetstreifen, als Speicher für Programme, auf den Markt. Die ersten ebenfalls mit Magnetsstreifen ausgestatteten digitalen Karten ließen dann als Mitarbeiterausweise in Firmen nicht lange auf sich warten.
Durch die Magnetstreifentechnologie war es nun unter anderem auch möglich Guthaben auf einer Bankkarte abzuspeichern. Da die ursprüngliche Bankkarte nun jedoch zum multifunktionalen Ausweis mutierte, wurden mit der *ISO*-Codierung neue Maßstäbe gesetzt. Der Magnetstreifen bekam nun insgesamt drei Magnetspuren, die für verschiedene und voneinander unabhängige Anwendungen genutzt werden konnten. Anfangs gab es den so genannten LoCo-Magnetstreifen (Low Coercivity), der jedoch bereits in den 80er Jahren durch den HiCo (High Coercivity) ersetzt wurde, da dieser nicht mehr durch Magnete einfach gelöscht werden konnte.
In den 80er Jahren (erste Patente lagen bereits 1968 vor) wurde dann die kontaktbehaftete Chipkarte entwickelt. Auf diesem Chip sollten Daten dauerhaft gespeichert werden ohne dabei von Stromquellen abhängig zu sein. Zunächst wurde diese Technologie bei

Telefonkarten, zuerst bei den Franzosen, eingesetzt und später dann auch bei den Krankenversicherungskarten.
In den 90er Jahren wurde dann schließlich die kontaktlose Chipkarte entwickelt. Auch diese Karten besitzen einen Chip, der jedoch im Gegensatz zur bereits erwähnten Chipkarte, im Inneren der Karte sitzt und von außen nicht sichtbar ist. Die Kommunikation mit dieser Karte wird mittels einer in der Karte sitzenden Antenne möglich. Wird diese Karte nun in den Bereich eines Kartenlesers bewegt, empfängt der Chip ein starkes Signal, das wiederum gleichzeitig den Chip mit Strom versorgt (*RFID*).
Neben ständigen Weiterentwicklungen im Bereich der Chipkarten, gab es am Ende des 20. Jahrhunderts auch noch die Entwicklung und Standardisierung der Optischen Speicherkarte. Diese hatte gegenüber allen anderen digitalen Karten den Vorteil auch große Speichermengen aufbewahren zu können. Um die optische Speicherkarte gibt es bis heute eine große Kontroverse in Fachkreisen, da zwar ihre Datenkapazität gelobt wird, die Möglichkeit die Sicherheit der Daten auch wirklich zu gewährleisten jedoch umstritten ist.

2.4 Aufgaben digitaler Karten

Eine mögliche Erklärung für die sehr erfolgreiche Verbreitung der digitalen Karten ist, dass mit ihnen in den meisten Fällen nur eine Transformation bereits funktionierender Prozesse stattgefunden hat.
Telefon-, Geld- und Kopierkarten ersetzen zum Beispiel das Horten und Einwerfen von Münzen. Karten zum Türöffnen ersetzen den Schlüssel oder eventuell die persönliche Kontrolle durch Pförtner oder Sicherheitspersonal. EC-Karten ermöglichen den direkten Zugriff auf das Girokonto, wo man vorher noch das Geld extra abheben musste und Kreditkarten erleichtern das Ausgeben von Geld, das man im Moment selbst nicht hat (man nimmt die Beantragung eines Kredits vorweg).
Eine der wenigen neuen Anwendungsformen ist, in unseren Augen, der Gebrauch der *SIM*-Karte (Subscriber Identification Module). Diese Chipkarte ist für jedes handelsübliche Handy notwendig, um die Dienste des Endgeräts, mit Ausnahme des Notrufs, nutzen zu können. Eventuell entsteht dieser Eindruck des „Neuen“ aber auch nur, da sie sehr viele Funktionen in sich vereint (Identifizierung der Rufnummer; enthält das Sicherheitsmerkmal (*PIN*) zur Identifizierung des Nutzers der Rufnummer; ggf. enthält sie eine Telefonliste; ggf. bewahrt sie Kurznachrichten auf;...).

2.4.1 Identifikation und Informationssicherheit

Wenn man sich nun die grundlegenden Vorgänge hinter all den konkreten Aufgaben digitaler Karten betrachtet, so wird man feststellen, dass man diese auf wenige gemeinsame Aspekte reduzieren kann.
Nimmt man es ganz genau, dann werden durch digitale Karten, ganz unabhängig von der verwendeten Technologie, lediglich personenbezogene oder aber personenunabhängige Informationen repräsentiert. Personenbezogene Informationen sind dabei zum Beispiel

der Name, die Anschrift aber auch die gespeicherten Telefonnummern auf der *SIM*-Karte eines Handys. Personenunabhängige Informationen sind zum Beispiel der gespeicherte Geldwert auf einer Telefon- oder Kopierkarte.
Für die Verwendung der personenabhängigen Informationen ist die Übereinstimmung (die Identität) der Person, welche durch die Karte repräsentiert wird, und der natürlichen Person, welche die Karte in der Hand hält, ein elementares Kriterium.
Darüber hinaus ist es wichtig, dass die *Informationssicherheit* der Informationen auf der Karte gewährleistet wird. Die *Informationssicherheit* beschreibt nichts anderes, als die Bewahrung der *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*, der auf der Karte vorhandenen Informationen.
Das bedeutet auf die Informationen der Karte dürfen lediglich autorisierte Personen oder Prozesse zugreifen (*Vertraulichkeit*). Die Informationen müssen fehler- und verlustfrei behandelt werden (*Integrität*) und der Zugriff muss dem autorisierten Nutzer im Rahmen seiner Optionen im vollen Umfang gewährleistet werden können (*Verfügbarkeit*).
Für digitale Karten mit personenunabhängigen Daten entfällt die Notwendigkeit der Feststellung der Identität eines Nutzers. Hier wird einfach vorausgesetzt, dass der Nutzer automatisch der berechtigte Inhaber der Karte (die autorisierte Person) ist. Die *Informationssicherheit* der auf der Karte abgelegten Informationen muss natürlich dennoch gewahrt bleiben.

2.4.2 Anforderungen und Realität

Nun stellt sich die Frage, ob die digitalen Karten, mit ihren technologischen Merkmalen den Anforderungen der sicheren Informationsrepräsentation (Wahrung der Identität bei personenbezogenen Daten; generell Wahrung der *Informationssicherheit*) gerecht werden.
Wie später auch vereinzelt bei der Vorstellung der Technologien der digitalen Karten festzustellen sein wird ist dem bei einer kritischen Betrachtung leider nicht so.

Allein das Problem der Wahrung der Identität kann nur durch zusätzliche Sicherheitsmerkmale gewährleistet werden. Die digitale Karte kann das auf keinen Fall selbst leisten. So sind zur Identifizierung im einfachsten Fall eine Unterschrift oder die Vorlage eines zusätzlichen Personennachweises (in der Regel der Personalausweis) oder aber die Eingabe einer *PIN* notwendig.
Besonders die Verwendung der *PIN* (personal identification number) kann man in diesem Zusammenhang kritisieren, da eine normalerweise vierstellige Nummer sicher nicht geeignet erscheint eine Person zweifelsfrei zu identifizieren. Zudem darf angezweifelt werden wie sicher eine vierstellige Zeichenfolge sein kann, die in der Regel keine regelmäßigen Änderungen zulässt und nur Ziffern enthält. Der Vorteil der *PIN* ist jedoch, dass sie von den Kunden als Sicherheitsmerkmal angenommen wurde.
In Zukunft sollen als Instrument der Identifizierung weitere persönliche Merkmale verwendet werden, die eine größere Aussicht auf Fälschungssicherheit bieten (auch gegenüber einer Unterschrift). Zu nennen sind dabei zum Beispiel Daumen- oder Fingerab-

druck, Retinascan oder Stimmerkennung. Ob es zu einem Einsatz kommt, hängt natürlich davon ab, wie sich die jeweilige Technologie auch im Zusammenspiel mit den digitalen Karten und den Anwendungen durchsetzen kann.

Bei der Wahrung der *Informationssicherheit*, so wie sie oben bereits definiert wurde, hängt vieles von den verwendeten Technologien auf der digitalen Karte sowie weiteren Sicherheitsmerkmalen ab.
Digitale Karten, die zum Beispiel lediglich auf der Basis hochgeprägter Zeichen arbeiten würden, könnten das Kriterium der *Informationssicherheit* nicht erfüllen. Hochgeprägte Zeichen sind im Klartext lesbar und könnten schon deshalb einfach notiert und selbst geprägt werden. Unautorisierte Personen hätten somit Zugriff. Dieses Problem ist natürlich seit Jahrzehnten bekannt und deshalb reicht das Merkmal der hochgeprägten Zeichen alleine nicht aus um eine Transaktion durchzuführen.
Die Weiterentwicklung der Technologien rund um die digitalen Karten kann unter anderem auch als eine ständige Verbesserung der Gewährleistung der *Informationssicherheit* betrachtet werden.
War auch bei den Magnetstreifenkarten eine direkte Manipulation (einfach zu realisierender Lesbarkeit, Wiederbeschreibbarkeit, und Störanfälligkeit) möglich, so wurde mit Hilfe der Mikroprozessorkarten diese Möglichkeit erheblich eingeschränkt. Ob die Frage der *Informationssicherheit* durch die kontaktlose Datenübertragung wieder verschärft wird bleibt abzuwarten. Dem unberechtigten Auslesen der übertragenden Daten stehen immer die Verschlüsselung der Daten, deren generelle Verwendbarkeit, sowie andere Sicherungsmethoden gegenüber.

2.5 Technologien digitaler Karten

Eines der wichtigsten Merkmale digitaler Karten ist ihre technische Ausstattung. Viele Publikationen nehmen daher eine Unterscheidung digitaler Karten lediglich anhand der verwendeten Technologien vor.
Wir selbst haben dazu eine differente Meinung (siehe Kategorisierung digitaler Karten 2.7), gehen in diesem Abschnitt aber natürlich dennoch auf die etablierten Technologien ein.

2.5.1 Hochgeprägte Karten

Hochgeprägte Karten enthalten eine Reihe von Zeichen, die sich von der Oberfläche einer Karte abheben (Abbildung 2.2) und sich daher sehr einfach auf Papier übertragen lassen.
Sie stellen eine simple Möglichkeit dar in sehr kurzer Zeit, die Daten einer Karte, insofern diese als hochgeprägte Zeichen vorliegen, zu erfassen und zur späteren Verarbeitung in Papierform aufzubewahren. Es werden also keine besonderen Vorraussetzungen an die Verwendung dieser Art von Karten gestellt. Die Hochprägung eignet sich daher besonders

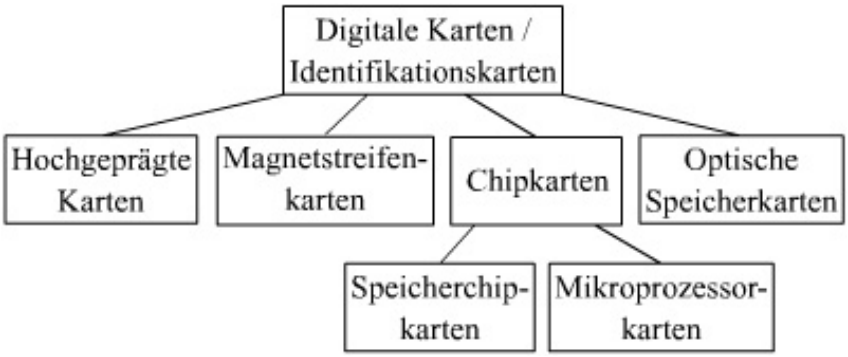


Abbildung 2.1: Technologien im Überblick

Abbildung 2.2: Hochgeprägte Karte, Pro Card Systems GmbH

gut für Gelegenheiten oder Orte, wo ein Zugriff auf technische Hilfsmittel (Datenverbindung, oder gar Strom) eingeschränkt oder generell nicht möglich ist.
Eine Spezifikation, die sich mit diesem Merkmal beschäftigt, ist *ISO/IEC* 7811-1:2002 der International Organization for Standardization (*ISO*) und International Engineering Consortium (*IEC*). In dem Standard werden verschiedene Anforderungen an das Prägen von Karten behandelt, unter anderem Form, Größe und Lage der Prägung, sowie welche Daten geprägt werden sollten.
Die Prägungen findet man in der Regel auf allen Kreditkarten und zahlreichen Kundenkarten wieder.
Man kann annehmen, dass die Hochprägung der kleinste gemeinsame Nenner ist um eine einfache oder besser gesagt technisch anspruchslose Verarbeitung der Benutzerdaten für eine Transaktion zu gewährleisten. Man muss jedoch hinzufügen, dass der Abdruck einer Prägung nie alleine gültig ist um den Verursacher einer Transaktion als den Inhaber der Karte zu identifizieren. In der Regel sind in diesem Zusammenhang eine Unterschrift (die meist mit einer Unterschrift auf der Karte verglichen werden kann), sowie ein weiterer Personennachweis (zum Beispiel der Personalausweis) notwendig.

2.5.2 Magnetstreifenkarten

Wie der Name schon verrät, befindet sich als technisches Merkmal ein Magnetstreifen (Abbildung 2.3) auf der Karte.

Der Magnetstreifen, mit seinen drei Magnetspuren ist der Träger codierter Informationen. Insgesamt können 125 Byte an Daten aufgenommen werden.
Eine ganze Reihe von Vorgaben beschreibt die *ISO* in den Dokumenten der Reihe *ISO/IEC* 7811. Dort werden unter anderem die Eigenschaften des Magnetstreifens, die Codiertechnik, und die Lage der einzelnen Magnetspuren festgelegt.

Abbildung 2.3: Magnetstreifenkarte, Flexocard Kartensysteme GmbH

Auf den ersten beiden Magnetspuren sind, nach *ISO/IEC* 7811, die Daten des Karteninhabers, sowie die Kartennummer codiert (sie entsprechen den Daten der Hochprägung). Auf der dritten Magnetspur wird normalerweise die zuletzt ausgeführte Transaktion verzeichnet.
Für das Auslesen des Magnetstreifens werden entsprechende Lesegeräte benötigt.
Magnetstreifenkarten werden erhebliche Nachteile nachgesagt: Die Daten auf den Magnetspuren sind für den eigentlichen Karteninhaber nicht transparent. Außerdem sind die Daten sind relativ leicht zu kopieren, bzw. zu manipulieren.
Nichtsdestotrotz setzt man Magnetstreifenkarten zum Auslesen der Karteninhaberdaten weiterhin ein (Bankarten, Kreditkarten, Kundenkarten). Zur Absicherung werden in der Regel zusätzliche Sicherheitsmerkmale eingesetzt, zum Beispiel eine Codierung im Kartenkörper, die im Terminal zusätzlich ausgelesen wird (z.B. bei EC-Karten). Auch wird bei persönlichen Transaktionen mit einer Magnetstreifenkarte oftmals ein zusätzlicher Nachweis der Identität des Nutzers verlangt (Unterschrift, Personennachweis).

2.5.3 Chipkarten

Unter dem Begriff der Chipkarten (manchmal auch als Smart Cards bezeichnet, selbst wenn der Begriff „smart“ nicht wirklich auf alle Chipkarten zutrifft) werden viele technologische Ansätze zusammengefasst. Allgemein enthalten solche Karten einen integrierten Chipsatz, welcher das Speichern und Verarbeiten von Daten ermöglicht.
Eine Vielzahl der Chipkarten-Technologien wurde von *ISO* und *IEC* unter der Nummer *ISO/IEC* 7816 spezifiziert.
Im Folgenden nehmen wir eine Unterteilung der Chipkarten-TEchnologie in Speicherchip- und Mikroprozessorkarten, sowie kontaktbehafteten und kontaktlosen Chipkarten vor.

Abbildung 2.4: Chipkarten, Deutsches Ärzteblatt

Im Abschnitt „Angriffe auf Chipkarten“ 2.6) gehen wir separat auf Möglichkeiten ein, wie die auf Chipkarten gelagerten Informationen eventuell ausgelesen werden können, bzw. wie man sich Zugang zu den Chipsätzen verschafft.

Speicherchipkarten I

Diese Karten beschränken sich auf Speicherchips (*ROM* oder *EPROM*, *EEPROM*). Sie können Sicherheitsansprüchen nicht wirklich gerecht werden, da der Speicher einfach auszulesen ist. Natürlich ist es möglich die Daten auf dem Chip verschlüsselt abzulegen, aber ein Zugriff ist dennoch möglich und damit die *Informationssicherheit* bei Weitem nicht mehr gewährleistet.
Der Vorteil der Speicherchipkarten liegt in der billigen, massentauglichen Produktion und das sie mehr Daten halten können (maximal 32 Kilobyte) als der reguläre Magnetstreifen.

Speicherchipkarten II - mit fest verdrahteter Logik

Der Vorteil der Speicherchipkarten mit fest verdrahteter Logik gegenüber den „normalen“ Speicherchipkarten besteht in der Einführung verschiedener Schutzniveaus. So können Lese- bzw. Schreibvorgänge eingeschränkt oder sogar unterbunden werden.
Auch eine „Personalisierung“ der Karte ist durch die Integrierung von implementierten (verdrahteten) Sicherheitsfunktionen möglich. So kann die Eingabe eines Codes (*PIN*) verlangt und überprüft werden. Hierbei verursachte Fehlversuche können mitgezählt werden und zu entsprechenden Konsequenzen führen.

Mikroprozessorkarten I

Mikroprozessorkarten enthalten einen Mikroprozessor und verschiedene Arten von Speicher (*RAM*, *ROM*, *PROM*, *EEPROM*). Neben Daten können sie auch Programme laden und diese ausführen.
Der Mikroprozessor ermöglicht das Ausführen von komplexeren Zugriffskontrollen und Sicherheitsmaßnahmen (z.B. Verschlüsselung), um die aufbewahrten und übertragenen Daten zu schützen.

Mikroprozessorkarten sind meist für Anwendungen vorgesehen, die erhöhte Sicherheitsanforderungen benötigen.

Mikroprozessorkarten II - Kryptocontrollerkarten

Kryptocontrollerkarten gehören zu den Mikroprozessorkarten. Sie sind jedoch zusätzlich mit einem kryptografischen Koprozessor ausgestattet, der den Aufwand der Berechnung von Verschlüsselungsalgorithmen aber auch anderen Rechenoperationen deutlich verkürzt. Sie sind damit in der Lage die Sicherheit eines Mikroprozessors (zumindest im Sinne einer effektiven Verschlüsselung der Daten und Datenübertragung) noch einmal deutlich zu verbessern.

Kontaktbehaftete Chipkarten

Die Übertragung von Daten kann über eine Kontaktfläche des Chips oder aber kontaktlos erfolgen. Bei der kontaktbehafteten Datenübertragung ist eine direkte Verbindung zwischen den Kontakten des Chips und dem Lesegerät notwendig.

Abbildung 2.5: Kontaktbehaftete Chipkarte, SISDID

Da unter anderem die Lage des Chips, dessen Ausmaße und die Position der Kontakte bei einer solchen Vorgehensweise bekannt und allgemein anerkannt sein müssen, sind auch diese durch einen *ISO*-Standard (*ISO/IEC* 78162) spezifiziert.

Kontaktlose Chipkarten

Bei kontaktlosen Chipkarten ist der Chip im Innern der Karte integriert und von Außen (wenn nicht gerade eine transparente Chipkarte vorliegt; Abbildung 2.6) nicht zu erkennen. Er ist deshalb besonders gut vor äußeren Einwirkungen, wie Schmutz oder Wasser, geschützt.
Die Übertragung von Daten findet über eine in die Karte integrierte Antenne auf dem Funkweg statt. Die für diese Übertragung notwendige Energie wird durch elektromagnetische Induktion gewonnen (es ist aber nicht auszuschliessen, dass es nicht auch Chipkarten mit aktiven Energiequellen geben wird). Kontaktlose Chipkarten reihen sich damit in die Vielzahl der möglichen *RFID*-Technologien (Radio Frequency Identification) ein.

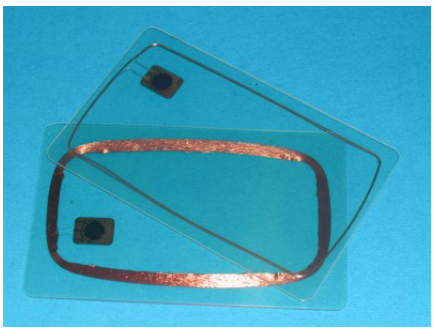


Abbildung 2.6: Kontaktlose Chipkarten (transparent), Novo-Shop

2.5.4 Optische Speicherkarten

Abbildung 2.7: Optische Speicherkarten,Lasercard

Wird auf einer Karte deutlich mehr Speicher benötigt als eine Speicherchipkarte zur Verfügung stellen kann, so empfehlen sich optische Speicherkarten. Auf einer Speicherkarte können mehrere Megabyte an Daten (derzeit maximal 6 MByte; mit Fehlerkorrektur jedoch nur noch ca. 4 MByte) gespeichert werden.
Mit Hilfe eines Lasers wird auf der Oberfläche der optischen Speicherkarte ein wieder einlesbares Muster gebrannt. Bereiche der Karte, die bereits beschrieben wurden, können nicht erneut beschrieben werden.
Die Daten auf der Karte können zwar verschlüsselt abgelegt werden, eine wirkliche Sicherheit (also zum Beispiel der Schutz vor dem unberechtigten Auslesen) wird jedoch nicht gewährleistet.
Die Standards der *ISO* und des *IEC* zu den optischen Speicherkarten sind in jeweils mehreren Teilen unter *ISO*/*IEC* 11693 und *ISO*/*IEC* 11694 zu finden.

2.6 Angriffe auf Chipkarten

Die folgende Zusammenfassung stellt keinen Anspruch auf Vollständigkeit, es soll jedoch eines vermittelt werden: Chipkarten sind heutzutage sehr weit verbreitet und geniessen

bei den Nutzern den Ruf sicher zu sein. Dieser „Ruf“ geht sogar soweit, dass bei einem auftretenden Sicherheitsproblem in Bezug auf eine Chipkarte, in der Regel davon ausgegangen wird, dass der Nutzer den sicherheitsrelevanten Fehler begangen hat (zum Beispiel die PIN weitergegeben). Das jedoch auch der Chip selbst unsicher sein kann und dieses Sicherheitsproblem dann auch ausgenutzt wurde, wird meist gar nicht berücksichtigt. Im Folgenden werden deshalb Möglichkeiten vorgestellt Informationen von Chipkarten zu gewinnen, auch ohne das man eine entsprechende Berechtigung für die Karte besitzt.

2.6.1 Time Attack

Beim Time Attack beobachtet man die Rechenzeiten des Chipsatzes für verschiedene Eingaben. Diese Beobachtungen werden analysiert und Rückschlüsse auf die im Chipsatz durchgeführten Operationen (zum Beispiel Verschlüsselungen) gezogen.
In der Realität ist diese Art des Angriffs relativ schwer durchzuführen, auch da es relativ einfach ist Sicherheitsmechanismen gegen diese Art Angriff zu implementieren. Man muss einfach eine variable Verzögerung durchführen, bevor man Ausgaben auf erfolgte Eingaben tätigt. Damit lässt man keine weiteren Rückschlüsse auf die Dauer der Berechnung zu. Der Nachteil ist natürlich: Da der Chipsatz nicht sofort nach Beendigung der Berechnung antwortet, gibt es einen Perfomanceverlust. Im Rahmen der Sicherheit kann dieser aber wahrscheinlich vertreten werden.

2.6.2 Bellcore-Angriff

Bei dem Bellcore-Angriff wird der Chipsatz verschiedenen physikalischen Extremsituationen ausgesetzt. Das reicht von der Mikrowellenbestrahlung über Temperaturwechsel bis hin zu Taktfrequenz-Störungen. Durch diese Situationen werden Rechenfehler produziert. Diese werden abschliessend mit dem Verhalten bei korrekten Rechenergebnissen verglichen und Rückschlüsse auf die Rechenoperationen des Chips gezogen.

2.6.3 Differentielle Fehler-Analyse

Als Systematisierung des Bellcore-Angriffs tritt die differentielle Fehler-Analyse auf. Dabei wird versucht ein einzelnes Bit in einem der Register der CPU umzukippen und somit ein falsches Ergebnis zu provozieren. Dieses Ergebnis wird mit dem richtigen Ergebnis verglichen. Je nach Ergebnis kann man somit Rückschlüsse auf die Verschlüsselung ziehen (vorausgesetzt das Verschlüsselungsverfahren ist bekannt), da die meisten Verfahren wohl selbst nur eine Bitmanipulation vornehmen.

2.6.4 Direkte Angriffstechniken gegen Chipkarten

Bei den direkten Angriffstechniken wird der Chip vom Kartenkörper gelöst (zum Beispiel durch Wegätzen des Plastik). Danach gibt es verschiedene Möglichkeiten: man kann den Chip unter dem Elektronenmiskroskop untersuchen, man kann ihn in Betrieb nehmen

und versuchen mit Mikroprobennadeln Berechnungen auf Leiterbahnen nachzuvollziehen oder man verändert direkt den Schaltkreis, um die Sicherheitslogik des Chips zu umgehen.

2.6.5 Stromverbrauchsanalyse

Bei der Stromverbrauchsanalyse wird, wie der Name schon sagt, der Stromverbrauch des Chipsatzes gemessen und anhand dessen versucht herauszufinden, welche Operationen der Chipsatz durchführt, bzw. ob diese erfolgreich waren.

2.7 Kategorisierung digitaler Karten

Wie schon im Abschnitt Technologien digitaler Karten angedeutet, halten wir die Abgrenzung digitaler Karten anhand der verwendeten Technologien für nicht ausreichend. Die Gründe sind verschieden und sollen hier kurz aufgeführt werden.
Eine Abgrenzung nach Technologien gibt zum Beispiel keinen Aufschluss über die Anwendungen der digitalen Karte. So ist es durchaus möglich, dass eine Karte viele technische Merkmale enthält, aber nur eine Anwendung realisiert wurde (DHL Packstation-Karte). Genauso ist aber auch der Fall denkbar, dass viele Anwendungen auf einer Karte realisiert wurden, die auch verschiedene technische Merkmale nutzen (ADAC-Dienstausweis).
Auch sind bei dieser Abgrenzung keine Aussagen darüber möglich, ob an der digitalen Karte nun eine einzige Organisation oder gar mehrere Organisationen beteiligt sind, die dann eventuell alle Zugriff auf ihre Transaktionsinformationen erhalten wollen (einige Payback-Karten).
All die genannten Beispiele haben Konsequenzen für die Sicherheit im Umgang mit digitalen Karten, die über die Betrachtung der einzelnen Technologien hinausgehen. Wenn mehrere Anwendungen auf einer Karte vorhanden sind: Lässt das Aushebeln der Sicherheitsmerkmale einer Technologie (einer einzigen Anwendung der Karte) Rückschlüsse auf den Zugang oder die Manipulation der anderen Anwendungen der Karte zu? Wenn mehrere Organisationen an einer Karte beteiligt sind, erhält dann wirklich nur die Organisation die Information zu einer Transaktion, die es auch wirklich betrifft?

Wir haben uns deshalb zusätzlich zu der Unterscheidung nach Technologien zu einer weiteren Kategorisierung digitaler Karten hinreißen lassen und möchten diese hier kurz vorstellen.

2.7.1 Single-Vendor-Single-Application

Diese Kategorie umfasst alle digitalen Karten, welche von einer einzelnen Organisation herausgegeben wurden und nur eine einzelne Anwendung gestatten. Beispiele hierfür sind die Telefonkarte (einer Telefongesellschaft) und die Kopierkarte (einer Institution).

Der Vorteil der Anbieter einer solchen Karte liegt darin, dass sie die alleinige Entscheidungsfreiheit über die Sicherheitsaspekte der Karte und auch den Umgang mit der Karte haben.

2.7.2 Single-Vendor-Multi-Applications

In diese Kategorie fallen alle digitalen Karten, welche von einem Anbieter herausgegeben werden, jedoch viele Anwendungen unterstützen. Je nachdem welche Anwendungen es konkret sind, sind auch die technischen Anforderungen verschieden. So finden sich nicht selten sehr viele verschiedene technische Merkmale auf der Karte wieder. Beispiele für diese Art von Karten sind der ADAC-Dienstausweis, den wir ganz unten konkreter vorstellen.

2.7.3 Multi-Vendor-Single-Application

Diese Kategorie mag kurios erscheinen, aber es gibt sie tatsächlich. Eine Gruppe von Organisationen gibt eine digitale Karte heraus und „teilt“ sich sozusagen die Anwendung dieser Karte. Das prominenteste Beispiel dafür sind eine Vielzahl der Payback-Karten.
Ein Hauptproblem dieser Art von Karten ist, dass zwar jede beteiligte Organisation von der gemeinsamen Anwendung profitieren möchte, sich aber dennoch niemand in die Karten schauen lassen will. So wird bei solchen Karten oftmals ein Betreiber zwischengeschaltet, der eine neutrale Verarbeitung der Kartendaten im Sinne aller Interessensgruppen (natürlich auch der Kartennutzer, soweit es der Datenschutz vorschreibt) erlaubt.

2.7.4 Multi-Vendor-Multi-Applications

Die Zukunft der digitalen Karten?
Bisher existiert - soweit wir wissen - keine digitale Karte, die versucht völlig verschiedene Anwendungen von unterschiedlichen Organisationen auf eine Karte zu konzentrieren.
Wenn man sich jedoch die Anzahl an persönlich mitgeführten digitalen Karten betrachtet, dann kann man durchaus zu dem Schluss gelangen, dass ein solcher Schritt notwendig ist, bzw. wenigstens in eine richtige Richtung gehen würde.
In einer Präsentation [4], die uns von Herrn Wilke zur Verfügung gestellt wurde, wird im Rahmen eines Smart-Card-Projekts über die Vorraussetzungen für ein solches Vorhaben spekuliert. Man geht davon aus, dass es eine Art Grundkarte gibt, deren Gerüst eine standardisierte technische Plattform und eine gewisse Anzahl festgelegter und standardisierter Grundfunktionen bildet (eine digitale Signatur, die Funktion einer Geldkarte). Darauf können zusätzliche Funktionen (Bankkarte, Betriebsausweis, usw.) aufsetzen, die an sich nicht festgelegt sind, aber dennoch die standardisierte technische Plattform verwenden. Die digitale Signatur (als unveränderliche Grundfunktion) soll das Binden aller Transaktionen an eine natürliche Person gewährleisten.
Die größten Hürden der Umsetzung eines solchen Konzepts scheinen dabei, laut Präsentation, weniger technischer sondern vielmehr rechtlicher Natur zu sein. So müssten

neben den rechtlichen Gegebenheiten zwischen Karteninhaber und der behördlich genehmigten Zertifizierungsstelle auch sämtliche Aspekte aller an der Karte beteiligten Organisationen (die Funktionen beitragen) geklärt werden.

2.8 Beispiele digitaler Karten

An dieser Stelle sollten ursprünglich mehrere Beispiele digitaler Karten genauer unter die Lupe genommen werden. Da jedoch abzusehen ist, dass wir den geplanten Umfang der Ausarbeitung damit deutlich überschreiten würden, verbleiben wir bei einem einzigen Beispiel.

Abbildung 2.8: ADAC-Dienstausweis, ADAC-Broschüre zum CarPool [1]

Unsere Wahl fiel auf die ADAC-Mitarbeiterkarte, da diese mehrere Anwendungen in sich vereinigt.
Die Karte besitzt zum einen eine Infrarot-Kodierung. Diese wird im Moment noch vorwiegend für die Zugangskontrollen innerhalb des Dienstgebäudes benutzt. Ab 2006 wird dieses technische Merkmal jedoch nicht mehr benötigt, da man dann in einen Neubau wechselt, der über eine andere Technologie verfügt.
Des Weiteren befindet sich in der relativ dicken Karte ein Legic Chip, der vor allem im Bankenbereich sehr verbreitet ist. Auf diesem Chip kann man mehrere Segmente für unterschiedliche Aufgaben kodieren. Im Moment ist jedoch nur ein Segment aktiviert worden, das für die Kantine. Da beim Legic-Verfahren der Chip einen bestimmten Kodierungsschlüssel verwendet, ist dieser auch nur mit einem entsprechenden Lesegerät der Firma auslesbar. Durch die automatische Transaktion in der Kantine wird der Essensbetrag direkt vom Konto des Karteninhabers abgebucht. Ab 2006 wird dann ein weiteres Segment der Karte frei geschaltet, der den Zugang zum neuen Gebäude regeln wird.
Eine weitere Technik dieser Karte ist die Hitag-Technik, die in einem niedrigen Frequenzbereich (Ĩ5Hz) arbeitet. Diese Technik wird für die Dienstfahrzeuge des ADAC verwendet. Benötigt ein Mitarbeiter für die Dauer seines Aufenthaltes ein Fahrzeug, kann er es online buchen. Sobald das Auto eintrifft kann er direkt zum Wagen gehen und diesen mittels der kontaktlosen Technik öffnen. Die Karte wird während der Benutzung des Wagens nur zweimal benötigt, einmal für die Erstaktivierung und letztendlich um den Wagen wieder abzugeben.

2.9 Zusammenfassung

Selbst wenn die Flut der digitalen Karten erst in den letzten zehn Jahren für die Allgemeinheit wirklich spürbar wurde, haben sie sich in einem langen Prozess, über Jahrzehnte, in unserer Gesellschaft durchgesetzt. Da die digitalen Karten auch immer mehr in Bereiche vordringen, die für das Leben in unserer Gesellschaft einen hohen Stellenwert einnehmen (genannt seien hier zum Beispiel alle möglichen Arten von Bezahlsystemen) muss der Schutz der Daten auf den Karten gewährleistet sein.
Je nach Anforderung und wahrscheinlich auch immer im Wettstreit mit denjenigen, die es geschafft haben digitale Karten zu missbrauchen, sind in den letzten 60 Jahren sehr viele verschiedene Technologien entstanden. Interessant ist, dass selbst die älteren dieser Technologien, wie die Hochprägung und der Magnetstreifen, nicht einfach verdrängt wurden, sondern inzwischen eher als kleinster gemeinsamer technischer Nenner bei der Verwendung der Karten gelten.
In unserer Ausarbeitung haben wir versucht zu vermitteln, dass sich die Technologien immer wieder einer Prüfung unterziehen müssen, da ein absoluter Sicherheitsanspruch nie gewährleistet werden kann. Auch wurde hier klar, dass die digitalen Karten manche ihrer Aufgaben eigentlich gar nicht gerecht werden, da sie nicht ohne zusätzliche Sicherheitsmerkmale auskommen. Werden aber zusätzliche Sicherheitsmerkmale eingeführt, so müssen diese auch konsequent verwendet und geprüft werden.
Ein blindes Vertrauen in die Technologie der Kartensysteme ist jedenfalls nicht angebracht, besonders wenn die alltägliche Verwendung der digitalen Karten zu einem fahrlässigeren Umgang führt.

Da das Thema der Identifikationskarten sehr breit gestreut ist, entstehen auch sehr viele verschiedene Eindrücke, wenn man versucht deren Zukunft zu prognostizieren.
Die derzeit etablierten Technologien, dass heißt Mikroprozessorkarten und Speicherchipkarten, eventuell auch die Optischen Speicherkarten, werden sich sicherlich weiterentwickeln. Die optischen Speicherkarten selbst sind jedoch in Europa scheinbar etwas in Vergessenheit geraten. 1996 gab es in der EU sehr intensive Beratungen darüber, welche Technologie Chipkarte [6] oder Optische Speicherkarte [7] für die eigenen Verwendungen zu bevorzugen sei.
Abseits der Technologien haben wir bereits mit unserer Kategorisierung (Abschnitt 2.7) versucht aufzuzeigen, in welche Richtung es ebenfalls noch gehen könnte. Eine Realisierung, von Projekten im Bereich der Multi-Vendor-Multi-Applications wäre ein deutlicher Fortschritt gegenüber der weiter anwachsenden Flut digitaler Karten.
Alles in allem kann man sagen, dass sich die digitalen Karten auch in Zukunft weiter durchsetzen werden. Es gibt momentan keinen wirklichen Grund, warum sich staatliche oder wirtschaftliche Institutionen, derzeit von dem Modell der Identifikationskarten verabschieden sollten.

Glossar

Availability: Siehe *Verfügbarkeit*.

Confidentiality: Siehe *Vertraulichkeit*.

EEPROM: Electrically Erasable PROM.

EPROM: Erasable PROM.

IEC: International Electrotechnical Commission. Internationale Organisation zur Standardisierung.

Informationssicherheit: Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen (engl. information security).

Information security: Siehe *Informationssicherheit*.

Integrität: Informationen müssen fehler- und verlustfrei behandelt werden (engl. integrity).

Integrity: Siehe *Integrität*.

ISO: International Organization for Standardization. Internationale Organisation zur Standardisierung.

ISO 7811: Sammlung von Spezifikationen zu hochgeprägten Karten, sowie Magnetstreifenkarten.

ISO 7816: Sammlung von Spezifikationen zu hochgeprägten Karten, sowie Magnetstreifenkarten.

ISO 11693: Sammlung von Spezifikationen zur Optischen Speicherkarte.

ISO 11694: Sammlung von Spezifikationen zur Optischen Speicherkarte.

PIN: Personal identification number.

PROM: Programmable ROM.

RAM: Random Access Memory.

RFID: Radio Frequency Identification.

ROM: Read Only Memory.

PROM: Programmable ROM.

SIM: Subscriber Identification Module.

PROM: Programmable ROM.

Verfuegbarkeit: Der Zugriff auf Informationen und damit verbundene Optionen ist für autorisierte Personen im vollen Umfang gewährleistet (engl. availability).

Vertraulichkeit: Auf Informationen dürfen nur autorisierte Personen und Prozesse zugreifen (engl. confidentiality).

Literaturverzeichnis

[1] ADAC. *Broschüre ADAC-CarPool*, 2005. Inklusive freundlicher Beratung durch den ADAC und Herrn Steinkamp!

[2] Frank Hofmann. *Webseite über Identifikationskarten*, 2001. http://archiv.tu-chemnitz.de/pub/2001/0050/data/Kapitel1_1.html.

[3] Philipp Schlicker. *Smart Cards*, 2002. http://www-ti.informatik.uni-tuebingen.de/deutsch/lehre/ss02/proseminar/ausarbeitungen/philipp_schlicker.pdf.

[4] Wolfgang Schneider. *Umsetzung Des Digitalen Signaturgesetzes*. GMD und Fraunhofer Insititut, 2005-06-06 verarbeitet. http://www.darmstadt.gmd.de/TDOT99/schneider99.ppt.

[5] Daniel Sirz. *Chipkarten-Systeme*, 2005-06-06 verarbeitet. http://pi1.informatik.uni-mannheim.de/~pagnia/mobile/ausarbeitungen/T6-Chipkarten.pdf.

[6] Europäische Union. *Anhörung Chipkarten (Card Dynamics Limited)*, 1996-10-14. http://www.europarl.eu.int/hearings/transit/dynamics_de.htm.

[7] Europäische Union. *Anhörung Optical Card (Canon)*, 1996-10-14. http://www.europarl.eu.int/hearings/transit/canon_de.htm.

[8] Wolfgang Rankl und Wolfgang Effing. *Handbuch der Chipkarten*. Carl Hanser Verlag München Wien, 4. Auflage, 2002.

3 eHealth: Gesundheitskarte, elektronische Rezepte

Katja Warczecha, Tim Friese

3.1 Abstract

In diesem Dokument wollen wir uns mit dem Thema eHealth beschäftigen. Nach einer kurze Bestandsaufnahme zum Thema eHealth werden wir einen Vergleich, besonders in Bezug auf die elektronische Gesundheitskarte, zu anderen Staaten vornehmen. Des weiteren gehen wir auf das Konzept der Gesundheitskarte ein und zeigen Vor- und Nachteile sowie die Sicherheit des Systems auf.

3.2 Einleitung

Über den Kunstbegriff eHealth herrscht Uneinigkeit, was dieser genau bezeichnen soll. Je nach Zielgruppe vermischt sich eHealth mit anderen Begriffen wie zum Beispiel Telemedizin, Online Health und Cybermedizin. Es gibt viele Definitionen was eHealth eigentlich sei, jedoch sticht eine besonders hervor. Nach Eysenbach (2001) wird unter eHealth nicht nur "eine technische Entwicklung, sondern auch eine [...] (besondere) Denkweise, Einstellung und Verpflichtung zu vernetztem und globalem Denken, um die Gesundheitsversorgung [...] durch den Gebrauch von Informations- und Kommunikationstechnologie zu verbessern" [6], gesehen. Mit dem Begriff eHealth soll also gezeigt werden, dass etwas Neues entstehen soll, dass Teile der Medizin und das Internet vereinigt. "E-Health wird vorangetrieben von Non-Professionals, namentlich den Patienten (Konsumenten), die mit ihren Interessen neue Services im Gesundheitswesen entstehen lassen - zumeist um ihre Emanzipationsbestrebung durch den Zugang zu Informationen und Wissen zu stärken." [6] (Della Mea, 2001; cf. Allen, 1999). Aber welche Gebiete beinhaltet eHealth? eHealth umfasst unter anderem das Gebiet der Telemedizin, sofern es sich auf die Internet-Infrastruktur/-Technik bezieht. Auch wird der Ansatz einer direkten Patient-Computer-Interaktion als Ergänzung des Arztgesprächs eHealth zugeordnet. Weiterhin wird die Vernetzung im Gesundheitssystem und auch generelle IT-getriebene Infrastrukturen zu eHealth gezählt. Hinzu kommt das Bestreben von verschiedensten Stellen, wie zum Beispiel Leistungsträger und Verbraucher, die Informationen und Dienstleistungen über das Internet für jeden einfach und benutzergerecht zugänglich machen wollen.

3.3 Status heute

Das Großprojekt eGK wird bereits in kleinen Testprojekten, z.B. in Trier, erprobt. In diesen Gebieten zeichnet sich das Vorhaben der eGK als positiv ab, jedoch gibt es bisher noch keine klaren Lösungsvorschläge, wenn das Problem der Umsetzung europaweit betrachtet wird. Von oben her werden Beschlüsse gefasst, wobei der Blick für die Auswirkungen teilweise fehlt, die dadurch entstehen. Der Starttermin 01.Januar 2006, für Deutschland, scheint utopisch, in Anbetracht dessen, dass weder mit der Programmierung begonnen noch die Hardware festgelegt wurde.
Phasen zur eGK:

1. Phase

    a. Einführung eGK mit Versichertendaten, Lichtbild, E111

    b. Accesspoints; Integrationsszenarien mit Primärsystem; Applikationen nachladen können; Möglichkeit für Updates von Administrativen Daten

2. Einführung eRezept

3. Einführung Notfalldaten, Arzneimitteldokumentation

4. Mehrwertapplikationen

3.4 Internationaler Vergleich

Es gibt viele Ansätze für das eHealth-System, besonders vielfältig sind die Lösungen der Gesundheitskarte. Sie reichen von RFID-Chips bis zu ID-Cards. In Deutschland soll als eGK ein Prozessor-Chipkarte eingesetzt werden, welche Informationen über den Patienten speichern kann. Zum einen sind das Grunddaten, wie Name, Adresse, Kassen- und Versichertennummer. Weiterhin können optionale Daten, wie Blutgruppe, Allergien und Spenderinformationen abgelegt werden. Die Karte soll auch die persönliche elektronische Patientenakte (ePA) speichern, die auf Grund der Größe jedoch nicht direkt auf der Karte gespeichert wird, sondern über einen Link auf der Karte erreichbar ist. Ein ähnliches Prinzip wird in Österreich angewandt, die Karte beinhaltet jedoch dort zusätzlich eine Signatur des Patienten. Das Rollout der eGK in Östereich hat am 30.Mai 2005 begonnen. Pro Tag werden ca. 70000 Karten verschickt. Pro Woche werden 500 Arztpraxen an das Gesundheits-Informations-Netz (GIN) angeschlossen. Insgesamt sollen 8 Millionen "e-cards" und 24.000 Ordinationskarten für Ärzte und Apotheker ausgeliefert werden. Die Kosten für die Karte, 10 EURO, müssen von dem Versicherten bezahlt werden. Hardware- und Anschlusskosten werden von der österreichischen Sozialversicherung übernommen. Laufenden Kosten müssen jedoch von den Arztpraxen selbst übernommen werden. In Deutschland hingegen müssen die Kosten für Hard- und Software von den einzelnen Arztpraxen selbst getragen werden. Diese belaufen sich auf ca. 2000 EURO für eine kleine Arztpraxis. Für die eGK werden wahrscheinlich einmalig ca. 30 EUR fällig. Bei zusätzlicher Nutzung der Signatur werden nochmals 10 EURO pro Jahr fällig. Diese

wird jedoch nur benötigt um die ePA auf einem Server zu hinterlegen und deren Zugriffsrechte sowie Authorisationen zu regeln. Während in Österreich die Arztpraxen über ein gesondertes Netz verbunden werden, soll dies in Deutschland hingegen über das Internet stattfinden. Viele der europäischen Staaten führen die Prozessorkarte ein. In Luxemburg,

Abbildung 3.1: Kartenlayot der verschiedenen eGK

Dänemark, Niederlande und Portugal werden dagegen Magnetstreifenkarten eingesetzt. Vereinzelt ist geplant die Gesundheitskarten mit der EHIC (European Health Insurance Card) zu kombinieren. Dies Kombination soll den Auslandskrankenscheins ablösen. In

Abbildung 3.2: Kartenlayout mit EHIC

Amerika werden RFID-Chips eingesetz, welche durch geeignete Lesegeräte ausgelesen werden können und das Laden der Patientendaten von einem Server ermöglichen. Auf Grund der gesetzlichen Lage der einzelnen Ländern müssten eGK und RFID-Chip jeweils angepasst werden, es sei denn es würden entsprechende Gesetzesänderungen folgen.

3.5 Konzept Gesundheitskarte

Wesentlicher Bestandteil der Umsetzung von eHealth ist die eGK. Sie betrifft Gesetzgeber, Leistungsträger, Ärzte und Patienten. Dazu sollen die einzelnen Parteien in hinblick auf ihre Vorstellungen genauer betrachtet werden.

3.5.1 Gesetzgebung

§291a im SGB V [4, 2] beschreibt, welche Anforderungen die eGK zu erfüllen hat. Laut diesem gesetz müssen folgende Punkte erfüllt sein. Technisch mus die eGK geeignet sein die Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen. Administrative und medizinische Daten des Patienten muss sicher und geschützt sein. Durch einen Pflichtteil wird festgelegt welche administrativen Daten gespeichert werden müssen. Im optionalen Teil können medizinische Daten gespeichert werden. Administrative Daten sind: allgemeinen Patientendaten, Versicherungsstammdaten (Name, Anschrift, usw.), Versicherungsnummer und elektronische Rezepte (eRezept). Zu den optionalen Daten zählen Arzneimitteldokumentation, um z.B. Unverträglichkeiten oder Wechselwirkungen zu verhindern, medizinische Notfalldaten, Patientenquittungen, elektronische Arztbriefe (eArztbrief), elektronische Patientenakte (ePA) - Befunde, Diagnosen, Therapieempfehlungen, Behandlungsberichte - von Versicherten selbst oder für sie zur Verfügung gestellte Daten, wie Diabetiker-/ Blutdruck-Tagebuch, Medikamenteneinnahmeplan, usw.. Um Patientenrechte und Datenschutz zu gewähren muss ein Patient erst seine Einwilligung erteilen, damit ein Arzt Zugriff auf die Daten der eGK des Patienten erhält. Im Sinne der Datenschutzkontrolle müssen mindestens die letzten 50 Zugriffe auf die Daten protokolliert werden.

3.5.2 Erwartungen (qualitative und ökonomische Gesichtspunkte)

Um eine grundlose Einführung der eGK zu verhindern, werden Erwartungen an das Großprojekt gestellt, die aktuelle Defizite ausgleichen sollen. Als wichtigstes Argument wird immer wieder die Vermeidung von Doppeluntersuchungen angebracht, welches durch das Aufsuchen mehrerer Ärzte für ein und die selben Beschwerden entstehen. Des weiteren sollen durch die Einführung des Lichtbildes die Vergabe der eGK an dritte Personen verhindert werden. Sektorenübergreifende Verzahnung und Abstimmung von gemeinschaftlichen Behandlungsprozessen sind auch wesentliche Argumente. Die stärkere Einbindung in Behandlungsprozess fördert die Selbstverantwortlichkeit des Patienten. Warum diese Selbstverantwortlichkeit wichtig ist, lässt sich klar daraus entnehmen, dass sich das Problembewusstsein der Patienten mit den Jahren gesteigert hat. Gesundheit ist heutzutage nicht mehr nur der reine Arztbesuch, sondern auch das eigenen, durch Bücher und Internet, erweiterte Wissen, welches von Ärzten unterschiedlich aufgenommen wird. Eine erste Anwendung der eGK ist das eRezept. Es stellt die digitale Version eines herkömmlichen Rezeptes dar. Es enthält Informationen zur Verschreibung von Arzneimitteln und wird vom Arzt elektronisch signiert. In der Apotheke wird das Rezept

um apothekenspezifische Daten ergänzt und an deren Rechenzentren weitergeleitet. Von dort aus gelangen die Daten zu den Kostenträgern (Versicherungen). Mit Einführung der ePA und des eArztbrief soll eine elektronische Zusammenfassung des Zustandes eines Patienten verfügbar gemacht werden. Dies beinhaltet Informationen aller beteiligten medizinischen Bereiche mit deren jeweiligen geeigneten Formaten/Medien (Text, Grafik, Bild, Film, Ton). Im Idealfall werden nicht nur die Daten des aktuellen Falles zusammengetragen, sondern auch alle verfügbaren Informationen früherer Krankheiten und Behandlungen integriert. Wie bei der eGK werden auch an die ePA Anforderungen gestellt. Dazu gehören unter anderem technische Aspekte, wie die verlustfreie, revisions- und rechtssichere Langzeitarchivierung aller Daten, die Zugriffsregulierung auf Personendaten und der elektronischen Austauschs über kryptografisch gesicherte Kommunikationswege. Bei der Übertragung eines eArztbriefes werden nur Informationen, die sich auf den jeweiligen Behandlungsfall beziehen, übermittelt. Dies geschieht jedoch nur mit Zustimmung des Patienten.

3.5.3 Zielsetzung der Telematik

Die Telematik verfolgt mit ihren Erwartungen also konkrete Ziele, die hier nun genauer betrachtet werden sollen.

Motivation

Warum beschäftigen wir uns mit dem Thema Gesundheit so umfangreich, wenn alles so gut läuft? Wie in allen Gebieten des Lebens gibt es auch in der Medizin eine nicht enden wollende Flut von Informationen, die so nicht mehr zu handhaben ist. Wartezeit und dokumentarischer Aufwand sind enorm, dass teilweise die Qualität leidet und Kosten, eigentlich gesenkt werden sollen, steigen. Es bestehen Koordinierungs-/ Integrations- / Vernetzungs- und Kommunikationsprobleme zwischen allen Beteiligten.

Ziele

In einer groß angelegten Aktion werden versucht viele Probleme zu lösen und dementsprechend sind die Ziele hoch gesteckt. Eines der Ziele ist der hohe Qualitätsanspruch. Genauer gemeint sind hiermit optimierte Behandlungskonzepte und -prozesse, insbesondere bei chronischen Erkrankungen. Ambulante und stationäre medizinische Leistungen sollen enger miteinander Verzahnt werden. Alle medizinischen Daten sollen sicher verfügbar gemacht werden, um wie bereits erwähnt Doppeluntersuchungen und somit auch sekundäre Beeinträchtigungen (Nebenwirkungen) zu vermeiden, dazu gehört auch, dass die Daten valide sind. Unteranderem soll der Missbrauch oder die Fehlverabreichung von Medikamenten reguliert werden, dies wird als Arzneimittelsicherheit bezeichnet. Auch die informationelle Selbstbestimmung (unter anderem die des Patienten) soll gesichert werden. Das "eigentliche" Ziel sind medizinische Dokumentations-, Terminologie- und Klassifizierungssysteme, mit hohem Verbindlichkeitsgrad. Diese sollen die individuelle Versorgungsqualität, bei gleichzeitiger Senkung der Ausgaben, im Gesundheitswesen

steigern.

3.6 Sicherheit und Schutzmechanismen

Nun wollen wir genauer durchleuchten, was unter Sicherheit verstanden wird und welche Schutzmechanismen es geben soll. Auch die Ausfallsicherheit und Reaktionszeit des Systems soll hier betrachtet werden. Es unterschiedliche Akteure, die unterschiedlich schädliche Aktivitäten auslösen können. Zunächst wäre da der Angreifer. Er ist ein unautorisierter Nutzer von außen, der vorsätzlich unerlaubt Zugriff auf die Daten nehmen will. Der häufigste Akteur ist der Benutzer, ihm sind oftmals Unachtsamkeit, Fehlverhalten und teilweise auch vorsätzliches Handeln, nachzutragen. Gleiches gilt für administratives Personal. Nicht auszuschließen sind die Hard- und Software, welche unter Störungen und Fehlern leiden können.

3.6.1 Technische Sicherheitsmechanismen

Unter technischen Sicherheitsmechanismen werden hier die allgemeinen Schutzziele, die verfolgt werden sollen, verstanden. Hierzu zählt in erster Linie die Verfügbarkeit. Diese umfasst System- und Komponentenausfälle. Weiterhin spielt die Integrität eine große Rolle, wobei hier der Schutz vor Manipulation und Autorisation dazu gehören. Vertraulichkeit, also der Schutz vor unbefugter Kenntnisnahme und Autorisation schließen sich dem an. Wichtig sind auch Verbindlichkeiten, die hier die Authentizität, also die Identität von Mensch, Programm und Maschine bescheinigen können, sowie die Nicht-Abstreitbarkeit. Die Anforderungen, die sich also aus den technischen Sicherheitsmechanismen ergeben sind Authentifizierung, Autorisierung, vertrauliche Datenspeicherung, Nicht-Abstreitbarkeit, sichere / vertrauliche Kommunikation und sichere Empfangsbestätigung. Hierzu ist ein hoher Vernetzungsgrad mit existierenden Primär- und Backendsystemen, also den IT-Systeme von Krankenhäusern, Apotheken, Arztpraxen usw. nötig. Im folgenden werden die genannten Sicherheitsmechanismen erläutert.

Authentifizierung

Die Prüfung der angegebenen Identität einer Person gegenüber einem System oder zwischen Systemen wird als Authentifizierung bezeichnet. Dieser Sicherheitsmechanismus ist uns allen bekannt, aus dem täglichen Leben, wenn wir unseren PIN der Geldkarte eingeben müssen oder uns in unsere Rechner einloggen. Ein weiterer möglicher Mechanismus ist die Prüfung der biometrischen Eigenschaften. Für die Umsetzung der Authentifizierung gibt es verschiedene kryptographische Verfahren und Protokolle (z.B. ISO/IEC 9798 oder ISO/IEC 10181-2).

Autorisierung

Ob man eine gewünschte Anwendung ausführen darf oder nicht, wird durch die Autorisierung bestimmt. Dies heißt zum Beispiel, dass die Berechtigung erteilt werden kann,

auf bestimmte Daten Zugriff zu nehmen, diese sogar zu manipulieren oder eine Transaktion mit einer Kreditkarte durchführen zu können. Weiterhin ist es möglich, dass durch die Authentifizierung einer Person auch schon die Autorisierung festgelegt ist. Bei der eGK beinhaltet die Autorisierung, je nach Arzt, auch die Erlaubnis des Patienten, auf seine Gesundheitsdaten zuzugreifen zu dürfen.

Vertraulichkeit

Folgende Anforderungen müssen erfüllt sein, um einen vertrauenswürdigen und sicheren Austausch von elektronischen Daten zu gewährleisten:

- Identifikation und Authentifizierung der Person
- Erkennung von Manipulation (Integrität der elektronischen Daten)
- Authentizität (Echtheit des Datenursprungs)
- Vertraulichkeit (Verschlüsselung der elektronischen Daten)
- Verbindlichkeit (Nichtabstreitbarkeit von Datenursprung und Datenempfang).

Nicht-Abstreitbarkeit

Die Verbindlichkeit einer Nachricht kann über kryptographische Verfahren nachgewiesen werden. Dabei sind gemäß dem ISO/IEC-Standard 10181-4 mehrere Arten zu unterscheiden. Die zentralen Dienste sind die Nichtabstreitbarkeit des Ursprungs einer Nachricht (non-repudiation of origin, NRO) und die Nichtabstreitbarkeit des Empfangs einer Nachricht (non-repudiation of receipt, NRR). Im ersten Fall kann der Empfänger einer Nachricht nachweisen, von welchem Sender die Nachricht verschickt wurde. Im zweiten Fall kann der Sender einer Nachricht beweisen, dass der Empfänger diese bekommen hat. Das Prinzip entspricht dem Einschreiben mit Rückantwort der Post.

Ver-/Entschlüsselung

Wenn Daten durch einen bestimmten Algorithmus verändert werden und die Regel zur zur Wiederherstellung der Daten (Entschlüsselung) nur ausgewählten Personen zugänglich ist, die somit die Daten interpretieren können, wird dies als Verschlüsselung bezeichnet. Es gibt unterschiedliche Verschlüsselungsverfahren wie symmetrische, asymmetrische und hybride Verschlüsselung. Asymmetrischen Verfahren bestehen aus einem Schlüsselpaar, einem öffentlichen Schlüssel, der zum Verschlüsseln verwendet werden kann und einem privaten Schlüssel, der nur zum Entschlüsseln der Daten dient. Beide Schlüssel werden in einem so genannten Trustcenter zertifiziert. Beim symmetrischen verschlüsseln geschieht die Ver- und Entschlüsselung mit ein und dem gleichen Schlüssel.

Zeitstempel

Der Zeitstempel (time stamp) ist eine authentische und unfälschbare Verknüpfung von Daten mit einem Datum. Es handelt sich hierbei um eine elektronische Signatur, welche eine elektronische Bescheinigung einer Zertifizierungsstelle besitzt.

Integritätsprüfung

Die Eigenschaft einer Nachricht wird als Integrität beschrieben, wenn sie unverändert zwischen Sender und Empfänger übertragen worden ist.

3.6.2 Umsetzung von eHealth

Folgende Abbildung zeigt den schematischen Aufbau des "Gesundheitsnetzes". Anhand der Abbildung sollen die Kommunikationskanäle dargestellt werden. Rotmarkierte Linien stellen gesicherte Verbindungen oder Bereiche dar. Nachfolgend wird die Abbildung

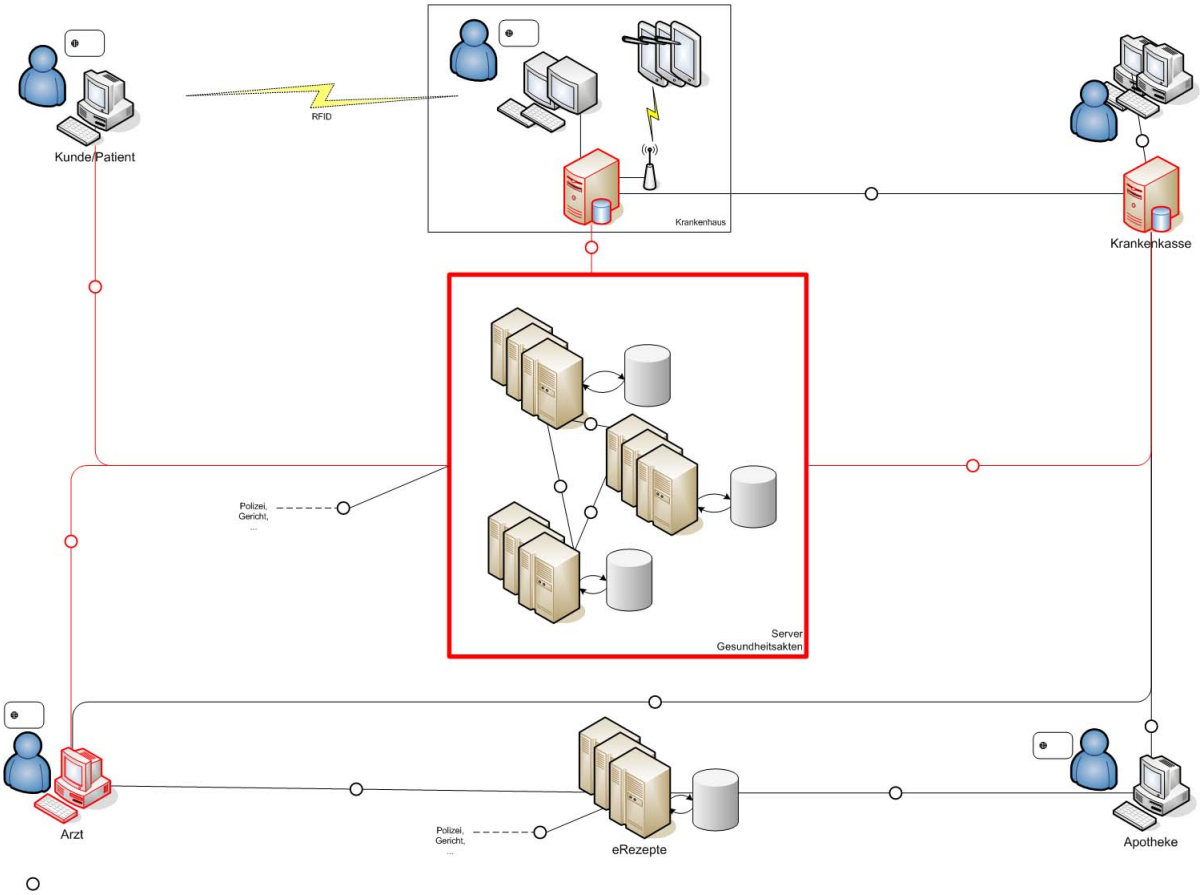


Abbildung 3.3: Aufbau des eGK-Systems

genauer erläutert. Die Krankenkassen nehmen die Kundendaten auf und erstellen die

eGK, die dann dem Kunden zugestellt wird. Weiterhin besteht die Möglichkeit für die Krankenkasse, einen Teil der Daten der Gesundheitsakte vom Server zu lesen. Ärzte, Krankenhäuser und Apotheken sind ebenfalls mit den Krankenkassen verbunden, um die Abrechnungen ihrer Leistungen zu tätigen. Durch den Zugriff der Apotheken auf den eRezepte-Server, können eRezept des Patienten gelesen und entsprechenden Medikamente ausgeben werden. Der Zugriff auf den Server der Gesundheitsakten ist den Apotheken verwehrt. Der Arzt hat Zugriff auf den eRezepte-Server um das Rezept des Patienten zu hinterlegen. Weiterhin besitzt der Arzt Zugriff auf den Gesundheitsakten-Server, für den er eine Karte benötigt, die ihn dazu berechtigt, in Verbindung mit der eGK des Patienten, auf die entsprechenden Akten zugreifen zu können. Er kann dort der Akte neue Befunde hinzufügen und alte Befunde lesen. Dies kann Mehrfachdiagnosen verhindern. Durch Setzen von Zugriffsrechten kann der Patient dennoch Mehrfachdiagnose fordern, indem er dem Arzt andere Befunde vorenthält. Der Patient selbst kann die Akte einsehen, jedoch nicht verändern. Einfluss auf die Akte kann der Patient nur nehmen, in dem er entscheidet welche Diagnosen / Befunde aufgenommen werden bzw. Zugriffsrechte für die einzelnen Ärzte setzt. Die Krankenhäuser besitzt eigene Patientenakten auf internen Servern, hat jedoch auch Zugriff auf den Gesundheitsakten-Server. Dort kann die Akte eines Patienten gelesen und neue Befunde hinzugefügt werden. Weiterhin können die Krankenhäuser Rezepte auf den eRezepte-Server hinterlegen. Dieser Kanal ist in der Grafik auf Grund der Übersichtlichkeit nicht eingezeichnet. Es ist möglich den Patienten mit einem RFID-Sender auszustatten, damit die Krankenhäuser schnelleren Zugriff auf die einzelnen Patientendaten erhalten. Per PDA kann der RFID-Chip auslesen und die Patientendaten vom internen Server abgerufen werden. Änderungen an der bestehenden Akte dürfen nicht gemacht werden.

3.6.3 Performanz und Verfügbarkeit

Es gibt bereits Anforderungen, die die Antwortzeiten des Systems spezifizieren und die maximalen Ausfallzeiten des Gesundheitssystems beschreiben.
Die Antwortzeiten werden unterteilt in zwei Kategorien:

- Kategorie AZ1 - Hierbei handelt es sich um kurze Antwortzeiten. Als wünschenswert werden bis zu 3 Sekunden, in 98% aller Fälle gezählt. Als tolerierbar gilt eine Antwortzeit bis zu 8 Sekunden, in weniger als 2% der Fälle. Als nicht tolerierbar gilt eine Antwortzeit über 8 Sekunden in weniger als 0,1% der Fälle.

- Kategorie AZ2 - Hierbei handelt es sich um längere Antwortzeiten. Als wünschenswert werden bis zu 8 Sekunden, in 98% aller Fälle gezählt. Als tolerierbar gilt eine Antwortzeit bis zu 30 Sekunden, in weniger als 2% der Fälle. Als nicht tolerierbar gilt eine Antwortzeit über 30 Sekunden in weniger als 0,1% der Fälle.

Die Verfügbarkeit wird ebenso in Kategorien aufgeteilt:

- Kategorie V1 - Hochverfügbare Geschäftsvorfälle, die einen Ausfall max. im Minutenbereich zulassen. Längere Wartezeiten sind nicht akzeptabel. Der Prozess fällt

aus und kann ggf. durch einen Alternativprozess ersetzt werden. Bei kritischen Services können gravierende Folgen eintreten. Eine Verfügbarkeit von mindestens 99,999% ist zu erfüllen.

- Kategorie V2 - Zeitkritische Geschäftsvorfälle, die einen Ausfall im Minuten- bis 0,5 Stundenbereich zulassen. Es drohen schwere Akzeptanzverluste für die Telematik-Infrastruktur. Eine Verfügbarkeit von mindestens 99,99% ist zu erfüllen. Die Prozesse müssen durch Ausweichlösungen ablaufen, wenn die entstehenden Wartezeiten nicht zumutbar sind. Falls keine Ausweichlösungen existieren, muss der Prozess ausfallen und soweit möglich später nachvollzogen werden.

- Kategorie V3 - Weniger zeitkritische Geschäftsvorfälle, wobei ein Ausfall von mehreren Stunden hinnehmbar ist. Ein Ausfall von bis zu 8 Stunden ist akzeptabel. Eine Verfügbarkeit von 99,9% ist zu erfüllen.

3.7 Kritik

Es gibt eine Menge Kritikpunkte, die man betrachten kann, deshalb erfolg hier nur eine Zusammenfassung, der wichtigsten Punkte. In den wesentlichen Punkten unterliegt die eGK den Entscheidungen des Patienten, d.h. er kann allein bestimmen, welche Daten gespeichert werden und welche nicht. Datenschützer sind der Meinung, dass der Patient auch entscheiden können sollte, ob bestimmte Daten, zum Schutz der persönlichen Gesundheitsdaten, für bestimmte Ärzte gesperrt werden oder nicht. Wenn wir uns aber das Ziel der eGK vor Augen halten, welches besagt, dass kostspielige Doppeluntersuchungen dezimiert werden sollen, bleibt offen, wie hier weiter zu verfahren ist. Unberechtigte Nutzung der Karte durch dritte wird durch die einführung des Lichtbildes verhindert. Die Datenhoheit der Patienten vernichtet also den vermeintlichen Nutzen der elektronischen Gesundheitskarte, weil der behandelnde Arzt sich nicht auf die Vollständigkeit der gespeicherten Daten verlassen kann und somit nochmals alle Untersuchungen vornehmen muss. Anderseits, wenn ein Arzt die Daten eines anderen Arztes vorliegen hat, wie objektiv und unbefangen kann er sich dem Fall dann annehmen? Datenschützer sehen durch die zentrale Speicherung aller Daten über einen Patienten, die Möglichkeit des Missbrauchs der Gesundheitsdaten, d.h. es ist möglich Statistiken über die Patienten zu erheben und diese dann gezielt z.B. mit Werbung zu bombardieren. Ein weiteres Problem sind die "historisch gewachsenen" Rechnersysteme in den Krankenhäusern und ihrer Verwaltung sowie das unsichere Internet als Medium der Kommunikation. Anbindungs- und Umstellungskosten bei Ärzten und Krankenhäusern usw. müssen getragen werden, die Finanzierung ist jedoch noch nicht endgültig geklärt worden. Laut einer Umfrage in Deutschland, wie die Deutschen zur Einführung der eGK stehen, entstand folgendes Resultat: 72% der Bürger finden die eGK wünschenswert, 27% finden sie weniger wünschenswert und 1% wusste nicht / hat keine Angabe gemacht. Die Regierung will zur Umsetzung der eGK ein subjektives Gefühl größerer Sicherheit in den Punkten Arzneimitteldokumentation und Verringerung der Papierdokumente zugunsten der Karte erzeugen, d.h. z.B. größere Gewähr, dass der Notarzt im Notfall relevante Informationen

besser erfassen kann. Fraglich hierbei ist allerdings, inwieweit die Bürger aufgeklärt werden über den Datenschutz und welche Risiken sich womöglich hinter der Zentralität aller Daten einer Person verstecken. Auch wichtig ist es zu wissen, dass im Rahmen (lebensbedrohender) Notfallsituationen das Recht auf körperliche Unversehrtheit des Patienten höher wiegt als sein informationelles Selbstbestimmungsrecht. Kritik gibt es auch an der elektronische Patientenakte. Die Befürchtungen gehen dahin, dass die gesammelten Daten für andere Zwecke, z. B. strafrechtliche Ermittlungsverfahren, Täterprofile etc. verfügbar gemacht werden könnten. Der Patient hat häufig keine Übersicht und auch keinen Einblick in die gesammelten Daten, somit kann sein Recht auf informationelle Selbstbestimmung verletzt werden. Ob die erhofften Einspareffekte durch die elektronische Akte tatsächlich realisiert werden können, ist auch fraglich, die Theorie geht davon aus, dass Doppeluntersuchungen vermieden werden, wenn jedem Arzt alle Ergebnisse vorangegangener Untersuchungen bekannt sind. Ein gewissenhafter Arzt wird sich aber schon aus haftungsrechtlichen Gründen nicht auf die Befundergebnisse und Untersuchungen der vorbehandelnden Ärzte verlassen können. Anhand der Abbildung 3.3 aus dem Kapitel 3.6.2 sind zwar gesicherte Zugänge ersichtlich, jedoch fehlen dort vielleicht Absicherungen, an die bisher noch nicht gedacht wurde. Im Kapitel 3.6.3 wurden Antwortzeiten und Verfügbarkeit aufgelistet, jedoch ist nicht klar, was passiert, wenn diese Zeiten nicht eingehalten werden. Wer ist dann zur Rechenschaft zu ziehen? Wie sollen diese Zeiten umgesetzt/eingehalten werden? Anwendbarkeit ist auch bereits als Anforderung erfasst, sodass auch ältere und kranke Menschen die Anwendungen der eGK bedienen können müssen. Allerdings kann es hier schnell unübersichtlich für den Patienten werden, wenn er z.B. entscheiden soll, ob die Daten von Dritten gelesen werden können sollen. Auch die Entscheidung für eine Karte ist etwas vorschnell gefallen, so hätte man sich bereits ausreichende Gedanken über das Medium machen müssen, damit alle Beteiligten einen effektiven Nutzen davon tragen können. Positiv zeichnet sich ab, dass durch die eGK auch das eRezept eingeführt werden soll. Die Kosten für ein herkömmliches Rezept sollen angeblich von aktuell 0,34 EURO auf 0,07 EURO gesenkt werden. Dies macht bei der Annahme, dass 750 Mio. Verordnungen pro Jahr ausgegeben werden eine Einsparung von ca. 202 Mio. EURO.

3.8 Fazit

Bisher gibt es noch kein ausgereiftes System, d.h. keine komplexe Lösungsstrategie und -Umsetzung. Derzeit läuft überwiegend der Testbetrieb in kleineren Gebieten. Das ganze Projekt ist sehr kostenintensiv und es muss sich noch zeigen, inwiefern wirklich Einsparungen erfolgen werden oder vielleicht doch mehr Kosten entstehen als es heutzutage bereits der Fall ist. Teile des Projektes wurden nicht intensiv genug durchdacht, sondern einfach beschlossen. Als offene Punkte stehen also immer noch die Finanzierung und die genaue Kennzeichnung der Einspareffekte, an. Weiterhin sind die Haftungsfragen bei Nichtverfügbarkeit des Systems oder Teilen davon zu klären. Um eine einheitliche Struktur für die medizinischen Daten zu erhalten muss eine standardisierte medizinische Dokumentation definiert werden. Die Rahmenarchitektur ist im Allgemeinen vorhanden,

aber eine Lösungsarchitektur fehlt, bis auf die der kleinen Testprojekte, vollends.

Glossar

eGK: Elektronische Gesundheitskarte.

EHIC: European Health Insurance Card - Nachfolger des Auslandskrankenscheins.

ePA: Elektronische Patientenakte.

eRezept: In elektronischer Form vorliegendes Rezept.

E111: Auslandskrankenschein.

GIN: Gesundheits-Informations-Netz.

Magnetstreifenkarte: Etwa visitenkartengroße Plastik-Karte auf deren Rückseite ein Magnetstreifen angebracht ist, welcher die Daten speichert.

Prozessorkarte: Etwa visitenkartengroße Plastik-Karte mit integriertem Chip, welcher die Daten speichert. Ein Prozessor regelt den Zugriff auf diese Daten.

Telematik: Auch Gesundheitstelematik, ist ein Kunstwort aus den beiden Bereichen Telekommunikation und Informatik. Darunter versteht man die Informationsverknüpfung von mindestens zwei EDV-Systemen mit Hilfe eines Telekommunikationssystems mit einer speziellen Datenverarbeitung. Anders ausgedrückt, eine patientenorientierte und gesundheitliche Versorgung.

Telemedizin: Ist ein Teilbereich der Telematik im Gesundheitswesen und bezeichnet den Einsatz von Telematikanwendungen, wie Diagnostik und Therapie, in räumlicher Distanz zwischen Arzt/Ärzten und Patienten. (Kommunikationsverbesserung im Gesundheitswesen.)

Literaturverzeichnis

[1] A. Kurtz. Elektronische Patientenakte. *www.uni-heidelberg.de*, 2004. http://www.rzuser.uni-heidelberg.de/~akurtz/vortraege/epa_praesentation.pdf.

[2] Bund. SGB V - Sozialgesetzbuch Fünftes Buch - Gesetzliche Krankenversicherung. *www.sozialgesetzbuch.de*, 2000. http://www.sozialgesetzbuch.de/gesetze/05/.

[3] Bund. Bundesdatenschutzgesetz (BDSG). *www.bfd.bund.de*, 2002. http://www.bfd.bund.de/information/BDSG_neu.pdf.

[4] Bund. Krankenversichertenkarte. *www.bfd.bund.de* , 2005. http://www.bmgs.bund.de/download/gesetze_web/sgb05/sgb05x291.htm.

[5] CompuGROUP Health Services GmbH. VITA-X: vita-X Gesundheitsakte. *www.cg-hs.de*, 2005. http://www.cg-hs.de/?poid=abd6526c-00cc-4553-80a2-a5ce3f84c8fb.

[6] ComputerBase. ComputerBase - Lexikon: E-health. *ComputerBase*, 2005. http://www.computerbase.de/lexikon/E-health.

[7] DIMDI. DIMDI - Die elektronische Gesundheitskarte. *DIMDI - Deutsches Institut für Medizinische Dokumentation und Information*, 2000. http://www.dimdi.de/static/de/ehealth/karte/index.htm.

[8] Dipl.-Ing. Heinz Otter. Die e-card im internationalen Vergleich. *www.chipkarte.at*, 2004. http://www.chipkarte.at/mediaDB/81625.PDF.

[9] diverse. Diverse Artikel zur Gesundheitskarte. *www.heise.de*, 2000. http://www.heise.de/newsticker/search.shtml?T=Gesundheitskarte.

[10] Dr. Frank Warda, Dr. Guido Noelle. *Telemedizin und eHealth in Deutschland*. DIMDI, 2002. ISBN 3-89906-701-0 http://www.dimdi.de/static/de/ehealth/public/telematikbuch19_02_03_web.pdf.

[11] EUROPÄISCHE KOMMISSION. eGesundheit. *EU-NACHRICHTEN*, 2002. http://www.eu-kommission.de/pdf/eunachrichten/eEur-Thema_INTERNET.pdf.

[12] KrankenkassenRatgeber. Kritik am Gesetzesentwurf zur elektronischen Gesundheitskarte. *www.medizininformatik-treffpunkt.de*, 2005. http://www.medizininformatik-treffpunkt.de/article.php?articleID=3238&cat01=3&cat04=8.

[13] Mario Lehmann. Die eRezept-ID - der Umgang mit Arzneimitteldaten. *www.gesundheitskunde.de*, 2004. http://www.gesundheitskunde.de/index.php?option=content&task=view&id=58.

[14] Mario Lehmann, Joachim Preißler . Persönliche Daten an vertraulichen Orten - ein Modell. *www.gesundheitskunde.de*, 2004. http://www.gesundheitskunde.de/index.php?option=content&task=view&id=52.

[15] Peter Thelen. Schlamperei-Vorwürfe bei Gesundheitskarte. *www.handelsblatt.com*, 2005. http://www.handelsblatt.com/pshb/fn/relhbi/sfn/buildhbi/cn/GoArt!200013,200050,885699/SH/0/depot/0/.

[16] protego-net.de. Feldtest der Gesundheitskarte - Konzept zur Auswahl von Testregionen. *protego-net.de*, 2004. http://www.protego-net.de/dwnld/Hinweise_zur_Auswahl_von_Testregionen_20041210.pdf.

[17] protego-net.de - DP/TS. Äußere Gestaltung der elektronischen Gesundheitskarte. *protego-net.de*, 2004. http://www.protego-net.de/dwnld/AN_20040922Aeussere_Gestaltung_eGK_V1_01.pdf.

[18] protego-net.de - FS. Lastenheft für die Spezifikation der elektronischen Gesundheitskarte. *protego-net.de*, 2004. http://www.protego-net.de/dwnld/protego_AN_20040722_Lastenheft_elektronischeGesundheitskarte.pdf.

[19] protego-net.de - MJ/RS/TS. Versichertenstammdaten/Vertragsdaten gemäß § 291 Abs. 2. *protego-net.de*, 2004. http://www.protego-net.de/dwnld/protego_Anhang_AN_20040804_Vertragsdaten_V_0_821.pdf.

[20] Thilo Weichert. Die elektronische Gesundheitskarte. *www.datenschutzzentrum.de*, 2004. http://www.datenschutzzentrum.de/medizin/gesundheitskarte/dud_gesundheitskarte.pdf.

[21] Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein. Patienten-Chipkarte, Vertrauensschutz und Datenschutz. *www.datenschutzzentrum.de*, 2002. http://www.datenschutzzentrum.de/material/themen/gesund/geschip.htm.

[22] Univ.-Lekt. Dr. Georg Lechleitner. Gesundheitsdialog. *bmgf.cms.apa.at*, 2004. http://bmgf.cms.apa.at/cms/site/attachments/4/3/9/CH0118/CMS1080651204762/lechleitner.pdf.

[23] WIKIPEDIA. WIKIPEDIA. *WIKIPEDIA*, 2005. http://de.wikipedia.org/wiki.

[24] WUV. Glossar rund um die Telematik im Gesundheitswesen. *WUV Werbe- und Vertriebsgesellschaft Deutscher Apotheker mbH*, 2000. http://www.wuv-gmbh.de/1377_1408.htm.

[25] www.abc-der-krankenkassen.de. Kritik am Gesetzesentwurf zur elektronischen Gesundheitskarte. *www.abc-der-krankenkassen.de*, 2004. http://www.abc-der-krankenkassen.de/template.php3?page=newspageinc.php3&right=rightinc.php3&usr=&id=5247.

[26] www.heute.de. Datenschützer für enge Grenzen bei Nutzung digitaler Daten. *www.heute.de*, 2005. http://www.heute.de/ZDFheute/inhalt/29/0,3672,2276061,00.html.

[27] www.holz-elektronik.de. Elektronische Gesundheitskarte: GI und VDE fordern eine erweiterte Risikoanalyse. *www.holz-elektronik.de*, 2005. http://www.holz-elektronik.de/ccic/ccicnews/050310_1.html.

[28] www.netcards-project.com. Pilot-Kartenprojekte in Europa. *www.netcards-project.com*, 2000. http://www.netcards-project.com/pilots.php#23.

[29] www.welt.de. Diverse Artikel zur Gesundheitskarte. *www.welt.de*, 2005. http://www.welt.de/extra/service/444127.html?mss=easy&user=searchintranet&ds=date&q=gesundheitskarte&search.x=0&search.y=0.

[30] www.zahn-forum.de. Patientenhoheit über die Daten muss sein. *www.zahn-forum.de*, 2004. http://www.zahn-forum.de/zf/zf.nsf/ContentByKey/GRER-63BHYP-DE-p.

[31] Zentrum für Telematik im Gesundheitswesen GmbH. ZTG. *Zentrum für Telematik im Gesundheitswesen GmbH*, 2005. http://www.ztg-nrw.de/.

4 ELSTER - die elektronische Steuererklärung

Andreas Erber, Benedikt Meuthrath

4.1 Abstract

Im Jahre 1999 führt die Bundesregierung ein Verfahren zur elektronischen Übermittlung von Steuerdaten namens ELSTER ein. Was mit der Einkommensteuer beginnt, umfasst mittlerweile ein ganzes Paket von Steuervorgängen, die mit dem System durchführbar sind. Als ein Prestigeobjekt des eGovernments wird die Entwicklung und Verbreitung stark vorangetrieben, doch es gibt einige Schwächen, die sowohl technischer als auch gesellschaftlicher Art sind.
In dieser Arbeit wird das ELSTER-System aus verschiedenen Blickrichtungen vorgestellt. Ein geschichtlicher Abriss zeigt die Entwicklung in groben Zügen, die Ziele und Möglichkeiten werden im Anschluss dargestellt. Danach wird auf die technische Architektur eingegangen.
Es folgen eine Darstellung des Sicherheitskonzeptes und die sich daraus ergebenden technischen, aber auch praktischen, d.h. beispielsweise gesetzlichen, Probleme. Mit einem Blick auf die gesellschaftlichen Aspekte ELSTERs und elektronische Steuersysteme anderer Länder werden die Betrachtungen abgeschlossen.

4.2 Einleitung - Was ist ELSTER?

4.2.1 Was ist ELSTER?

Das Akronym ELSTER steht für *EL*ektronische *ST*euer*ER*klärung. Es handelt sich dabei um ein verteiltes Softwaresystem mit dessen Hilfe Bürger[1] und Unternehmen der Bundesrepublik Deutschland steuerbezogene Vorgänge mittels des Internets durchführen, Verwaltungen und Organisationen Steuerdaten mit der Finanzverwaltung austauschen können.
Mit Hilfe des Programms *ElsterFormular* übermittelte Steuererklärungen werden bevorzugt und schnell behandelt, Steuerbescheide können damit auch elektronisch vom Finanzamt übermittelt werden. [9]

4.2.2 Zeitliche Entwicklung

(Siehe [9], [13, S. 2ff], [17] und weitere Angaben im Folgenden).

1996 - 1997 Das ELSTER-Projekt wird von der deutschen Steuerverwaltung (Bund und Länder) mit Beauftragung einer inneren Arbeitsgruppe initiiert. Unter der Leitung der Oberfinanzdirektion München wird eine Windows-basierte, modulare Client/Server-Architektur zur Datenübertragung über eine zentrale Kommunikationsstelle.
Auslieferung der ersten Clientsoftware an ausgewählte Unternehmen im Oktober 1997.

Januar 1999 öffentliche Einführung als Verfahren zur elektronischen Übermittlung der Einkommensteuererklärung.

2000 / 2001 Möglichkeiten zur Lohnsteuer-Anmeldung und Umsatzsteuer-Voranmeldung werden umgesetzt; zum 01. Januar 2001 die Umsatzsteuererklärung und weitere Steuerarten.

Anfang 2000 Dienste für Städte, Gemeinden, Landkreise, Kammern und Verbände bezüglich der Übermittlung von KFZ-Zulassungs-, Sterbe- und anderen Daten sind in das System integriert.

Anfang 2001 Bescheiddaten[2] können elektronisch abgerufen werden.
Client-Anwendung *ElsterFormular*, das zunächst nur für einige wenige Betriebssysteme[3] umgesetzt wurde[4], ist kostenlos im Internet oder bei den Finanzämtern

[1] Es wird die sprachlich männliche Geschlechtsform in diesem Text verwendet. Diese soll aber geschlechtsneutral verstanden werden.
[2] Damit ist der Steuerbescheid gemeint.
[3] Windows 95 und Windows NT werden nicht unterstützt.
[4] Für die Nutzung unter Mac OS X ist laut [17, Arbeitnehmer > Betriebssysteme] der Emulator MS Virtual PC zum Betrieb notwendig. Unter Linux soll die Emulationssoftware Wine (http://www.winehq.com) verwendet werden, lauffähig sind damit aber nur Programme mit *ElsterTeleModul*.

erhältlich.

Juli 2002 Pilotbeginn der plattformunabhängige Java-Implementierung mit der neuen Client-Komponente COALA in einigen Bundesländern.
Seit Sommer 2002 ist ELSTER mit der elektronischen Signatur erweitert, so dass eigenhändig zu unterschreibende Ausdrucke sowie Postversand an das Finanzamt nicht mehr notwendig waren.

Mitte 2003 werden die Planungen für die standardisierte Übertragung aller einzureichenden Belege begonnen.

Oktober 2003 ELSTER erhält den **TeleTrusT Innovation Prize 2003**:
"*Die Auszeichnung für die Integration der digitalen Signatur in die Elektronische Steuererklärung wurde anlässlich der Information Security Solutions Europe (ISSE) Expertenkonferenz in Wien für das ELSTER-Teilprojekt Phase 2 überreicht.*"

Anfang 2004 beginnt die bundesweite Pilotphase zur elektronischen Übermittlung von Lohnsteuerkarte und Lohnsteuerbescheinigungen. Bremen und Nordrhein-Westfalen starten Pilotversuch zum Ausdruck der Erklärungen mit einem Barcode.
Die Planungen für ein integriertes und personalisiertes Webportal, durch das Bürger alle Vorgänge mit den Finanzbehörden online abwickeln können, beginnen.

März 2004 Pilotbeginn der Online-Steuerkontoabfrage in Hessen

Januar 2005 Die elektronische Übermittlung von Umsatzsteuer-Voranmeldungen ist gesetzlich verpflichtend. [1, S. 13]

April: 2005 NRW-Finanzministerium stellt klar, dass die Papierform der Umsatzsteuer-Voranmeldung die vorgegebene Anmeldung ist

4.2.3 Ziele

Grundgedanke: "*Neben den Steuerberatern erstellen immer mehr Bürger ihre Steuererklärungen am Computer. Bei dieser Gelegenheit werden die Daten für den Ausdruck der Steuererklärungsformulare elektronisch erfasst. Diese bereits erfassten elektronischen Daten will die Steuerverwaltung zur Weiterverarbeitung in den Rechenzentren der einzelnen Bundesländer nutzen.*" [17, Projekt]
In Anbetracht der allerorts in den öffentlichen Verwaltungen angestrebten Kostenersparnis, soll die Verminderung des Aufwands der Datenerfassung erreicht werden. Das Drucken von Formularen, Klebeheftung der Mantelbögen, Postversand entfällt ganz oder teilweise. [17, Projekt], [6]
Die Eingaben der Benutzer werden schon im Client-Anwendung einer Plausibilitätsprüfung unterzogen [13, S. 8] und werden bei sachlicher Richtigkeit behördenseitig übernommen. Durch die Automatisierung zahlreicher Abläufe wird die Bearbeitungsdauer erheblich reduziert. Bürger, Unternehmen und Steuerberater haben stets Einblick in ihre

eigenen Steuervorgänge, können also etwaige Abweichungen seitens der Behörden einsehen. [17, Projekt] Dies soll zukünftig mit Hilfe eines umfassenden, kompletten und personalisierten Steuerportals im Internet realisiert werden und ortsunabhängig von jedem Anwender nutzbar sein. Die papierlose Kommunikation soll in absehbarer Zeit möglich, später sogar verpflichtend sein. [13, S. 11, 13]
Die Umsetzung dieser Ziele ist in einigen Bereichen schon zu großen Teilen erreicht (siehe folgenden Abschnitt 4.2.4), allerdings sind wesentliche Bestandteile noch in Arbeit. Die Unterstützung eines einzelnen Betriebssystems ist in dieser Hinsicht ein eklatanter Mangel, ebenso das immer noch nicht fertiggestellte ElsterOnline, was diese Nachteil aus Sicht des Bürgers aufwiegen könnte.

4.2.4 Möglichkeiten/Fähigkeiten

Derzeit (Stand Ende Mai 2005) sind folgende Vorgänge mittels der Software ausführbar[16]:

- Einkommensteuererklärung (seit 1999)
- Umsatzsteuererklärung (seit 2001)
- Gewerbesteuererklärung (seit 2001)
- Umsatzsteuer-Voranmeldung (seit Mitte 2000, gesetzlich verpflichtend für Unternehmen und Arbeitgeber seit 01.01.2005)
- Lohnsteuer-Anmeldung (seit Mitte 2000, gesetzlich verpflichtend für Unternehmen und Arbeitgeber seit 01.01.2005)
- Lohnsteuerbescheinigungsdaten (seit Mitte 2000, gesetzlich verpflichtend für Unternehmen mit maschineller Lohnabrechnung seit 28.02.2005)
- Bescheiddatenbereitstellung (seit 2001)
- Steuerkontoabfragen (in Hessen seit März 2004 verfügbar)
- zahlreiche Datenübermittlungen zwischen Finanzverwaltung und Städten, Kommunen, Landkreisen, Kammern und Verbänden (z. B. Übermittlung von KFZ-Zulassungsdaten von den Kommunen an die Steuerbehörden, Abruf der beitrags- und gebührenrelevanten Daten durch Industrie- und Handels- (IHK) sowie Handwerkskammern (HWK), u.v.a.)
- verbesserte Steuerbetrugsbekämpfung

4.3 Architektur

Komponenten [13, S. 8f]

- ElsterFormular (Client)

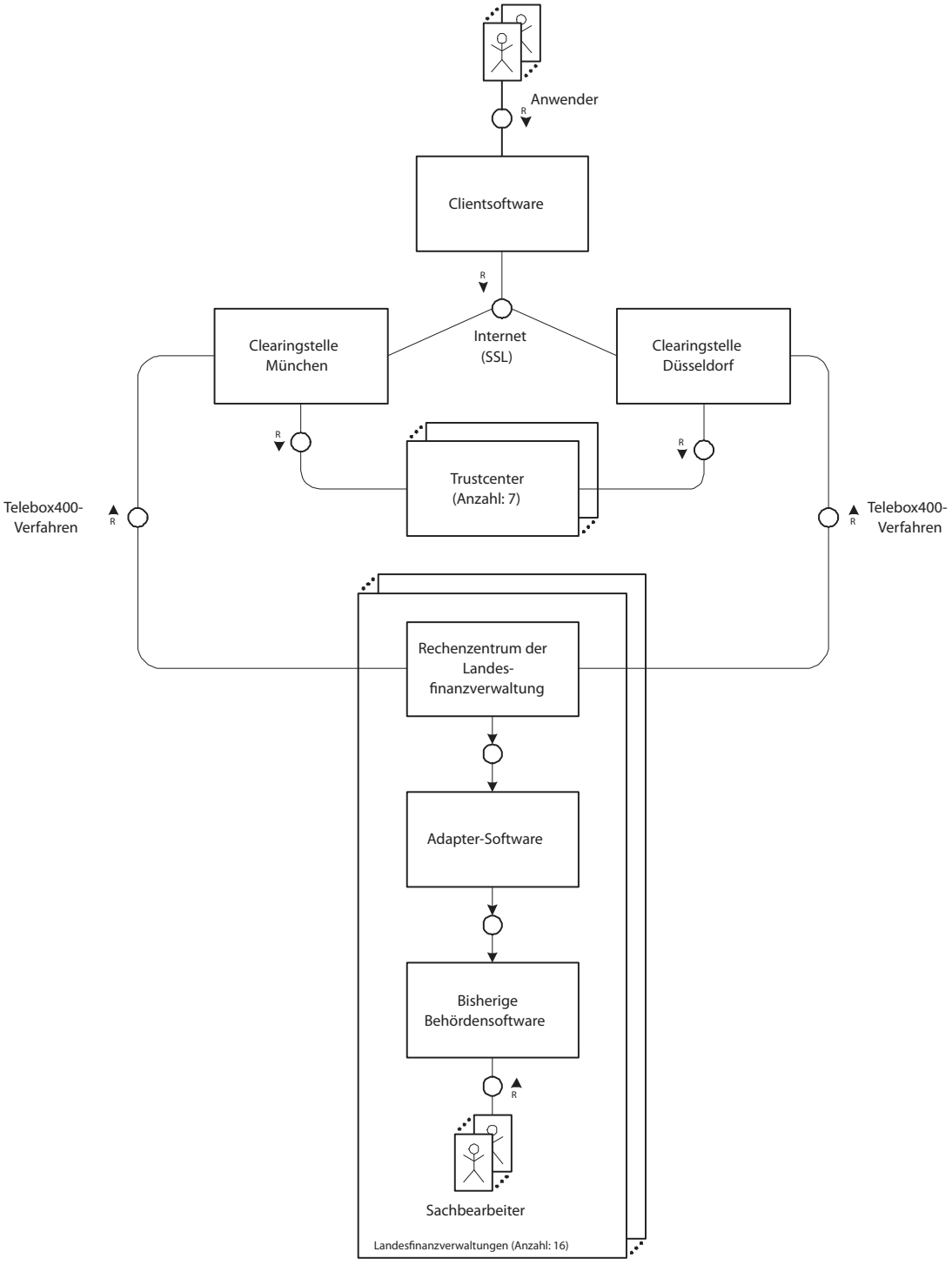


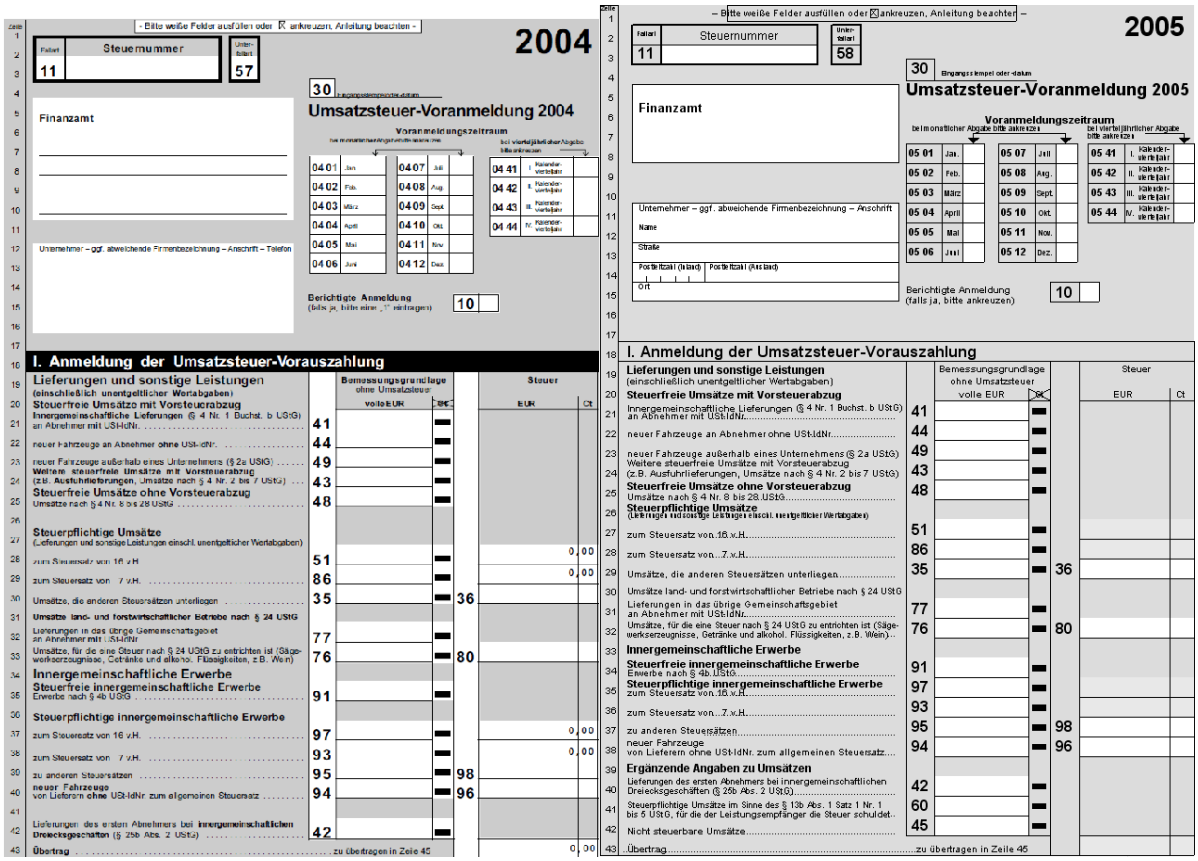
Abbildung 4.1: Aufbau des Systems (in FMC dargestellt)

- ElsterFT (ElsterFileTransfer)
- ElsterLohn (ElsterLohn I, ElsterLohn II)
- ElsterSignatur, ElsterOnlineManager (EOM) - Digitale Signatur [17, Projekt > Signatur]
- ElsterOnline
- ElsterSuch

Der Aufbau des ELSTER-Systems für das bekannteste Beispiel – die Funktionen, die mittels *ElsterFormular* ermöglicht werden – ist in Abbildung 4.1 schematisch[5] dargestellt. Basis ist eine Client/Server-Architektur von den so genannten *Clearingstellen* (Server) aus gesehen sowohl in Richtung Nutzer (Client - Bürger/Unternehmen) als auch in Richtung Rechenzentren der Finanzverwaltung (Client). Der Nutzer gibt die benötigten Daten in die *Clientsoftware* ein und sendet sie aktiv[6] an eine der beiden Clearingstellen. Die Daten werden von der Clientsoftware per SSL[7] verschlüsselt. Das SSL-Verfahren sieht eine hybride Technik bei der Verschlüsselung vor, die in Kapitel 4.4 kurz erläutert wird. Die Clearingstelle überprüft die Signatur, mit der die Daten digital unterschrieben wurden, mittels der *Trust Center*, sofern der Nutzer die Daten signiert hat. Dies ist nicht zwingend vom System vorgesehen bzw. die technischen Möglichkeiten dazu sind derzeit nicht gegeben. Die Daten des Nutzers werden, bis auf benötigte Metadaten wie z.B. Name und Steuernummer, in den Clearingstellen weder entschlüsselt noch gelesen. Die einzelnen *Rechenzentren* der *Landesfinanzverwaltungen* holen sich daraufhin aktiv die verschlüsselten Daten von den Servern der jeweiligen Clearingstelle, entschlüsseln sie und bereiten sie mittels einer *Adaptersoftware* so auf, dass sie von der in der jeweiligen Länderfinanzbehörde bisher verwendeten Softwarelandschaft genutzt werden kann. Dem Sachbearbeiter stehen die Daten also in der bisher gewohnten Umgebung zur Verfügung. [13, 10], [17, Projekt > Technisches]
Ein eklatanter Mangel dabei ist, dass die Clientanwendung ElsterFormular nur für ein einziges Betriebssystem zur Verfügung steht und Schnittstellen nur bedingt und zeitlich sehr spät offengelegt wurden, sodaß eine Entwicklung alternativer Software unnötig erschwert wurde.
Dem Anwender stehen unterschiedliche Möglichkeiten zur Verfügung seine Daten an die Clearingstelle zu senden. Für den Bürger gibt es dabei sowohl das von den Behörden entwickelte (bzw. in Auftrag gegebene) *ElsterFormular*, als auch zahlreiche Steuerprogramme, welche die angebotenen Schnittstellen *ElsterTeleModul*[8] oder COALA

[5] nach den Fundamental Modeling Concepts (FMC) - für weitere Information sei die offizielle Website unter http://www.f-m-c.org/ empfohlen.
[6] *Aktiv* meint in diesem Zusammenhang, dass die Clientsoftware den Kontakt zu den Servern der Clearingstelle herstellt - nicht andersherum. Die Clearingstellen versenden also ungefragt keine Daten.
[7] Secure Socket Layer
[8] eine C-Bibliothek, die benötigte Funktionen zur Prüfung und dem Versand der Daten etc. zur Verfügung stellt

[9]verwenden. *ElsterFormular* ist dem klassischen Papierformular nachempfunden und es kann Einkommen-, Umsatz- und Gewerbesteuererklärungen, sowie Umsatzsteuer-Voranmeldungen sowie Lohnsteuer-Anmeldungen übermitteln. Dabei unterstützt das Programm den Anwender beim Ausfüllen durch integrierte Anleitungen und Prüfung der Eingaben auf logische Stimmigkeit vor der Übertragung. Die Abgabe von Umsatzsteuer-Voranmeldungen und Lohnsteuer-Anmeldung ist gesetzlich seit dem 01.01.2005 vorgeschrieben, allerdings gibt es mittlerweile in 4.5.1 beschriebene anders lautende Gerichtsurteile.



(a) Papier Formular (b) ElsterFormular

Abbildung 4.2: Vergleich der Umsatzsteuervoranmeldung auf Papier und in ElsterFormular

ElsterFT ist eine Client-Anwendung, die den Datenaustausch mittels Disketten, Magnetbändern oder Papierformularen zwischen externen Partnern und der Finanzverwaltung ablösen soll. Dabei soll diese Anwendung auch auf andere Bereich z.B. KFZ-Zulassungsdaten, Gewerbe- und Grundsteuermessbeträge etc. erweitert werden. Als externe Partner sind "Städte, Gemeinden, Universitäten, Landschaftsverbände etc." [13, S. 8] anvisiert.[17, ElsterFT]

[9]eine Java-Bibliothek

ElsterLohn unterteilt sich in die zwei Pilotprojekte *ElsterLohn I* und *ElsterLohn II*. Beide befassen sich mit der Lohnsteuerkarte und sollen dieses analoge Medium schrittweise ersetzen. *ElsterLohn I* ist eine Schnittstelle, ähnlich *ElsterTeleModul*, die von Softwareanbietern bzw. Arbeitgebern in vorhandene Buchhaltungssoftware integriert werden kann. Diese Schnittstelle soll es ermöglichen, die auf der Rückseite der Lohnsteuerkarte befindlichen und vom Arbeitgeber auszufüllenden Lohnsteuerbescheinigungsdaten über das Internet an die Finanzbehörden zu senden. Dieses elektronische Verfahren soll den technischen und organisatorischen Aufwand, der bisher von den Arbeitgebern für die Erstellung und Übermittlung der notwendigen Daten aufbringen mussten, verringern und ist seit dem 28.02.2005 für Unternehmen mit maschineller Lohnabrechnung verpflichtend [3]. *ElsterLohn II* soll langfristig die bisherige Lohnsteuerkarte komplett durch ein elektronisches Datenhaltungssystem ersetzen. [17, Arbeitgeber]
ElsterSignatur ist ein zentrales Modul aller ELSTER-Projekte, welches genutzt werden soll, um zu übermittelnde Daten vom Anwender digital zu signieren, und welches die Nutzung alle rechtlich anerkannten Signaturkarten erlauben soll. Dies umfasst sowohl staatliche Signaturkarten (etwa die Jobcard) als auch von Banken herausgegebene Karten mit Signaturmodul. Die Entwicklung der zur Nutzung von *ElsterSignatur* nötige Software - *ElsterOnlineManager (EOM)* - wurde eingestellt und die Softwarepflege wird nicht mehr fortgeführt. Eine neue Software wird derzeit entwickelt und soll ab 2006 Anwendung finden[17, Projekt > Signatur].
ElsterOnline umfasst alle Leistungen, die Online via Webseiten, angeboten werden und damit vom Anwender per Browser genutzt werden können. Derzeit ist damit die Abfrage des Steuerkontos möglich, eingeschränkt auf Finanzämter in Hessen, die den Pilotversuch durchführen. Geplant sind Umsatzsteuer-Voranmeldungen und Lohnsteuer-Anmeldungen ab dem 01.01.2006. [17, ElsterOnline]
Eine weitere Anwendung ist *ElsterSuch*, welche für die Finanzverwaltung ein Werkzeug darstellt, um eine bundesweite Onlinefahndung nach Umsatzsteuerbetrug durchzuführen.

4.4 Sicherheitskonzept

4.4.1 Eingesetzte Sicherheitsmechanismen

Das wichtigste Sicherheitskonzept bei ELSTER ist die Verschlüsselung der Daten. Dies stellt sicher, dass nur die zuständige Steuerbehörde die Daten entschlüsseln und lesen kann. Das verwendete Verfahren ist an SSL angelehnt, allerdings ist im Fall von ELSTER die Schlüsselverteilung interessant.
Es wird ein hybrides Verschlüsselungsverfahren eingesetzt, welches sich den Geschwindigkeitsvorteil der symmetrischen Verschlüsselung[10] zu Nutze macht und andererseits für den dazu nötigen Schlüsselaustausch kein sicheres Medium, wie Diskette, CD-ROM o.ä.

[10] symmetrisch heißt, dass beide Seiten den gleichen Schlüssel benötigen, um ver- und entschlüsseln zu können

auf dem Postweg o.d. benötigt. Hierzu wird ein asymmetrisches Verschlüsselungsverfahren[11] dergestalt verwandt, dass der für jede Sitzung neu erstellte symmetrische Schlüssel mit dem öffentlichen Schlüssel des Empfängers chiffriert und an die symmetrisch chiffrierte Nachricht angehängt wird. Nur ein Empfänger mit dem passenden privaten Schlüssel kann den einmalig gültigen symmetrischen Schlüssel und damit die eigentliche Nachricht dechiffrieren.
ELSTER verwendet konkret für die symmetrische Verschlüsselung der Daten 3-DES mit 112 Bit Schlüssellänge und für die asymmetrische Verschlüsselung des Schlüsselaustauschs RSA mit 2048 Bit Schlüssellänge. Um sicherzustellen, dass nur die zuständige Finanzbehörde die Daten entschlüsseln kann, existiert für jedes Bundesland ein eigenes RSA-Schlüsselpaar. Diese Schlüsselpaare werden von einer von der Oberfinanzdirektion München bereitgestellten Software dezentral in den einzelnen Ländern erzeugt und besitzen eine Gültigkeitsdauer von einem Jahr. Das ELSTER-Modul, welches für die Verschlüsselung zuständig ist, ermittelt anhand der vom Nutzer eingegebenen Daten die entsprechende Länderfinanzbehörde und wählt den entsprechenden öffentlichen RSA-Schlüssel aus.
Um eine Manipulation an der Nachricht zu verhindern wird ein so genannter *Message Authentication Code* (MAC) an die Nachricht angehängt. Ein MAC ist eine Prüfsumme, anhand deren die Integrität der Nachricht überprüft werden kann. Normalerweise wird eine Hashfunktion[12] für die Berechnung eines solchen MAC verwendet. An die eigentliche Nachricht wird ein geheimes Stück Nachricht, das nur dem Sender und dem Empfänger bekannt ist, z. B. der einmalig verwendete symmetrische Schlüssel, angehängt. Von der gesamten Nachricht, inklusive Geheimnis, wird die Prüfsumme berechnet. Der verwendete Algorithmus stellt sicher, dass von dieser Prüfsumme nicht auf die Nachricht geschlossen werden kann. Manipuliert ein Angreifer die Nachricht, so ändert sich die Prüfsumme und der Empfänger kann anhand des übermittelten MAC und der zum Vergleich auf der übertragenen Nachricht berechneten Prüfsumme die Manipulation entdecken. Eine korrekte Neuberechnung des MAC ist nur möglich, wenn das geheime Stück Nachricht bekannt ist. Somit ist auch sichergestellt, dass ein Angreifer nicht Nachricht und Prüfsumme manipulieren kann. [17, Projekt > Sicherheit], [15], [20]
Eine weitere Sicherheitsmaßnahme ist die Bereitstellung eines Bytecode-Checkers, der auf den Internetseiten des ELSTER-Projektes angeboten wird. Dieser Bytecode-Checker kann das installierte *ElsterFormular* auf Unversehrtheit überprüfen und gibt im Falle einer Manipulation am Programm eine Warnung aus. [17, Projekt > Sicherheit]
Unbefugter Zugriff auf die von ELSTER verwendeten Server wird durch Firewalls abgewehrt. [17, Projekt > Sicherheit]
Die gesamte Infrastruktur von ELSTER wurde durch die TÜV Informationstechnik GmbH überprüft. (*Trusted Site* Siegel 2001 und 2002) [17, Projekt > Sicherheit]

[11] asymmetrisch heißt, dass es ein Schlüsselpaar gibt. Mit dem einen, öffentlichen Schlüssel wird verschlüsselt, mit dem anderen, privaten wird entschlüsselt
[12] z.B. MD-5

4.4.2 Technische Schwachstellen

In der Benutzerauthentisierung besteht derzeit die gravierendste Schwachstelle des Systems. Seit dem 01. Januar 2005 sind sämtliche Unternehmen verpflichtet ihre monatliche Umsatzsteuer-Voranmeldung elektronisch an das Finanzamt zu übermitteln (§ 18 Abs. 1 Satz 1 Umsatzsteuergesetz (UStG) bzw. § 41 a Abs. 1 Einkommensteuergesetz (EStG)). Dabei besteht das Problem, dass die Unternehmen nicht adäquat authentifiziert werden, da ein sicheres Verfahren bisher nicht implementiert wurde. Das ELSTER-Projekt verzichtete bisher auf die Verwendung der qualifizierten elektronischen Signatur, die gemäß § 87a Abs. 3 Satz 2 Abgabenordnung (AO) eine sichere Authentifikation darstellt, aufgrund deren geringer Verbreitung. [21, S. 114]
Die Umsatzsteuernummer, die ein Unternehmen verpflichtend auf Rechnungen nach § 14 Abs. 4 UStG angeben muss [21, S. 114], und Name der Firma reichen aus, um eine Voranmeldung abzugeben. [18] Da viele Unternehmen ihrem Finanzamt eine Einzugsermächtigung für den daraus resultierenden Vorabzug erteilt haben, werden die angemeldeten Beträge in kurzer Zeit abgebucht. Unternehmen mit geringem Kapital können also leicht Opfer überhöhter Fehlangaben und dadurch in den Ruin getrieben werden.
Die Tragweite dieser Sicherheitslücke wird durch die derzeit immer noch gültige Gesetzeslage verstärkt. Da nur in Ausnahmefällen, beim Vorliegen unbilliger Härten, die Einreichung der Voranmeldung in Papierform durch das jeweilige Finanzamt gestattet wird, stehen Unternehmen in einem Dilemma. Die Klage gegen die elektronische Übermittlung eines Hamburger Rechtsanwalts auf der Basis, er habe keinen Internetanschluss, ging durch die Presse (siehe [23], [24, Abs. 4]). Eine Entscheidung gegen die elektronische Übermittlung gibt es bereits in Nordrhein-Westfalen. So hat das NRW-Finanzministerium klargestellt, dass Umsatzsteuer-Voranmeldungen auch künftig (seit April 2005) in Papierform abgegeben werden dürfen. Außerdem "seien die Referatsleiter Abgabenordnung der obersten Finanzbehörden der Länder mehrheitlich der Auffassung, dass der maßgebliche §150 Absatz 1 AO die Papier-Anmeldung als vorgeschriebene Anmeldung meint."[13]
Das *Virtuelle Datenschutzbüro - Ein gemeinsamer Service ihrer Datenschutzinstitutionen* unter http://www.datenschutz.de stellt auf seiner Presseseite eine Presseerklärung der Deutschen Vereinigung für Datenschutz e.V. (DVD) bereit. [22] Darin weist die DVD auf einen Musterbrief für den Antrag auf Weiterführung der papiergestützten Erklärung hin. Nach Ansicht der DVD liege die Entscheidung unbilliger Härtefälle – und damit das Recht auf Sicherheit – im Ermessen der jeweiligen Finanzbeamten, was zu willkürlichen und ungleichen Behandlungen führen werde.
Eine weitere Schwachstelle stellt eine vom Benutzer unbemerkte Manipulation der verwendeten Software dar. So kann man nicht davon ausgehen, dass der vom Benutzer verwendete Rechner eine sichere Umgebung darstellt. Über den verwendeten Internetzugang können Schadprogramme auf den Rechner gelangen und Manipulationen an der ELSTER-Software vornehmen. Beispielsweise könnten die vorhandenen öffentlichen

[13] Diese Information stammt laut einem Leserbrief der c't Ausgabe 11/05 aus einem Erlass des Finanzministeriums Nordrhein-Westfalen vom 07.04.05 Aktenzeichen S 0061-65-V1, was aber aufgrund der kostenpflichtigen Recherche der Erlasse an dieser Stelle nicht nachgeprüft werden kann.

Schlüssel der Länderfinanzbehörden gegen eigene Schlüssel ausgetauscht und die Software so manipuliert werden, dass die Daten an einen Server unter eigener Kontrolle geschickt werden. Damit wäre es möglich die Daten zu entschlüsseln, zu manipulieren, mit den richtigen Schlüsseln zu chiffrieren und die Daten an die Clearingstelle weiterzuleiten. Eine klassische *Man-In-The-Middle*-Attacke. Der Bytecode-Checker hilft dagegen nur, wenn der Anwender ihn regelmäßig vor jeder Übertragung verwendet.
Möglich wäre auch eine *Distributed-Denial-of-Service*-Attacke auf die Server der Clearingstellen. Wenn genügend Rechner für die Attacke zur Verfügung stehen, wäre es möglich die Server für Tage durch wahllose Anfragen arbeitsunfähig zu machen, so dass niemand seine Steuerdaten an die Server senden kann. Wählt man dafür einen entsprechenden Zeitpunkt (etwa, wenn die Server aufgrund der eintreffenden Umsatzsteuer-Voranmeldungen jeden Monat belastet sind) so ließe sich das System treffend stören. Die regulären Nutzer würden irgendwann genervt aufgeben und sich bei den entsprechenden Stellen beschweren. Das Vertrauen der Nutzer wäre nachhaltig gestört und die Akzeptanz des Systems würde sinken.

4.5 Gesellschaftliche Aspekte

4.5.1 Rechtliche Grundlagen

Eine Steuererklärung gilt rechtlich gesehen als eine Willenserklärung, die von einer natürlichen oder juristischen Person (Privatrechtssubjekte) gegenüber den Steuerbehörden abgegeben wird, um den Steuerbehörden die Ermittlung der Besteuerungsgrundlage und die Festlegung der Steuer zu ermöglichen. Juristisch ausgedrückt ist eine Willenserklärung die Äußerung eines Willens einer Person, die einen so genannten Rechtserfolg beabsichtigt. Dabei definiert das Bürgerliche Gesetzbuch (BGB) den Begriff der Willensäußerung nicht näher, sondern setzt ihn voraus. Privatrechtssubjekte können durch die Abgabe von Willenserklärungen Rechtsgeschäfte vornehmen. Das wichtigste Beispiel für ein Rechtsgeschäft ist der Vertrag. Die Tatsache, dass das BGB verschiedene Formen einer Willenserklärung kennt und speziell auch die elektronische Form[14], ist an dieser Stelle von Interesse. So sieht das BGB vor, dass, wenn die normalerweise gesetzlich vorgeschriebene schriftliche Form durch eine elektronische Form ersetzt werden soll, der Aussteller der Erklärung, im Fall von ELSTER also die Person, die eine Steuererklärung abgeben möchte, seinen Namen hinzufügen und das elektronische Dokument mit einer "qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen" muss.[15]
Das Signaturgesetz soll die nötigen rechtlichen Rahmenbedingungen für elektronische Signaturen schaffen mit dem Ziel der erhöhten Rechtssicherheit im elektronischen Geschäftsverkehr. Es definiert aus diesem Grund Mindestinhalte, die eine Signatur haben muss, um als qualifiziert zu gelten und Vorschriften für Aussteller von Zertifikaten die Sicherheit des Ausstellungsverfahrens und der dazu eingesetzten Mittel betreffend.

[14] §126a Bürgerliches Gesetzbuch (BGB)
[15] §126a, Absatz 1, Bürgerliches Gesetzbuch (BGB)

Da aufgrund der niedrigen Verbreitung solcher Signaturen ELSTER nicht in dem Maße genutzt werden könnte, wie es das Gesetz seit dem 01.01.2005[16] bzw. 28.02.2005[17] vorsieht, wollten die Finanzverwaltungen eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung (StDÜV) vom 28.1.2003 nutzen, und bis Ende 2005 lediglich eine so genannte "qualifizierte elektronische Signatur mit Einschränkungen" vorschreiben. Die Beauftragten der Länder und des Bundes für Datenschutz und Informationsfreiheit lehnten dieses Vorgehen ab, da Dokumente, die solche Signaturen verwenden, unerkannt manipulierbar sind[18] und diese Signaturen damit eine geringeren Beweiswert als eine eigenhändige Unterschrift haben. Außerdem befürchteten die Datenschutzbeauftragten, dass bei Schaffung weiterer Signaturverfahren[19] mit geringerer Sicherheit die Transparenz für die Nutzer verloren geht und damit der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte, was der eigentlich beabsichtigten Rechtssicherheit zuwider läuft.[2]
Daher wurde das derzeit gültige Verfahren entwickelt, nachdem die elektronischen Daten ohne qualifizierte elektronische Signatur verschlüsselt an die Finanzbehörden übermittelt werden können, der Nutzer allerdings danach eine verkürzte (komprimierte) Steuererklärung ausdrucken und unterschreiben muss. Diese Steuererklärung enthält die einmalige Transaktionsnummer (TAN), unter der die Daten übermittelt wurden, und muss gegebenenfalls mit weiteren Belegen in der bisherigen analogen Form bei den Finanzbehörden eingereicht werden. Bei Umsatzsteuer-Voranmeldungen und Lohnsteuer-Anmeldungen ist das Verfahren komplett elektronisch, ebenfalls ohne Signatur, allerdings muss der Datenlieferer[20] vorher seine Teilnahme an dem Verfahren erklären[21] und von der Steuerverwaltung zur Datenübermittlung zugelassen sein. Hier stellt sich die Frage der Authentizität der Daten, die in 4.4.2 diskutiert wird.

4.5.2 Bekanntmachung des Systems

Als eines der Vorzeigeprojekte des Bundes in Sachen *EGovernment* wurde die Öffentlichkeit intensiv mit Informationsmaterial versorgt. Eine ganze Reihe von Websites (z. B. `http://www.elster.de`, `http://www.elsterformular.de`, `http://www.elsterft.de`, `http://www.elsterlohn.de`) enthalten jede Menge Information zum Thema, die aber insgesamt recht oberflächlich bleibt. Technische Angaben zur Software und der Infrastruktur sind kaum zu finden, sog. *White Papers* mit Spezifikationen und Schnittstellendefinitionen sind nicht frei zugänglich, was sicherlich auch daran liegt, dass die Quellen nicht offen sind.[22]

[16] Umsatzsteuer-Voranmeldung
[17] Lohnsteuerbescheinigung
[18] bei qualifizierten Signaturen ist anhand der darin enthaltenen Prüfsummen eine nachträgliche Manipulation an dem signierten Dokument leicht festzustellen
[19] neben denen, die im Signaturgesetz vorgesehen sind
[20] in diesem Fall Steuerberater, Unternehmer oder Arbeitgeber
[21] in analoger schriftlicher Form
[22] vgl. auch [7]

4.5.3 Annahme durch die Bevölkerung

Der Bundestag, sowie das Projekt selbst veröffentlichen immer wieder Presseerklärungen, die Zahlen über die Verwendung von ELSTER enthalten. So wurden innerhalb der ersten vier Monate 2004 insgesamt etwa 800.000 Steuererklärungen elektronisch eingereicht, [5] insgesamt nutzten 2004 1,8 Millionen Bundesbürger ELSTER [4]. Einen detaillierteren Überblick gibt Tabelle 4.1.

Datenüberm.	1999	2000	2001	2002	2003	2004	04.2005
Einkommenst.	27.000	140.000	320.000	550.000	1.100.000	1.810.000	1.500.000
Voranm.pfl. Untern.[23]	2.886.268	2.909.150	2.920.983	2.926.570	2.915.482		
Ust.-Voranm.		260.000	2.450.000	3.100.000	4.370.000	5.680.000	6.120.000
Lst.anm.		310.000	3.160.000	4.030.000	5.700.000	6.530.000	4.450.000
Lst.besch.						6.250.000	36.800.000

Tabelle 4.1: Entwicklung der Nutzung [9]

4.5.4 Andere Staaten

In den Staaten der OECD sind elektronische Steuersysteme bereits recht weit verbreitet. In einer Umfrage des *Forum on Tax Administration*[24] stellte sich heraus, dass die Einführung oftmals mit staatlichen Anreizen unterstützt wurde. Einher damit gingen eine kundenfreundlichere Ausrichtung der Finanzbehörden. Beispielsweise sind Telefon-Hotlines und umfangreiche Internet-Informationsangebote heute im Prinzip Standard. [14, Kap. 5.2] Einige Staaten seien als Beispiele herausgegriffen (ohne Wertung):

Australien Im Durchschnitt von 2002/2003 wurden 34,6% der Steuererklärungen elektronisch eingereicht. [14, Kap. 4.2]

Dänemark: Ein elektronisches System wurde erst 2004 eingeführt, Arbeitsentlastungen bei den Finanzbehörden sind bereits spürbar. [14, Kap. 4.3]

Mexiko: Es existiert ein großes, an das australische angelehnte System nicht nur mit elektronischer Signatur sondern auch Zahlungsmöglichkeit. Unselbstständig Erwerbende (bei Einkommen $>$ \$150.000) und Unternehmen sind gesetzlich zur elektronischen Abgabe verpflichtet. Künftig sollen auch biometrische Daten zur Authentifikation herangezogen werden. [14, Kap. 4.4]

Österreich: Seit Mai 2004 ist die elektronische Einreichung der Steuererklärung von Bürgern und Unternehmen mittels des Systems *Finanzonline* möglich. Bürger mit

[24] *Survey of Trends in the Delivery of Services to Taxpayers Using New Technologies [14, 19]*

einem Einkommen jenseits von 100.000 Euro und Unternehmen sind zur elektronischen Abgabe gesetzlich verpflichtet. [14, Kap. 4.7]

Finnland Die Software *eFinTax* verwendet keine digitale Signatur sondern eine mit Hilfe von Banken entwickelte UserID, die auch bei Bankgeschäften zum Einsatz kommt. Elektronische Einreichung steht nur Unternehmen zur Verfügung. [14, Kap. 4.8]

Island Auch hier kommt eine UserID zum Einsatz. Durch staatliche Anreize wurde eine Quote elektronischer Einreichungen von 70% erreicht. [14, Kap. 4.9]

4.6 Fazit

ELSTER ist ein Vorzeigeprojekt des EGovernments der Bundesregierung. Deren Interesse, schnell Erfolge vorzuweisen durch Bereitstellung von Online-Serviceleistungen, führte von 1996 bis 1999 zur raschen Entwicklung und Veröffentlichung einer proprietären Clientsoftware für den Steuerbürger. Dies wurde entsprechend durch Werbung (Pressemitteilungen, Webseiten, Broschüren etc.) der Bundesregierung unterstützt. Erst danach wurde die Software – neben der Vergrößerung der Angebote für Steuerbürger und Unternehmen – einerseits für den innerbehördlichen Betrieb erweitert, andererseits auf eine plattformunabhängige Implementationsform umgestellt.
Als interessant an den offiziellen Veröffentlichungen des Bundes ist zu bemerken, dass die bereitgestellte Information verwirrend erscheint. Es wird in visionärem Ton mit zahlreichen Fachbegriffen aus der Informationstechnologie formuliert, doch klare Strukturen werden vermisst. Mehr oder weniger unbedeutende Information finden sich an zahlreichen Stellen, wichtige Angaben widersprechen sich von der einen zur nächsten Quelle.[25]
Der politische Erfolg des Projektes genießt oberste Priorität. Umso erstaunlicher immerhin die Tatsache, dass sich auf der offiziellen ELSTER-Internetseite tatsächlich ein Verweis auf eine kritische Pressemitteilung (siehe [18]) des Branchenverbandes BITKOM befindet – allerdings mit dem deutlichen Hinweis, dass dieser korrigiert wurde und in seiner ursprünglichen Version "*offenbar zu einigen Fehlinterpretationen Anlass gegeben*" hat. [17, die neuesten Infos]
Der Bereich "die neuesten Infos" der ELSTER-Webseite belegt mit seinen in fast regelmäßigen Abständen erscheinenden, rundweg positiven Pressemitteilungen die Notwendigkeit zur kritischen Hinterfragung. Ob in fünfeinhalb Jahren der Nutzbarkeit der elektronischen Steuererklärung eine Angabe von fünf Millionen eingereichten Einkommensteuererklärungen als Erfolg zu bewerten sind, ist sehr fraglich. Otto-Normal-Verbraucher mag die Sicherheitsbedenken, wie sie seitens der Webseite heruntergespielt werden, als geringfügig abtun, doch bei den Fachleuten innerhalb der IT-Branche und im Datenschutz schrillen mit Recht die Alarmglocken.
So schreibt der Bundesbeauftragte für den Datenschutz, Peter Schaar, in [21, Kap. 8.6, S. 114]: "*Seit dem 1. Januar 2005 dürfen Steueranmeldungen gem. § 18 Abs. 1 UStG*

[25] Vergleiche Angaben zu Schlüssellängen auf den Webseiten des ELSTER-Projektes [17, Projekt > Sicherheit] vs. [17, ElsterFormular > Sicherheitsmechanismen]

sowie § 41a EStG grundsätzlich nur noch auf elektronischem Wege nach Maßgabe der Steuerdatenübermittlungsverordnung (StDÜV) an das Finanzamt übermittelt werden. Eine sichere Authentifizierung wäre gem. § 87a Abs. 3 Satz 2 AO durch den Einsatz einer qualifizierten elektronischen Signatur zu gewährleisten. Jedoch wurde hierauf wegen der geringen Verbreitung der digitalen Signatur verzichtet." Es habe Verzögerungen bei der Implementierung alternativer Authentifizierungsverfahren gegen, so dass "*[i]n der Zwischenzeit [...] allerdings Manipulationen möglich [sind]. Unberechtigte Dritte können fingierte Umsatzsteuer-Voranmeldungen unter Nutzung der Steuernummer, die auf Rechnungen gemäß § 14 Abs. 4 Umsatzsteuergesetz ausgewiesen sein muss (vgl. Nr. 29, dort Nr. 3), übermitteln.*"
Man muss sich nicht wirklich in Betriebswirtschaft auskennen, um eventuelle wirtschaftliche Folgen solcher Manipulationen für v.a. kleine und mittlere Unternehmen hinsichtlich der zu leistenden Umsatzsteuer-Vorauszahlungen einzuschätzen zu können.
Auch die Benachteiligung von alternativen Betriebssystemen, die mittlerweile gerade im Wirtschaftsbereich eine große Verbreitung gefunden haben (aber auch in Behörden eine immer größere Rolle spielen), gegenüber Microsoft Windows durch exklusive Bereitstellung eines Clientprogramms, ist ein Unding. Zwar steht mit COALA eine plattformunabhängige Schnittstelle zur Verfügung, allerdings kann der Endanwender diese meist nicht kostenlos nutzen, da die Hersteller für ihre Finanzsoftware, welche die COALA-Schnittstelle nutzen, ein Entgelt verlangen. So beschwert sich ganz aktuell der Linux-Verband auf dem diesjährigen LinuxTag über diesen Umstand[26]. Dieses Problem soll ab 2006 durch ElsterOnline gelöst werden. Warum nicht von vornherein eine plattformunabhängige Lösung entworfen wurde ist rätselhaft, denn die nötigen Konzepte und Referenzen gibt es ungefähr seit Anfang der 90er Jahre des vergangenen Jahrhunderts.
Zusammenfassend lässt sich sagen, dass die Pläne ambitioniert sind, die Umsetzung derzeit allerdings zu wünschen übrig lässt. Eventuell hätten sich einige Probleme, gerade im sicherheitstechnischen Bereich, vermeiden lassen, wenn durch eine quelloffene Entwicklung externen Experten, außerhalb der Finanzdirektion München, die Möglichkeit gegeben worden wäre, an dem Entwurf und der Entwicklung zu partizipieren. Dies hätte mit einiger Sicherheit frühzeitig die Schwachstelle der Benutzerauthentifizierung aufgedeckt und das Design hätte entsprechend korrigiert werden können. Der Grundsatz "Security by Obscurity", der von jedem Kryptographen als Negativ-Beispiel angeführt wird, scheint hier der Leitgedanke zu sein.

[26] siehe http://www.heise.de/newsticker/meldung/61014 und http://www.linux-community.de/Neues/story?storyid=16242

Literaturverzeichnis

[1] Deutscher Bundestag. Entwurf eines Zweiten Gesetzes zur Änderung steuerlicher Vorschriften (Steueränderungsgesetz 2003 - StÄndG 2003). Bundestagsdrucksache 15/1798, Oktober 2003. http://dip.bundestag.de/btd/15/017/1501798.pdf.

[2] Die Datenschutzbeauftragten des Bundes und der Länder. Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. - 28. März 2003 - Elektronische Signatur im Finanzbereich. u.a. http://www.lfd.nrw.de/pressestelle/presse_7_2_33.htm, März 2003.

[3] Rechenzentrum der Finanzverwaltung des Landes NRW. Website des ELSTER-Lohn-Projektes. http://www.elsterlohn.de/.

[4] Finanzminister/-innen der Länder. Elektronische Steuererklärung hat sich etabliert. http://www.elster.de/pro_pmit.php, Jan 2005. Pressemitteilung zu ElsterFormular 2004/2005 vom 17.01.2005.

[5] Pressezentrum Deutscher Bundestag. Über eine Million Einkommensteuererklärungen mit "Elster". http://www.bundestag.de/bic/hib/2004/2004_161/12.html, Juni 2004. Pressemitteilung hib - Heute im Bundestag.

[6] Pressezentrum Deutscher Bundestag. Wegfall der Datenerfassung ist ein Vorteil der elektronischen Steuererklärung. http://www.bundestag.de/bic/hib/2005/2005_124/05.html, April 2005.

[7] Jens Falk. Freie Software nicht erwünscht. Telepolis http://www.heise.de/tp/r4/artikel/18/18847/1.html, November 2004.

[8] Wikimedia Foundation. Elster. http://de.wikipedia.org/wiki/Elster, 2005.

[9] Wikimedia Foundation. ELSTER - (Elektronische Steuer-Erklärung). http://de.wikipedia.org/wiki/ELSTER, 2005.

[10] Wikimedia Foundation. European Magpie. http://en.wikipedia.org/wiki/European_Magpie, 2005.

[11] Wikimedia Foundation. Juristische Person. http://de.wikipedia.org/wiki/Juristische_Person, 2005.

[12] Wikimedia Foundation. Natürliche Person. http://de.wikipedia.org/wiki/Nat%C3%BCrliche_Person, 2005.

[13] Roland Krebs, Carsten Heims, Wolfgang Gölter, and Berthold Platzer. ELSTER - Meilensteine eines erfolgreichen eGovernment-Projektes. https://www.elster.de/download/elster_presse.zip, OFD München, Oktober 2004. Projektlenkungsgremium ELSTER.

[14] Werner Lüdin and Marc Borter. Mission Report OECD Forum für Steuerverwaltung (FTA Forum on Tax Administration) 3. Sitzung der 'Taxpayer Services Sub-Group'. http://www.estv.admin.ch/data/etax/dokument/mreports/d/oecd_subgroup_taxpayer_services_0904.pdf, November 2004.

[15] Oberfinanzdirektion München. Das Sicherheitskonzept. https://www.elster.de/elfo_sec.php.

[16] Oberfinanzdirektion München. Unterstützte Steuererklärungen. https://www.elster.de/elster_land.php.

[17] Oberfinanzdirektion München. Website des ELSTER-Projektes. https://www.elster.de.

[18] Anja Olsok. Elektronische Übermittlung von Steuerdaten wird ausgeweitet. http://www.bitkom.org/de/presse/8477_29193.aspx, Januar 2005.

[19] Forum On Tax Administration. Survey of Trends in Taxpayer Service Delivery Using N Technologies. http://www.oecd.org/document/0/0,2340,en_2649_33749_34904256_1_1_1_1,00.html, Februar 2005.

[20] Dr. Walter Rudolf. Siebzehnter Tätigkeitsbericht 1. Oktober 1997 bis 30. September 1999. Tätigkeitsbericht 17, Landesbeauftrager für Datenschutz Rheinland-Pfalz, 1999.

[21] Peter Schaar. Tätigkeitsbereicht des Bundesbeauftragten für den Datenschutz 2003–2004. Tätigkeitsbericht 20, Der Bundesbeauftragte für den Datenschutz, 2005.

[22] Deutsche Vereinigung für Datenschutz e.V. Steuererklärung per Internet: Elster-Verfahren nach wie vor unsicher. http://www.datenschutzverein.de/Pressemitteilungen/2005_Elster.pdf, Februar 2005.

[23] Martin Weigel. Papiersieg. Zwang zur Internetnutzung zweifelhaft. *c't Magazin für computer technik*, 20(10):180, Mai 2005.

[24] Steuerbüro Knapp & Wild. Mandantenbrief Juni 2005. http://www.steuerlex.de/cnt93172/mandantenbrief.html?y=2005\&m=06\&i=, Juni 2005.

5 e-Banking - Technische Systeme, Handhabungspraxis, Verträge

Robert Fiebelkorn, Tobias Nöring

5.1 Abstract

Der Begriff des Electronic Banking steht als Synonym für den schnellen und unkomplizierten Bankverkehr des Kunden mit seinem Geldinstitut. Leistungsfähige mobile Endgeräte werden in naher Zukunft der Bevölkerung das vollkommen unabhängige und mobile e-Banking ermöglichen. Dennoch gibt es Ängste und Risiken, die die Verbreitung dieser Technologie verlangsamen. Um neben den nur schwer auszuräumenden Vorurteilen und Wissenslücken um die relativ sichere elektronische Dienstleistung den wahren Risiken durch Angriffe von Hackern, Viren, Trojanern oder Phishing entgegenen zu können, wurden im Laufe der Jahre Sicherheitskonzepte erarbeitet und stetig weiterentwickelt. Zwar bieten Verfahren wie die digitale Signatur und SET ausreichende Sicherheit, doch können sie sich aufgrund vertriebstechnischer Schwierigkeiten nicht ausreichend gut etablieren, wie die in Deutschland weit verbreiteten und ebenfalls sicheren Verfahren PIN/TAN und HBCI. Das immernoch vorherrschende Misstrauen potentieller Kunden wird in Deutschland gut durch einen relativ sicheren Rechtrahmen aufgefangen und nährt die Hoffnung, dass in naher Zukunft mit der flächendeckenden Verbreitung des Internets und der Einführung von UMTS die Zahl der electronic banking Nutzer weiter merklich zunehmen wird, da auch die Banken die Risken auf ihrer Seite engagiert und in Kooperation zu mindern versuchen.

5.2 Motivation

Die rasante Entwicklung der Mobilgeräte in den letzten zehn Jahren und die zunehmend flächendeckende Anbindung der Haushalte mit kostengünstigen Internetzugängen hat es ermöglicht, dass Finanzgeschäfte nicht mehr nur per schriftlicher Anweisung am lokalen Bankschalter, sondern von einer Vielzahl von Bürgern bereits elektronisch von zuhause oder sogar unterwegs ausgeführt werden können. Diese moderne Form der Konto- und Depotführung ermöglicht dem Kunden Mobilität und Zeiteffizienz bei der Bewältigung seiner Transaktionen, stellt aber auch die Frage nach der Sicherheit der neuen Wege.

Modernes e-Banking ist nicht mehr wie früher beim BTX, dem ersten deutschen elektronischen Kontoführungssystem, über ein festes abgeschottetes Netz realisierbar, sondern wird heute im Endkundenbereich vollständig über das Internet abgewickelt. Dadurch sind alle Bankgeschäfte die man nicht persönlich am Bankschalter abwickelt, den Augen und Ohren des weltweiten Netzwerks ausgesetzt und erzwingen angepasste Authentifizierungs- und Verschlüsselungstechniken, um unbefugte Zugriffe zu unterbinden und die Privatsphäre des Kunden zu schützen.
Ziel dieser Ausarbeitung ist es, e-Banking-Systeme für den Privatkundenbereich zu untersuchen und die dabei zum Einsatz kommenden technischen Systeme vorzustellen. Neben der Übersicht über die Alternativen in der Technik geht es vor allem darum, die Handhabung in der Praxis, also die potentiellen Gefahrensituationen und Gegenmaßnahmen bezüglich der Sicherheit und die rechtlichen Rahmenbedingungen der Verträge zu untersuchen und zu bewerten. Das heute schon weitgehend elektronisch abgewickelte Großkundengeschäft unterliegt im Wesentlichen anderen geschäftspolitischen und sicherheitstechnischen Anforderungen und ist daher nicht Gegenstand dieser Arbeit.

5.3 Electronic Banking - ein Überblick

Um die einzelnen Sicherheitsaspekte des e-Banking richtig verstehen zu können, ist es notwendig zuerst einen Blick auf die Struktur dieses Dienstleistungsbereichs zu werfen. Neben den allgemeinen Begriffsklärungen ist das Wissen um die einzelenen Anwendungsbereiche für das Verständnis der Problematik sinnvoll.

5.3.1 Definition e-Banking

Das Electronic Banking bildet einen zentralen Teilbereich des auch „e-Commerce“ genannten elektronischen Geschäftsverkehrs, der alle über elektronische Netze laufende Geschäftzsprozesse sowohl zwischen Unternehmen untereinander(B2B) als auch zwischen Unternehmen und Kunden(B2C)umfasst. Von e-Banking wird in diesem Umfeld nur geredet, wenn Banken in die elektronische Abwicklung involviert sind.
E-Banking ist folglich kein reines Bankprodukt, sondern beschreibt vielmehr die Art und Weise einer Geschäftsabwicklung.
Die Begriffe Internet-, PC-, Online-, Telefon- oder Mobile-Banking umschreiben eine Vielzahl von Zugangswegen, mittels derer die Kunden mit ihrer Bank ohne Filialbesuch kommunizieren können. Daher kann der Begriff e-Banking wie in Abbildung 1 dargestellt als Oberbegriff für alle Arten der elektronischen Abwicklung von Bankgeschäften angesehen werden.

5.3.2 Bereiche

PC-Banking bezeichnet den Teil des e-Bankings, bei dem der Bankkunde seine Geschäfte über seinen heimischen PC abwickelt. Die Datenübertragung findet dabei über die Tele-

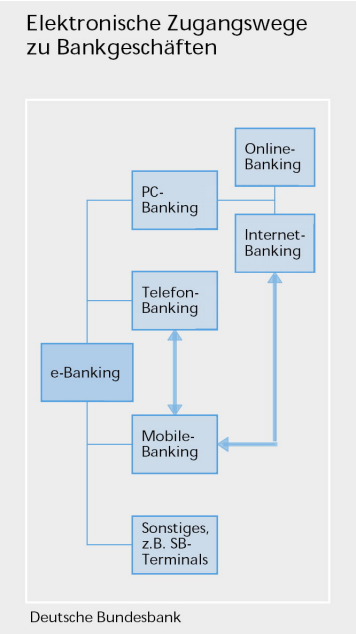


Abbildung 5.1: e-Banking Bereiche

fonleitung entweder analog über Modem, über DSL oder per ISDN statt. Grundsätzlich unterschied man hier bis vor kurzer Zeit noch zwischen dem Internet-Banking und dem Online-Banking, dass über das separate T-Online Classic Netz betrieben wurde. Dieses wurde allerdings mit dem Einstellen des letzteren hinfällig.
Das Telefonbanking ist aus heutiger Sicht weit weniger gefragt als vor einigen Jahren, da die Abwicklung von Bankgeschäften per Sprache heute sehr umständlich erscheint und die Alternativen Techniken weit mehr Funktionalität und Service bieten.
Dem Telefonbanking steht bespielsweise das moderne Mobile-Banking entgegen, dass ein anschauliches Beispiel dafür ist, dass die Grenzen zwischen den verschiedenen Formen des e-Banking zunehmend verschwinden. Durch tragbare Geräte wie Mobiltelefone, multifunktionale elektronische Assistenten (PDA) oder kleine Taschen-PCs (Handhelds) erhalten Bankkunden Dank moderner Übertragungstechniken wie WAP einen Internet-Zugang und damit die Möglichkeit zum Internet-Banking wie vom heimischen PC. Grundsätzlich ist zu beobachten, dass durch „mobile Commerce“ die Bereiche Internet und Telekommunikation immer stärker zusammenwachsen, so dass für den Kunden dieser drahtlose Zugangskanal für die Abwicklung von Bankgeschäften immer attraktiver wird. Doch befindet sich diese Entwicklung erst am Anfang, da der Nutzung von mobilen Endgeräten die geringen Datenübertragungsraten des WAP-Standards und das noch begrenzte Serviceangebot entgegen stehn. Mittelfristig wird WAP vom momentan in der Verbreitung befindlichen wesentlich schnelleren UMTS-Standard abgelöst werden, wodurch vermutlich ein großes Marktpotential für die Zukunft erschlossen werden kann.

5.3.3 Merkmale

Das electronic Banking hat durch seine moderne Form und die Nutzung mobiler Technologien und des Internets ganz eigene Merkmale entwickelt, die für die Betrachtung der Sicherheit bedeutsam sind.
e-Banking ist durch seinen virtuelle Charakter sektor- und länderübergreifend, wodurch die Abwicklung von Bankgeschäften nicht mehr an nationale Grenzen gebunden ist.
e-Banking ist ferner IT-abhängig, da der sichere und effiziente Einsatz der Informations- und Kommunikationstechnologie einen entscheidenden strategischen Erfolgsfaktor in jeder Stufe der Wertschöfungskette darstellt. Daher erhöht diese Abhängigkeit das Risiko der Banken, da eine direkte Beziehung zur Innovationsdynamik des Internets besteht.
e-Banking ist ebenso sehr dynamisch, denn Zyklen für neue Produkte im Internet sind zunehmend kürzer und fordern marktgerechte Gestaltung.

5.4 Technische Systeme

5.4.1 Überblick

Mit der Einführung des Bildschirmtext-Verfahrens BTX wurde bereits 1983 in der BRD der Einstieg in das Homebanking ermöglicht. Seitdem wurden für E-Banking besonders mit dem Aufkommen des Internets als alternative Plattform ab Mitte der neunziger Jahre neue Sicherheitsverfahren notwendig. Dabei waren teurere Verfahren wie HBCI auch aus Gründen der hohen Anschaffungskosten anfangs nur für gewerbliche Kunden interessant. Die Langlebigkeit und die behutsame Entwicklung begrenzen dabei das Angebot auf nur wenige akzeptierte und etablierte Verfahren. Das ab 1990 T-Online Classic genannte BTX-Netz wurde 2001 endgültig abgeschaltet, ist jedoch unter gleichem Namen, jedoch nun über herkömmliche Internetknoten vernetzt, noch aktiv, wodurch der frühere Schutz durch das separate Netzwerk nicht mehr gegeben ist und es somit auch nicht mehr als eigenständiges Sicherheitskonzept angesehen werden kann. Die heute verwendeten Konzepte sind daher generell auf den Einsatz im Internet ausgerichtet, legen aber die Art der technischen Umsetzung nicht fest.

5.4.2 Sicherheitskonzepte

PIN / TAN

Das schon bei BTX verwendete und damit älteste und bewährteste Verfahren um Kunden beim E-Banking einen sicheren Kontozugriff zu garantieren, ist das PIN/TAN-Verfahren. Es schützt sowohl den Zugang zum persönlichen Konto, als auch jede einzelne Transaktion an sich.
Um Zugang zum eigenen Konto zu bekommen, muss sich der Kunde zu Beginn jeder Sitzung als legitimer Kontoinhaber durch die Eingabe seiner persönlichen Identifikati-

onsnummer (PIN) authentifizieren, die ihm von der Bank initial mitgeteilt wurde. Die PIN ist je nach Bank und technischem Zugang vom Kunden selbst änderbar. Ist der Kunde vom System identifiziert und als rechtmäßiger Nutzer für das System freigeschaltet worden, kann dieser beliebige Operationen aus dem Angebot der Bank auf seinen Konten und Depots ausführen. Es muss dabei für jeden Auftrag, der den Zustand der Konten ändert, zum Beispiel bei Überweisungen und Daueraufträgen, eine nur einmal verwendbare Transaktionsnummer (TAN) eingegeben werden. Die TANs werden in Blöcken in der Regel zu insgesamt 50 Nummern von der Bank an den Kunden zuvor meist auf dem Postweg übermittelt. Um einen unbefugten Zugriff auf das Kundenkonto zu verhindern, sperrt das System den Zugang bzw. den Status automatisch, wenn PIN oder TAN dreimal hintereinander falsch eingegeben wurden.
Das System PIN/TAN gilt auch auf Basis der langjährigen Erfahrung mit BTX und T-Online als sehr sicher und wird von rund einem Drittel der deutschen Geldinstitute besonders im Privatkundengeschäft beim e-Banking eingesetzt.
Einer der wesentlichsten Nachteile dieses Systems ist das Risiko der Aufbewahrung der TAN-Listen. Diese müssen gerade bei regelmäßigem und häufigem Bedarf schnell verfügbar sein, dürfen aber auch nicht dritten Personen leicht zugänglich gemacht werden. Das ist auch einer der Gründe, warum das PIN/TAN-Verfahren nicht für das aufkommende mobile-Banking geeignet ist, da eine TAN-Liste zum Mitnehmen weder sicher noch zumutbar ist. Auch ist die regelmäßige Anforderung von neuen Listen für den Kunden auf Dauer lästig, aufwendig und unter Umständen zu langsam und somit eigentlich benutzerunfreundlich.

Digitale Signatur

Die Digitale Signatur ist eine in Chipkartenform vorliegende elektronische Unterschrift, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erstellt wird. Sie ist technisch gesehen eine Zahlenkombination und nicht, die eingescannte Unterschrift. Die sichere Digitale Signatur ist seit 2001 gemäß Signaturgesetz das Äquivalent zur eigenhändigen Unterschrift in der elektronischen Welt und wird auch als diese anerkannt.
Technisch betrachtet ist die eigentliche digitale Signatur der mit dem privaten Signaturschlüssel des Signators, der der Eigentümer der Unterschrift ist, verschlüsselte Hashwert des zu signierenden Dokuments. Sie ist daher für verschiedene Dokumente immer anders, beim identischen Dokument und demselben Verfahren zur Hashwertberechnung jedoch immer gleich. Eine nachträgliche Veränderung des Dokuments ist nicht möglich ohne die Signatur zu zerstören. Somit wird die digitale Signatur durch das zu ihrer Erstellung eingesetzte kryptographische Verfahren definiert.
Damit die digitale Signatur im elektronischen Rechts- und Geschäftsverkehr dieselben Rechtswirkungen wie die herkömmliche eigenhändige Unterschrift entfalten kann, bedarf es über den bloßen Einsatz des kryptographischen Verfahrens hinaus der sogenannten ßicheren elektronischen Signatur". Die sichere elektronische Signatur ist der eigenhändigen Unterschrift auch beim Formerfordernis der Schriftlichkeit zu hundert Prozent gleichgestellt. Durch eine sichere elektronische Signatur kann der Empfänger der elektronisch

signierten Daten eindeutig feststellen, von wem die übermittelten Daten stammen und ob die Daten inhaltlich unverfälscht sind. Um diesen Anforderungen vollständig zu genügen, hat der Gesetzgeber auf Basis der EU-Richtlinie im Signaturgesetz SigG und in der Verordnung zur elektronischen Signatur SigV von 2001 Rahmenbedingungen festgelegt, die ein Trust Center für qualifizierte Zertifikate zu erfüllen hat. Dabei unterscheidet man 3 wesentliche Bereiche:

- Registrierung des Besitzers eines qualifizierten Zertifikats und Übergabe der Signaturerstellungsdaten an den Signator
- Belehrung des Signators
- technische Komponenten und Verfahren für die sichere Signatur

Ein Internetanwender, der die digitale Signatur nutzen will, muss sich von einer allgemein vertrauenswürdigen Zertifizierungsstelle, dem Trustcenter, eine Signaturkarte mit einem kryptographischen Schlüssel zuschicken lassen. Zusätzlich benötigt er einen Kartenleser, der die Signatur ausliest und Funktionen zum Nutzen der Signatur bietet.
Praktisch kann man mit der digitalen Signatur e-Banking im Internet so betreiben, dass man Überweisungen ohne Eingabe von PIN und TAN ausführen kann. Zusätzlich können E-Mails und Dokumente ver- und entschlüsselt und über etwaige e-Government-Angebote Amtswege online erledigt werden.
Diese Technologie wird in Deutschland aber anscheinend nicht im Bereich e-Banking eingesetzt, da die Verbreitung auf angemessenem Niveau nicht gegeben ist.
Derzeit leidet daher auch die digitale Signatur an mangelnder Akzeptanz des Verbrauchers. Denn was viele Nutzer abschreckt ist die Tatsache, dass im Falle des Missbrauchs des Signaturmediums der Besitzer selbst nachweisen muss, dass seine Unterschrift gefälscht beziehungsweise missbraucht wurde. Außerdem gewährt auch die digitale Unterschrift bei unsachgemäßer Verwendung keinen ausreichenden Schutz vor Angriffen wie durch Trojaner.
Derartige Probleme würden aber nur bei mangelnder Sorgfalt und nicht ausreichenden Sicherheitsvorkehrungen auf Seitens des Benutzers auftreten. Ein gewisses Maß an Sicherheitsbewusstsein ist also auch beim Umgang mit dem Signaturmedium, wie bei der Nutzung von EC- oder Kreditkarte auch, unerläßlich.

SET - Secure Elektronic Transaction

Das Secure Elektronic Transaction Verfahren ist eingeführt worden, um das Bezahlen im Internet sicherer zu machen. Von VISA und MasterCard unter Beteiligung von IBM, Microsoft und anderer namhafter Unternehmen entwickelt, sollte sich das Verfahren als weltweiter Standard für Online-Transaktionen durchsetzen. Mit weltweiter Gültigkeit werden heuer die Kartensysteme von VISA und MasterCard unterstützt.
Die Sicherheit von SET beruht auf der Verwendung von digitalen Signaturen und der

Verschlüsselung der übertragenen Daten mit einem asymetrischen Verschlüssungsalgorithmus. Um mit dem SET-Verfahren sicher mit der Kreditkarte im Internet bezahlen zu können, müssen zunächst einmalig alle drei Teilnehmer, Kunde, Händler und Bank zertifiziert werden. Jeder Kunde benötigt ein so genanntes "Wallet", eine digitale Signatur, dass als Browser-Plugin auf dem PC installiert werden muss. Wie in der normalen Geldbörse können Kunden dort Ihre Kreditkarten virtuell ablegen und verwalten. Es aktiviert sich automatisch immer dann, wenn im Internet eine Zahlung per Kreditkarte und SET erfolgen soll.
Für jede Transaktion mit SET weisen sich Kunde und Händler je nach Kartenakzeptant mit einem gültigen Wallet aus. Die Transaktion beziehungsweise die Bestellung inklusive der Kreditkartendaten wird bei diesem Vorgang automatisch verschlüsselt, elektronisch unterschrieben und dem Händler zugeschickt. Der Händler entschlüsselt die für ihn relevanten Bestellinformationen und leitet die für die Kreditkartenfirma notwendigen Daten weiter. Die Kontodaten oder die Kreditkartennummer sind für den Händler bei der SET-Transaktion nicht einsehbar. Der Händler erhält dann von VISA die Bestätigung der Zahlung, der Kunde die Bestätigung für die Bestellung.
Die Vorteile dieses Verfahrens liegen auf der Hand. Sowohl Karteninhaber als auch Händler erhalten ein SET-Zertifikat, über welches sie sich bei einer Kreditkartenzahlung gegenseitig ausweisen können, wodurch eine eindeutige Identifizierung gewährleistet ist. Zudem ist SET auch aus datenschutzrechtlichen Gründen vorteilhaft, da bei den Transaktionen die Bank zwischengeschaltet ist und vertrauliche Bankdaten dem Händler verborgen bleiben. Auch die Bank erfährt nicht was der Kunde für sein Geld gekauft hat. Dies unterbindet somit auch Informationen über das Kaufverhalten eines Kunden, da aus Kreditkartenkäufen keine Rückschlüsse mehr gezogen werden können, was auch als einer der Gründe für die Etablierung von Kundenkarten zu vermuten ist.
Der große Nachteil dieses Verfahrens ist jedoch, dass der Kunde selbst die Initiative ergreifen und sich ein SET-Zertifikat ausstellen lassen muss, was letztendlich zum Scheitern des Standards führt, da er sich nicht wie erhofft verbreitet.

HBCI - FinTS

Mit dem 1998 erstmals praxistauglich eingeführten Home-Banking-Computer-Interface-Verfahren (HBCI) hat die deutsche Kreditwirtschaft einen neuen offenen Sicherheitsstandard gesetzt, um den besonderen Anforderungen im e-Banking gerecht zu werden und eine Plattform zu schaffen, die alle nutzen können, damit sich in Deutschland ein einheitliches Sicherheitsverfahren etabliert. Er wurde von verschiedenen Bankengruppen in Deutschland entwickelt und vom Zentralen Kreditausschuss (ZKA) bestätigt. HBCI definiert im Detail die Übertragungsprotokolle, Nachrichtenformate und Sicherheitsverfahren für den elektronischen Bankverkehr. Dabei sind die herausragenden Merkmale die Banken- und Providerunabhängigkeit sowie die öffentliche Verfügbarkeit des Standards. Er ist so offen gestaltet, dass er mehrere verschiedene Arten zur Authentifizierung des Kunden unterstützt und so relativ vielseitig anpassbar und einsetzbar ist.
Die sicherste Variante von HBCI ist momentan die Identifizierung über eine HBCI-

Chipkarte und einen Chipkartenleser, der die sichere PIN-Eingabe unterstützt. Diese vom Computer autarke Lösung schützt vor dem Mitlesen der PIN durch Tastaturüberwachungsprogramme aus Würmern und Trojanern und vor Phishing-Angriffen, da zur erfolgreichen Transaktion die digitale Signatur in Form der Chipkarte benötigt wird.
Die Weiterentwicklung des Standards in den letzen Jahren hat dazu geführt, dass heute mehrere Sicherheitsverfahren zur Authentifizierung und Verschlüsselung der Aufträge angeboten werden.
So wurden auch das PIN/TAN sowie der Einsatz von Signaturkarten zum Standard hinzugefügt. In der Version 4.0 des heute FinTS (Financial Transaction Services) genannten Standards wurden alle internen Datenstrukturen komplett auf XML und XML-Schemas umgestellt und HTTPS als zentrales Kommunikationsprotokoll festgelegt. Zusätzlich wurden neben der Ausweitung der definierten der Geschäftvorfälle wie zum Beispiel Einzelüberweisungen, Umsatzabruf eines Kontos oder Änderung eines Dauerauftrags neue Schnittstellen wie Web-Portale definiert.
HBCI ist somit kein neues Sicherheitsverfahren, sondern vielmehr ein umfangreiches standardisiertes Datenprotokoll für den Austausch von Nachrichten zwischen Kunde und Bank. Es gilt als besonders sicher, weil es mehrere bereits existierende Sicherungsverfahren kombiniert und diese zum Beispiel bei den Schlüssellängen an die heutigen Sicherheitsmaßstäbe anpasst.
Um über HBCI Bankgeschäfte zu tätigen, ist beispielsweise die Erzeugung eines RSA-Schlüsselpaares mit einer Länge je nach gewünschter Sicherheitsklasse von 1024 bis 2048 Bit nötig. Dies kann entweder auf dem PC geschehen oder auf modernen RSA-Chipkarten, die aber wegen des Schlüsselgenerierenden Prozessors noch sehr teuer sind. Alternativ gibt es auch Chipkarten mit DES-Schlüssel für synchrone Verschlüsselung, die ebenso sicher sind, da sie die Chipkarte nicht verlassen. Auch die Kombinierte Verschlüsselung mit RSA und DES ist möglich. Der persönliche Schlüssel des Kunden wird auf einer Chipkarte oder auf einer Diskette gespeichert und bei jeder Datenübermittlung automatisch überprüft. Schutz vor Missbrauch der Chipkarte oder Diskette des Kunden etwa bei Verlust wird zusätzlich gewährleistet, indem bestimmte Vorgänge durch eine PIN abgesichert werden. Soll etwa eine Nachricht verschlüsselt werden, muss der Kunde sich durch seine PIN identifizieren. Zudem ist die Chipkarte über ein persönliches Kennwort geschützt. Der Bankkunde benötigt, um HBCI nutzen zu können, eine entsprechende e-Banking-Software und in der Regel einen handelsüblichen Chipkartenleser.
Was die Sicherheit betrifft, wurde auch das HBCI-Verfahren schon von Kriminellen attackiert. Beispielsweise durch das Einschleusen von Viren oder Programmen, die die Verschlüsselung überwinden sollten. Derartige Angriffe können aber nur dann zu Problemen führen, wenn die Nutzer notwendige Sicherheitsregeln nicht beachten. Die EDV-Systeme auf Seiten der Banken bieten die höchstmögliche Sicherheit und sind beispielsweise mehrfach durch Firewalls gegen fremde Zugriffe geschützt.
Gegenüber dem üblichen PIN/TAN Verfahren ist das HBCI ohne PIN/TAN weniger umständlich, da die Eingabe und Verwaltung der TAN nicht mehr erfolgen muss. HBCI ist zudem multibankfähig, das heißt der Kunde kann mit seiner E-Banking-Software mehrere Konten bei unterschiedlichen Kreditinstituten bedienen. Außerdem bietet es durch die hohe Verschlüsselung besseren Schutz vor dem Mitlesen Dritter. Die fortschreitende

Etablierung dieses Standards führte dazu, dass HBCI bzw. das neue FinTS heute schon bei der Hälfte aller deutschen Banken angeboten wird.

5.4.3 Verschlüsselungssysteme

Als grundlegende Verschlüsselungsysteme werden im e-Banking im Wesentlichen zwei Verfahren angewandt, wobei das SSL-Verschlüsselungsprotoll weltweit der Standard ist und Transport/S als proprietäre Lösung nur in Randbereichen eingestzt wird.

SSL - Secure Socket Layer

Secure Sockets Layer (SSL) ist ein Verschlüsselungsprotokoll für Datenübertragungen im Internet. Die standardisierte Weiterentwicklung von SSL 3.0 bezeichnet man auch als Transport Layer Security (TLS).
Es ist aus technischer Sicht gesehen ein aus zwei Schichten bestehendes Protokoll, das zwischen Transport und Anwendungsschicht eine sichere Verbindung zum Gegenüber erstellt und die Verschlüsselung der zu sendenden Daten gewährleistet. Das Verbindungsaufbauende Handshakeprotokoll nutzt hierfür ein asymmetrisches Verschlüsselungsverfahren um den symmetrischen Schlüssel für die Verschlüsselung der Datenübertragung vom jeweiligen Server zu bekommen. Der Aufbau einer vertrauenswürdigen Verbindung kommt dabei auf Basis eines Zertifikats zustande. In der zweiten Schicht, dem Record Protokoll, werden dann die Daten beispielsweise mit einer stakren DES- und Triple-DES-Verschlüsselung kodiert.
SSL ist heute in jedem Internet Browser enthalten und wird dort zum Aufbau einer sicheren HTTPS-Verbindung genutzt. Dieses Konzept ist die Grundlage für alle in Deutschland gängigen e-Banking-Konzepte, die über das Internet abgewickelt werden. Die Banken nutzen den gesicherten Transportweg als Basisschicht für ihre Kommunikation mit dem Kunden.
Im Vergleich mit den zuvor vorgestellten Sicherheitskonzepten stellt SSL jedoch keine ausreichende eigenständige Absicherungsvariante dar, da ein expliziter Schutz besonders sensibler Daten nicht vorgesehen ist und bei einem durchaus möglichen Überlisten der Kodierung keine alternative Schutzmöglichkeit besteht.

Transport/S

Transport/S ist im Gegensatz zu SSL eine proprietäre Krypto-Bibliothek, die Basis für eine besonders sichere verschlüsselte Übertragung eingesetzt werden kann. Transport/S hat geringe Anforderungen an Systemressourcen und ist aufgrund seines schlanken Designs auch für Kleinstsysteme wie zum Beispiel PDA's geeignet, was den heutigen Anforderungen an Mobilität und Flexibilität der Kundenwünsche sehr entgegenkommt. Es bietet Schutz für Datenströme via TCP/IP, X.25/X.29, FrameRelay, ATM, GSM, DFÜ und RS232.

Das Transport/S-Verfahren ist ein kommerzielles Produkt und darf nur gegen Lizenzgebühren von Firmen implementiert werden, was die Verbreitung des Systems stark beschränkt aber auch eine stetige Prüfung der Sicherheit garantiert.
Besonders Positiv ist, dass es nach der E4-Norm als besonders sicher zertifiziert wurde, protokollunabhängig, multiplattformfähig und sogar in Kombination mit SSL einsetzbar ist. In der Praxis wird das System zum Beispiel beim internationalen Zugang Classic-Gate von T-Online zum unter anderem Schutz der E-Banking-Daten verwendet.

5.5 Handhabungspraxis

5.5.1 Marktsituation

Um eine sinnvolle Aussage über die momentane Sicherheitslage im e-Banking zu machen ist es notwendig, die Akzeptanz der Systeme in der Bevölkerung und die relative Verteilung beziehungweise die jeweiligen Markantiele der Verfahren im freien Bankverkehr zu untersuchen. Die Intensität mit der die verschiedenen Systeme benutzt werden, ist entscheidend für eine relalistische Einordnung der Sicherheitsrisiken für den einzelen Kunden und für die gesamte Bankwirtschaft.

Akzeptanz

Aktuelle Studien zeigen, dass das e-Banking momentan zu den beliebtesten kommerziellen Internetangeboten gehört was auch die folgende Abbildung verdeutlicht und voraussichtlich in den nächsten Jahren von einer stark steigenden Zahl von Bankkunden verwendet werden wird. Im Jahr 2004 haben bereits etwa 21 Millionen Europäer ihre Geldgeschäfte online abgewickeln. (Quelle: Studie von Datamonitor.com). Dennoch

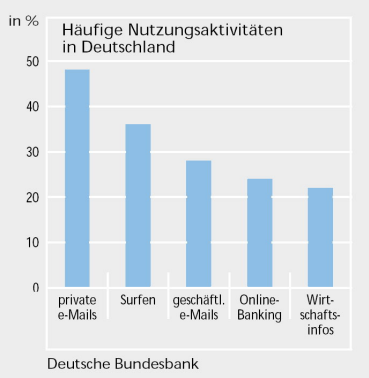


Abbildung 5.2: Aktivitäten im Internet

ist es noch ein weiter Weg, bis sich dieser Art des Bankverkehrs zum Standardverfahren in der Gesellschaft etabliert hat, denn lediglich 30 Prozent der Bevölkerung halten

Umfragen zufolge die Elektronische Geldverwaltung über das Internet für sicher(Quelle: Datamonitor.com).
Daher müssen sich die Banken um mehr Nutzer für das Online-Banking zu gewinnen und die bestehende Klientel zu halten, mehr als bisher der Befürchtung vieler Kunden stellen, dass Online-Banking zu hohe Sicherheitsrisiken birgt. Zitat: "Die Angst der potentiellen Nutzer von Online-Bank-Services vor Missbrauch ist das größte Hindernis, das der weiteren Nutzung im Wege steht."Benjamin Ensor, Senior Analyst von Forrester Research. Dies gilt im europäischen Vergleich besonders für Länder wie Italien, Frankreich oder Großbritannien, in denen eine doppelte Authentifizierung für das Online-Nutzen von Bankkonten bisher meist nicht notwendig war. Laut dieser Forrester-Studie resultiert die Unsicherheit der Verbraucher aus einer schwer definierbaren Kombination aus rationalen und eher irrationalen Ängsten vor Diebstahl und Verlusten. Die meisten Internet-Nutzer seien nicht bereit oder in der Lage, sich mit Themen wie 128-bit-Verschlüsselung oder Doppel-Authentifizierung auseinander zu setzen.
Es schein also als müssten die Banken Lösungen finden, um die bestehenden Sicherheitsbedenken der potentiellen Kunden auszuräumen, ohne sich nur auf Regierungen, Behörden oder Internet Provider zu verlassen.

Bankenrisiken

Aber auch die Banken tragen mehrere Risiken beim e-Banking. Neben den üblichen operationalen Risiken einer Bank, wie Investitions- und Konkurrenzdruck, bestehen auch Sicherheitsrisiken. Die Funktionsfähigkeit der Sicherheitsinfrastruktur steht als wesentlicher Teilbereich des e-Banking-spezifischen Risikos im Zentrum des Interesses. Denn es besteht die Gefahr, dass Daten abgehört, ausgespäht, verfälscht, missbraucht oder zerstört werden könnten. Eine andere Risikoquelle sind so genannte „Denial of Service-Ättacken (DoS) bei denen die Server der Bank mit einer Flut von falschen Anfragen überschüttet werden, so dass das System überlastet und berechtigte Benutzer keine Transaktionen mehr ausführen können. Auch die Möglichkeit eines gezielten direkten Angriffs mit Viren durch Hacker ist möglich.
Daher setzen Banken enorme Mittel zur regelmäßigen Erneuerung und Weiterentwicklung der Technik ein. Die Banken sind sich nach eigenen Angaben der besonderen Bedeutung einer funktionsfähigen Sicherheitsinfrastruktur bewusst und haben beispielsweise unternehmensübergreifende Arbeitsgruppen gebildet um Standards wie HBCI weiterzuentwickeln und Erfahrungen auszutauschen.
Ein weiteres Risiko stellt das Auslagern, das sogenannte Outsourcing, von IT-bezogenen Dienstleistungen dar. Sei es in der Entwicklung von Software im Bereich des „back office" oder im Vertrieb von Finanzdienstleistungen. Zwar können so enorme Kosten gespart werden, jedoch haben diese externen Partner auch meist nicht die ausreichende Kenntnis der komplexen, bankspezifischen Risiken. Auch die Zusammenarbeít mit mehreren Partnern in diesem Bereich stellt neue Risiken dar.

5.5.2 Allgemeine Sicherheitsrisiken

Trotz der wohldurchdachten bestehenden Schutzmaßnahmen und Verschlüsselungssysteme gibt es nicht zuletzt ,da es um Geld geht, auch beim e-Banking Wege und Mittel die Dritte ausnutzen, um sich unerlaubten Zugang zu den Konten zu verschaffen. Denn es ist vor allem auch der Faktor Mensch der es ermöglicht durch sein unvorhersehbares Verhalten logisch sicher scheinende Systeme unwirksam zu machen.

Viren, Würmer, trojanische Pferde

Die größte Gefahr im Internet-Banking geht von Viren aus. Die leichtesten Opfer sind dabei Personen, die ihr Passwort und ihre TAN-Liste auf ihrem Computer abspeichern. Jedoch auch das direkte Eingeben der Daten ist bei Virenbefall gefährlich. Wenn es eine Person mit böswilligen Absichten schafft, einen Virus oder ein Trojanisches Pferd auf den Computer des Bankkunden zu schmuggeln, was bei den häufig unzureichenden Sicherheitsmaßnahmen durchaus wahrscheinlich ist, ist es ein kleiner Schritt, die persönlichen Daten zu entwenden.
Viren haben jedoch verschiedene Auswirkungen und nicht jeder Viren-Programmierer hat böswillige Absichten. Viele dieser meist jungen Menschen möchten vor allem die Anerkennung ihrer Mitstreiter gewinnen oder mit ihren Bemühungen die oft groben Sicherheitslücken in den Programmen der Softwaregiganten aufdecken, was in diesem Sinne auch eine Art positiven Selbstreinigungseffekt haben kann, da diese Mängel sonst nicht aufgedeckt und von auf Gewinn fixierten Kriminellen ausgenutzt werden könnten
.
In erster Linie versucht sich ein Virus weiterzuverbreiten. Entweder geschieht dies als Trojanisches Pferd durch das unsichtbare Anhängen an Dokumenten und Programmen oder als Wurm durch direktes automatisches Weiterversenden per Mail über das Internet. Ein Beispiel dafür ist der im Jahr 2004 bekannt gewordene Wurm Sasser. Diese Art Viren nutzen nahezu alle vollständig die Schwächen der Microsoft Standardbetriebsysteme Windows 2000 und XP. Die dort vorhandenen technischen Sicherheitslücken und die der oft fehlerhaften Anwendungssoftware wie Internet Browser und E-Mail-Programme können vom Durchschnittsnutzer nicht erkannt werden, so dass ein Virenbefall im Normalfall nicht verhindert werden kann.
Ein Beispiel für einen erfolgreichen Versuch E-Banking mit einem Trojaner zu manipulieren, beschreibt das Magazin Internet World vom September 2004. Ein Kunde der Dresdner Bank sei demnach Opfer eines Trojanerangriffs geworden, bei dem der Virus namens „TR/small.az3“ eingesetzt wurde. Dieser zeichnete die PIN und TAN des Anwenders auf, als er seine Daten im Internet Explorer eingab. Nach der Eingabe der Daten unterbrach der Trojaner die Verbindung zum Server und lieferte anschließend beim Aufruf der Bankseite nur noch eine Fehlermeldung. Die aufgezeichneten Daten wurden dann sofort zu den wartenden Konstrukteuren des Trojaners gesendet, die dann versuchten mit diesen einen Betrag in Höhe von 6.800 Euro auf ein Konto in Lettland zu überweisen. Die Dresdner Bank konnte die Überweisung noch rechtzeitig stoppen, da der Kunde sich

umgehend an die Bank gewandt hatte. Der Trojaner nutzte dabei eine bereits bekannte Lücke im Internet Explorer und konnte alleine durch den Besuch einer präparierten Seite im Internet den Rechner infizieren. Um die Konten dann auszuspionieren, installiert er ein so genanntes Browser Helper Object (BHO), dass als Zusatzprogramm für den Microsoft Internet Explorer fungiert. Die im BHO befindliche Liste von Bankadressen, darunter auch sechs deutsche Banken, führt dazu, dass, sobald eine dieser Seiten besucht wird, alle Daten vor der Verschlüsselung mit SSL aufgezeichnet und an einen Server der Betrüger übertragen werden.
Um den Computer vor derartigen Angriffen zu schützen, ist der Einsatz von Zusatzsoftware wie Firewall-Programme und Virenscanner zwingend erforderlich. Diese können beim Auftreten einer Virusattacke aus dem Internet den Rechner zu schützen. Das ist jedoch nur durch ständiges Aktualisieren der Virensignaturen und Nachbessern des Betriebssystems durch Sicherheitsupdates möglich. Alternativ ist der Umstieg auf statistisch gesehen weniger gefährdete Systeme ratsam, wenn der Anwender nicht zwingend auf die Funktionen von beispielsweise Internet Explorer oder sogar Windows angewiesen ist, denn weniger genutzte Internet Browser wie beispielsweise Opera oder auch Linux-Betriebssysteme können eine Art Schutz bieten, da man sich so nicht mehr im primären Zielmuster der Angreifer befindet.

Spoofing

Spoofing nennt man einen Vorgang, bei dem sich Dritte bei der Übermittlung von Daten über ein Netzwerk unbefugt zwischen Sender und Empfänger schalten. Sie können so auf die Daten von Sender und Empfänger zugreifen, Daten herausnehmen, verändern oder einfach nur mithören. Übermittelt also beispielsweise ein Kunde einem Händler seine Kreditkartennummer online, können findige Experten diese Informationen auslesen und weiterverwerten.
Ein Gegenmittel um einen Spoofing-Angriff unwirksam zu machen ist es, alle sicherheitsrelevanten Daten zu verschlüsseln. Dabei können die Daten entweder symmetrisch oder asymmetrisch verschlüsselt werden.
Bei der symmetrischen Verschlüsselung ist das Kennwort für die Ver- und Entschlüsselung ist identisch. Dabei ist es allerdings notwendig das Kennwort von der Bank zu Kunden zu transportieren. Befinden sich Dritte im Besitz dieses Kennwortes bzw. fangen es bei der Übertragung ab ist die Verschlüsselung unwirksam und man kann beim Spoofing alle Daten entschlüsseln.
Die asymmetrische Verschlüsselung, die auch als Public-Key-Verfahren bekannt ist, verwendet einen Schlüssel zum Kodieren und einen zum dekodieren. Daher kann der öffentliche Schlüssel nicht zum Lesen der chiffrierten Datenpakete verwendet werden und muss nicht geschützt werden. Der private Schlüssel zum dechiffrieren liegt lokal beim Empfänger und kann nicht durch Spoofing abgefangen werden. Dieser Schlüssel ist der einzige der geschützt werden muss.

Phishing

Der Begriff Phishing ist eine englische Wortschöpfung aus den Begriffen Password und Fishing und bezeichnet sinngemäß den Versuch wichtige Passwörter dem Besitzer durch verschiedenste Tricks zu entlocken, um sich dann damit mit seiner Identität zu geschützten Bereichen Zugang zu verschaffen. Die hierbei am meisten verwendete Methode ist das kombinierte Vortäuschen von authentischen E-Mails und Internetseiten. Die E-Mails erwecken dabei den Eindruck, als stammten sie von einer vertrauenswürdigen Stelle und verweisen meist auf eine offiziell erscheinende Internetseite die vom Original optisch meist nicht unterscheidbar ist. Beispielsweise werden sie mit seriösen Nachrichten eines Kreditinstitutes getarnt, um dann den Empfänger darin aufzufordern persönliche Daten, Passwörter oder auch PIN-Codes zu verifizieren bzw. zu aktualisieren. Dies geschieht oft über einen in der Email enthaltenen Link der den Kunden scheinbar direkt zur Bankseite führt aber in Wahrheit auf eine nachempfundene Seite verweist. Dabei nutzen die Betrüger die Gewohnheit und Vertrautheit der Menschen aus, denn E-Mails und Zielseiten sehen dem Original täuschend ähnlich. Mit den eingegebenen Daten haben die Betrüger dann ungehinderten Zugang zu dem Konto.
Begünstigt wird ein solches Vorgehen auch durch Sicherheitslücken in Webbrowsern. Beispielsweise wurde Ende Mai 2005 bekannt, dass alle gängigen Internetbrowser sowohl unter Mac als auch unter Windows durch erzeugen einer JavaScript-Dialogbox auf einer vertrauenswürdigen Seite eine Abfrage von persönlichen Daten sehr einfach ermöglichen, ohne dass der Anwender, wie in den Abbildungen zu sehen, den Ursprung dieser Dialogbox verifizieren kann - siehe Abbildung.

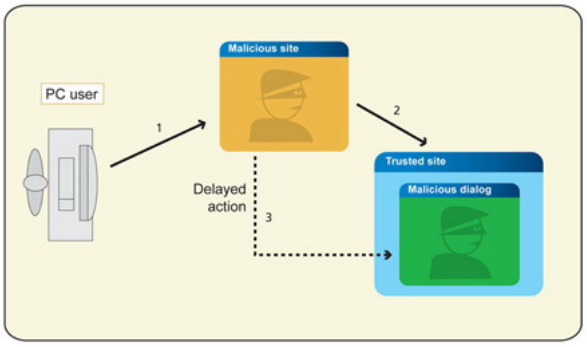


Abbildung 5.3: Phishingbeispiel

Um sich vor solchen Phishingangriffen zu schützen, hilft es nur sehr genau zu prüfen, ob man sich auch auf der richtigen Seite befindet und E-Mails mit fragwürdigen Bitten um Passwörter und TAN-Nummereingabe nicht zu folgen und stattdessen den Vorgang bei der Bank zu melden. Ungewohnte Abfragen und Dialogboxen um vertrauliche Daten auch in vertrauter Umgebung sollten immer erst nach Rücksprache mit der Bank beantwortet werden.

Social Engineering

Die wohl subtilste Methode um an Zugangsdaten für Bankkonten und Depots zu gelangen, kommt ganz ohne technische Tricks und Software aus. Die Schwachstelle Mensch ermöglicht es durch geschickte Manipulationen Informationen zu erfahren, die offensichtlich sonst auf direktem Wege fremden Personen nicht preisgegeben werden würden.
Dabei geht der Angreifer schrittweise vor und ruft beispielsweise viele verschiedene Leute im Unternehmen oder Umfeld der Zielperson an. Von jedem Angerufenen erhält er durch geschicktes Erfragen eine kleine Menge an Zusatzinformationen, die er aber beim nächsten Anruf wieder als Mittel zur Vertrauensbildung einsetzen kann. Diese Methode ist vielleicht nicht ideal um Passwörter für das E-Banking zu erfragen, kann aber unter Umständen Informationen entlocken, die dann kombiniert mit anderen Methoden, wie dem Phishing zum gewünschten Erfolg führen können.
Beispielsweise wurde nach der Auslosung der ersten Tickets für die Fußballweltmeisterschaft 2006 E- Mails mit einem Virus im Anhang an eine Vielzahl der Bewerber verschickt, mit der Information, dass sie Karten zugeteilt bekommen haben und den Anhang zur weiteren Bearbeitung öffnen sollen. Durch diese Vortäuschung eines Gewinns und der Manipulation hin zu einer gewollten Aktion wurden viele Empfänger dazu gebracht den mitgesendeten Wurm Sober.O zu aktivieren. Dieses Beispiel zeigt, dass besonders auch bei E-Mails die Manipulationen effektiv sein können.
Der Schutz vor Social Engineering ist nur in beschränktem Rahmen möglich, da diese Art der Angriffe auf der zwischenmenschlichen Ebene mit Mitteln wie Verführung und Beeinflussung arbeitet und man sich nur durch stetes skeptisches Verhalten und Überprüfen etwas absichern kann. Im Falle von E-Mails bedeutet dies, dass man besonders bei Mails die eine Aktion verlangen, die darauf drängen, einen Anhang zu Öffnen, die etwas Versprechen, die Komplimente von Unbekannten aufweisen und die viele sprachliche Fehler oder falsche Angaben beinhalten wachsam sein sollte um nicht in eine Falle zu geraten.

5.6 Rechtliche Aspekte

Die Sicherheit beim e-Banking ist für den Kunden nicht nur eine Frage des Schutzes vor kriminellem Zugriff, sondern auch eine Frage des Rechts auf Schadensersatz wenn ihm durch einen solchen Angriff ein Schaden entsteht. Da diese Fälle in Deutschland im Moment nur sehr selten auftreten, ist ein generelles Verhalten der Banken in diesen Fällen nicht vorherzusagen. Generell ist es momentan jedoch so, dass bei rechtzeitigem Melden von unnormalen Dialogen und Fehlern, illegale Transaktionen insofern sie noch nicht verbucht und der Zielbank überwiesen wurden, rückgängig gemacht werden. Über ein mögliches Verhalten der Banken bei einem nicht mehr umkehrbaren Schaden zu ergründen ist der Blick in das Kleingedruckte der Bankverträge notwendig.

5.6.1 Verträge

Um den rechtlichen Rahmen für den Kunden festzustellen, wurden exemplarisch zwei Verträge zweier bedeutender deutscher Kreditinstitute untersucht. Diese stellen in ihrem Kleingedrucken eindeutig die Bedingungen für die konto- und depotbezogene Nutzung des jeweiligen Online-Banking-Service klar. Die zwei untersuchten Banken sind die Comdirect Bank und die Deutsche Bank.
Die Comdirect Bank wurde als Direktbank-Tochter der Commerzbank gegründet und bietet quasi nur Online-Brokerage Dienste sowie umfangreiche Kurs- und Börseninformationen. Da es hier keine Filialen gibt, ist das Angebot vollständig auf den elektronischen Bankverkehr ausgerichtet. Alle folgenden Informationen entstammen ausschließlich dem Vertragstext bzw. den Bedingungen für die Onlinenutzung der jeweiligen Bank.
Als Sicherheitsplattform nutzt die Comdirect Bank das PIN/TAN-Verfahren auf einer 128 Bit verschlüsselten SSL Verbindung. „Diese Sicherungsvorkehrungen sind entsprechend den Vorgaben der Benutzerführung anzuwenden und geheim zu halten." Zusätzlich zu dieser Aufforderung wird darauf hingewiesen, dass „diese Geheimcodes Unbefugten zugänglich werden, wenn im Internet die Bankadresse nicht direkt angegeben wird (z.B. bei Links)." Um so das Ausspionieren über Phishing-Seiten zu unterbinden wird die Adresse der Bank explizit genannt. Um sich darüber hinaus noch abzusichern erklärt die Bank, „Sollte der Online-Nutzer dennoch andere, hier nicht genannte Zugangswege benutzen[...], oder den Zugang mittelbar über andere Dienstanbieter wählen, so geschieht dies auf sein Risiko." Ferner heißt es, „Dieses Risiko kann dadurch verringert werden, dass sich der Online-Nutzer zuvor das Zertifikat des Servers [...] anzeigen lässt, um sicherzustellen, dass eine direkte Verbindung mit der Comdirect Bank AG besteht."
Man schiebt also das Risiko für bekannte Risiken wie mögliche vorgetäuschte Bankseiten oder Abfangen der Logindaten vor dem eigentlichen Zugang dem Kunden zu und übernimmt hierfür keine Haftung. Im weitern Teil der Bedingungen werden auch die vorgeschriebenen Vorsichtsmaßnahmen der Kunden genannt.

Da heißt es unter anderem:
„Die Sicherheitsvorkehrungen [also PIN/TAN sind] geheim zu halten und[...] unverzüglich zu sperren, [...] wenn er den Verdacht hat, dass ein unbefugter Dritter davon Kenntnis hat oder haben könnte."
Sie „[..] sollten nicht abgespeichert werden, insbesondere ist im Internet der Cache des verwendeten Browsers zu deaktivieren oder nach der Nutzung zu löschen."
„Die Datenfreigabe darf im Internet erst erfolgen, wenn auf dem Bildschirm angezeigt wird, dass die Datenübermittlung verschlüsselt erfolgt." Entscheidend ist auch: „Der Online-Nutzer hat das ihm Mögliche zu tun, damit sich keine Computerviren auf seinem Gerät befinden. Fremdsoftware einschließlich besonderer Verschlüsselungssoftware ist nur von allgemein vertrauenswürdigen Anbietern zu beziehen." Diese Aussage ist rechtlich sicherlich weit auslegbar und nicht konkret an bestimmten Handlungen festzumachen. Ein möglicher Rechtsstreit auf Basis dieser Vorschrift wäre hier im Ernstfall wohl nicht zu vermeiden.

Die Deutsche Bank ist im Gegensatz zur Comdirect Bank eine Filialbank, die das Onlinegeschäft zusätzlich in ihr Serviceangebot aufgenommen hat. Basis der Onlinedienste der Deutschen Bank ist ebenfalls das PIN/TAN-Verfahren wobei auf eine verschlüsselte Verbindung über SSL nicht explizit hingewiesen wird. Auch ist der Weg zur Bankseite nur indirekt Beschrieben und versteck sich etwas hinter den Worthülsen des Kleingedruckten. Es heißt, „der Nutzer ist verpflichtet, die technische Verbindung zum Online-Banking-Angebot der Bank nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle herzustellen." Eine genaue Auflistung dieser Zugangskanäle ist im Text nicht enthalten, was zuerst nachteilig erscheint, aber durch separate Veröffentlichung an anderer Stelle eine höhere Aktualität ermöglicht. In den darauf folgenden Bestimmungen zur Geheimhaltung heißt es, „der Nutzer hat dafür Sorge zu tragen, dass keine Person Kenntnis von der PIN und der TAN erlangt." Ferner dürfen „PIN und TAN [...] nicht elektronisch gespeichert oder in anderer Form notiert werden[...]" und „die dem Nutzer zur Verfügung gestellte TAN-Liste ist sicher zu verwahren". Um die erste Formulierung für den konkreten Fall der Eingabe noch einmal zu betonen heißt es, „ bei Eingabe der PIN und TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können." Diese Aussagen der Bank stellen ihr rechtliches Verhalten eindeutig dar und übertragen die Verantwortung für die Sicherheit der Zugangsdaten alleine auf den Kunden ohne diesen über etwaige Gefahren und sinnvolle Verhaltensweisen aufzuklären.
Im Vergleich zu Comdirect Bank, bei der Hinweise zu Viren, Cache und Verschlüsselungssoftware zu finden waren, konzentriert sich die Deutsche Bank alleine auf die rechtliche Absicherung der eigenen Interessen und überlässt es dem Kunden welche Mittel er einsetzt um den Fremdzugriff zu unterbinden. Dies kann für den Kunden auch dazu führen dass Gefahren wie Cacheinhalte nicht erkannt und später im Rechtsstreit gegen ihn verwendet werden können. Subjektiv betrachtet scheinen sich die Bedingungen der Comdirekt Bank als reine Online-Bank näher am Kunden zu orientieren und etwas mehr auf die konkreten Gefahren zugeschnitten zu sein als die der Deutschen Bank. Inwiefern sich diese unterschiedlichen Bedingungen jedoch in einem Rechtsstreit auswirken, ist aus nicht-juristischer Sicht nicht einzuschätzen.
Zwar ist es in diesem Rahmen nicht möglich für alle deutschen Kreditinstitute die Vertragsbedingungen für den elektronischen Bankverkehr zu überprüfen, dennoch ist davon auszugehen, dass ähnliche Bedingungen auch in den hier vorgefundenen Abweichungen bei allen deutschen Bankgesellschaften anzutreffen sind, die Onlinedienste anbieten.

5.6.2 Bankenaufsicht

Die veränderte Risikosituation der Institute im Bereich des elektronischen Bankverkehrs hat auch Konsequenzen für das Aufsichtskonzept der Bundesbank und der Banken selbst. So erfordert die Entwicklung laut Bundesbank eine angemessene Anpassung der Kontrollmechanismen. Dabei sei eine nationale Lösung alleine schon schon wegen des grenzüerschreitenden Charakters des e-Bankings nicht ausreichend. Eine intensive internationale Zusammenarbeit und Abstimmung unter den Bankenaufsichtsbehörden scheint daher wichtiger denn je. Es zeichnet sich jedoch bereits ab, so die Bundesbank, dass die

Bankenaufsichten sich weit stärker als bisher mit der Anwendung der Informationstechnologie in Kreditinstituten und deren Auswirkungen beschäftigen müssen.

5.6.3 Rechtsrahmen

Für die auch oft internationnal tätigen deutschen Banken ergeben sich Rechtsrisiken aus der Tatsache, dass Gesetze zur Gültigkeit und Durchsetzbarkeit elektronisch geschlossener Verträge in vielen Ländern derzeit erst in der Erarbeitung sind. In Deutschland wurde dies bereits sehr früh durch das so genannte Signaturgesetz geregelt.
Das 2001 in Kraft getretene Signaturgesetz wurde geschaffen, um angemessene Rahmenbedingungen für den Einsatz von elektronische Signaturen zu schaffen. Dabei war es das Ziel der Gesetzgeber eine erhöhte Rechtssicherheit für den im Internet stattfindenden e-Commerce zu finden. Es bestimmt die Anforderungen an die qualifizierte Zertifikate und an ihre Aussteller. So wird ein bestimmteter Mindestinhalt festgelegt wie unter anderem das Vorlegen eines Sicherheitskonzeptes. Allerdings umfasst das Gesetz keine Rechtsfolgen für die Verwendung qualifizierter Signaturen, so dass hier auf bereits bestehende Gesetze zurückgegriffen werden muss, wie Paragraphen des Prozess, Verwaltungs um Zivilrechts um etwaige Schäde zu regulieren.
Mit dem Signaturänderungsgesetz von 2004 wurden dann diverse Veränderungen vorgenommen, so dass die Bundesregierung nun hofft, dass durch das erlaubte Einspringen der Kreditinstitute zur Zertifikatvergabe EC-Karte mit Signierfunktion eine weite Verbreitung der Signaturtechnik ermöglichen.
Insgesamt unterscheiden sich die Regelungsansätze derzeit noch von Land zu Land. Hieraus sich ergebende Unsicherheiten erhöhen sich zusätzlich bei grenzüberschreitenden Geschäften mit Ländern, in denen das Kreditinstitut keine eigene Zweigniederlassung beziehungsweise Tochtergesellschaft unterhält. Die mangelnde Vertrautheit mit fremden Rechtssystemen birgt darüber hinaus Risiken in Bezug auf Fragen des Verbraucher- und Datenschutzes.

5.7 Fazit und Ausblick

Die Sicherheit im Bereich E-Banking ist wie viele Dinge im Alltag nicht perfekt, aber trotz vieler kritischer Meinungen besser als ihr Ruf. Mit der ständig zunehmenden Zahl an Internetnutzern steigen auch kontinuierlich die Anhänger der elektronischen Bankdienstleistungen. Es ist nicht zuletzt die Unwissenheit der Bevölkerung um die Sicherheitstechnik und die realen Risiken die damit verbunden sind, die eine allgemeine Stimmung der Angst vor dem illegalen Zugriff auf das eigene Konto verbreiten. Die Banken verwenden im Allgemeinen für den Kunden sichere Verfahren, jedoch kann man die schnelle technische Entwicklung nicht vorhersagen, und daher nie wissen, welche Viren, Würmer und Tricks Kriminelle entwickeln werden um leichter an ihr Ziel zu kommen. Diese Tatsache und die wachsende Verbreitung mobiler Endgeräte mit denen in Zukunft Kontobewegungen geradezu spielerisch und auf einfachste Weise veranlasst werden können, mahnt zur Vorsicht und stetigen Weiterentwicklung der Sicherheitsmechanismen,

die zwar zunehmend unsichtbarer werden, aber dennoch nicht aufweichen dürfen. Eine weitere Neuerung die in den Kinderschuhen steck, ist das TV-Banking, das mit Einführung von MHP, HDTV und DVB die heimischen Wohnzimmer erobern soll. So werden nach optimistischen Schätzungen schon von führenden europäischen Analysten bereits in den kommenden Jahren einige Millionen Europäer ihre Bankgeschäfte über das neue interaktive Fernsehen abwickeln. Heute schon ist es technisch möglich mit Hilfe von Set-Top-Boxen Finanzgeschäfte mit der Fernbedienung über das Fernsehgerät zu tätigen. Doch auch im Bereich der Sicherheit darf der Kunde hier keine Revolution erwarten und muss auf die bereits etablierten Technologien wie das PIN/TAN Verfahren und Transport/S zurückgreifen. Kunden, die auf die Etablierung einer den neuen mobilen Anforderungen angemessenen und darüber hinaus noch benutzerfreundlichen Sicherheitsstrategie hoffen, werden sich wohl auch in den kommenden Jahren gedulden müssen.

5.8 Glossar

`ATM - Asynchronous Transfer Mode`
ist eine vermittelnde, verbindungsorientierte Basistechnologie für Weitverkehrsnetze und LANs, mit der zeitkritische Applikationen übertragen werden können.

`B2B - Business-to-Business`
Bezeichent die Geschäftsbeziehungen zwischen Firmen.

`B2C - Business-to-Costumer`
Bezeichent die Geschäftsbeziehungen zwischen Firma und Endkunde, dem Verbraucher.

`BTX - Bildschirmtext`
Informationssystem der Deutschen Telekom aus den 90-iger Jahren.

`DES - Data-Encryption-Standard`
Der Data-Encryption-Standard (DES) ist ein vom amerikanischen National Bureau of Standards (NBS) entwickelter kryptografischer Algorithmus d.h. ein abgeschlossener Verschlüsselungsrechenvorgang mit einer sich zyklisch wiederholenden Gesetzmäßigkeit für die Verschlüsselung und Entschlüsselung von Daten.

`DFÜ - Datenfernübertragung`
Die Datenübertragung von einer Datenverarbeitungsanlage zu einer anderen über Datenleitungen.

`DVB - Digital Video Broadcasting`
Ist ein europäischer Standard für Digitalrundfunk, Digital-TV, multimediale Dienste und interaktive Verteildienste.

`GSM - Groupe Spéciale Mobile`
Standard des europäischen Funktelefonsystems im 900-MHz-Bereich

`Handheld`
Tragbarer Kleincomputer in Form eines PDAs aber leistungsfähiger.
`HDTV - High Definition Television`
HDTV ist ein Überbegriff für Digital-TV, die mit mehr Zeilen arbeiten als NTSC (Fernsehstandard USA) oder PAL (Fernsehstandard Europa).

`HVB eFIN`
HBCI-Softwarelösung für E-Banking-Geschäfte.

`MHP - Multimedia Home Platform`
MHP ist ein offener Standard aus dem Jahr 2000 für Digital-TV und Multimedia.

`PDA - Personal Digital Assistant`
vieseitiger tragbarer elektronischer Terminplaner und Organizer.
`PIN - Personal Identification Number`
ist eine mehrstellige persönliche Geheimzahl zur Authentifizierung des Besitzers.

`RSA - Rivest-Shamir-Adleman`
Das bekannteste, bewährteste und am besten untersuchte asymmetrische Verschlüsselungverfahren.

`RS232`
ist eine Spannungsschnittstelle (im Gegensatz zur Stromschnittstelle z.B. Current-Loop oder 20mA-Schnittstelle). D.h. die verschiedenen Spannungspegel stellen die Information dar.

`SigG - Signaturgesetz`
Das Signaturgesetz regelt seit 1997 in Deutschland die Rahmenbedingungen für Zertifizierungsinstanzen.

`SigV - Signaturverordnung`
Die Signaturverordnungen enthalten die Durchführungsbestimmungen des Signaturgesetzes.

`WAP - Wireless Application Protocol`
Protokollstandard für die Bereitstellung von text- und grafikbasierten Informationen und Diensten für mobile Endgeräte

Literaturverzeichnis

[1] http://bsi-fuer-Buerger.de.

[2] http://fk.hypovereinsbank.de.

[3] http://www.a-trust.at.

[4] http://www.schoellerbank.at.

[5] https://ww2.homebanking-berlin.de.

[6] http://www.sparkasse-erlangen.de.

[7] http://www.nemeso.de.

[8] http://www.vobakrefeld.de/electronic-banking/internet_banking.

[9] http://www.internet4jurists.at.

[10] http://www.fun.de/deutsch/produkte/onlinebanking/tvbanking.htm.

[11] http://www.computerwelt.at/detailArticle.asp?a=91552&n=2.

[12] http://www.peterhuth.de/2004.php.

[13] http://de.wikipedia.org/wiki/HBCI.

[14] http://www.itwissen.info/.

6 Online-Auktionen: Technische Systeme, vertragliche Situation

Christian Simonsky, Mario Wegner

Dieses *paper* befasst sich mit dem Thema „Online-Auktionen“, speziell mit den technischen Systemen und der rechtlichen Situation. Im ersten Teil werden die sicherheitsrelevanten Aspekte von Online-Auktionen beleuchtet, wobei anhand von 3 Auktions-Plattformen die praktische Umsetzung bzgl. dieser Aspekte betrachtet wird.
Im zweiten Teil soll der rechtliche und vertragliche Rahmen beschrieben werden, in dem Online-Auktionen stattfinden. Hierbei werden Themen wie Vertragabschluss, Widerrufs- und Rückgaberecht und Haftbarkeit behandelt.

6.1 Einleitung

Irgendwo zwischen Jagdinstinkt, Spieltrieb, Sport und Hobby liegt die Erklärung für eines der zur Zeit größten (Freizeit-)Vergnügen: Online-Auktionen.
Unzählige Internet-Benutzer finden sich nach Arbeit oder Schule am heimischen PC wieder, um bei eBay und Co. ein Schnäppchen zu ersteigern oder ein wenig Kapital aus altem Ramsch zu erwirtschaften. Virtuelle Auktionen gibt es reichlich, doch das Vergnügen, welches Online-Auktionen bieten, greift über den virtuellen Raum hinaus: Verträge werden geschlossen, Ansprüche werden begründet und Bewertungen werden abgegeben. Dabei stellen sich häufig Fragen wie: Wer ist mein Gegenüber überhaupt? Kann ich dieser Person trauen? Wen bzw. was genau gilt es zu bewerten?
Oft interessiert man sich erst für die rechtlichen Grundlagen, die hinter einer Auktion stehen, wenn etwas schief gelaufen ist...dann ist guter und schneller Rat teuer, meist aber vergebens. Auch lebt man in der trügerischen Gewissheit, dass die Plattform, welche man zum Ver- oder Ersteigern gewählt hat, sicher sei bzgl. krimineller Machenschaften. Doch immer mehr ehrliche Nutzer werden Opfer von Betrügern, die ihnen unter eigennützigem Interesse das Geld für Waren aus der Tasche ziehen, die dann nie versandt werden oder fehler- bzw. mangelhaft sind.
Dazu sollte es eigentlich gar nicht erst kommen, doch leider bieten viele Auktions-Plattformen nicht die Sicherheit, die man als Benutzer erwartet. Auch der rechtliche Rahmen, in dem sich eine Online-Auktion bewegt, ist eher schleierhaft. Im Folgendem soll daher darauf eingegangen werden, welche sicherheitsrelevanten Aspekte bei Online-Auktionen zum tragen kommen, wie diese umgesetzt werden, und welche Möglichkeiten bestehen, sein Recht geltend zu machen.

6.2 Technische Systeme

In diesem Abschnitt soll auf die sicherheitsrelevanten Aspekte von Online-Auktionen eingegangen werden. Dabei wird der Schwerpunkt auf der Passwortsicherheit, der Identitätskontrolle und der Prävention von Phishing-Attacken liegen, da dies die wohl wichtigsten Ansatzpunkte für Sicherheit bei Online-Auktionen darstellen. Sicherlich bieten die Auktionsplattformen noch weitere Maßnahmen zur Sicherheit der Kunden beim Erwerb bzw. Verkauf von ersteigerten Artikeln, wie z.B. Treuhand- und Lieferservice oder Versicherungsschutz. Allerdings wird an der Stelle nicht näher auf diese Aspekte eingegangen, zum Einen aus Platzgründen, zum Anderen spielen sie bzgl. des Themas der Ausarbeitung eine eher untergeordnete Rolle.
Nachdem die Problemstellung als solches gezeigt wurde, wird anhand der 3 Online-Auktionsplattformen eBay, Ricardo und Atrada näher darauf eingegangen, wie die einzelnen Plattformen präventiv Sicherheitsmassnahmen ergreifen. Leider ließen die o.g. Unternehmen auf Anfrage keine detaillierten Blicke auf interne Sicherheitsmechanismen und Filter etc. werfen, weswegen sich hierfür nur auf die offiziellen Webseiten der Anbieter und diverse Artikel im Internet bezogen werden konnte.

6.2.1 Vorstellung der Auktionsplattformen

eBay

„eBay ist der weltweite Online-Marktplatz. 1995 in Kalifornien als Marktplatz für den Austausch von Sammlerartikeln gegründet, hat sich eBay sehr rasch zu einem der größten sowie leistungs- und besucherstärksten Marktplatz für den Verkauf von Gütern entwickelt.
Jeden Tag werden in Tausenden von Kategorien Millionen von Artikeln angeboten. Käufer und Verkäufer können dabei weltweit miteinander handeln, denn eBay ist in 31 internationalen Märkten auf vier Kontinenten präsent.
Inzwischen handeln bereits über 114 Mio. registrierte Mitglieder weltweit bei eBay. Der Reiz des Handelns bei eBay liegt nicht zuletzt darin, dass die Funktionsweise des virtuellen Marktplatzes kinderleicht ist.[ ]“ [ebay]

Ricardo

„ricardo.ch AG wurde im November 1999 unter dem Namen auktion24.ch in Baar (ZG) gegründet und ist seit November 2000 Mitglied der europäischen E-Commerce-Gruppe QXLricardo plc in London. Die Gruppe ist in 10 Ländern in Europa vertreten und hat 3,5 Mio. Mitglieder.
ricardo.ch entwickelt und betreibt eine Internet-Auktionsplattform, welche von den mehr als 700'000 Schweizer Mitgliedern für den Kauf und Verkauf von neuen und gebrauchten Waren genutzt wird. ricardo.ch beschäftigt heute mehr als 30 Mitarbeiter in der Schweiz und ist mit über 150'000 Auktionen der klare Marktführer bei den Schweizer Online-Auktionsplattformen .[ ]“ [ricardo]

Atrada

„Atrada steht für rund zehn Jahre Erfahrung im E-Commerce. Seit der Gründung 1995 hat sich das Unternehmen in Deutschland zu einem wichtigen Competence Center für den Online-Handel entwickelt. Neben den Marktplätzen Atrada und AtradaPro bietet die Atrada AG professionelle Beratung für Business Solutions im E-Commerce.
Seit 2001 ist die Atrada AG hundertprozentige Tochter der T-Online International AG. Die Allianz steht für konzentriertes Internet-Know-how sowie professionelle Vernetzung. [ ]“ [atrada]

6.2.2 Passwörter

sichere Passwörter

Die Wahl eines sicheren Passwortes bei der Anmeldung eines Benutzerkontos für eine Online-Auktion ist der erste wichtige Schritt für Kunden, um ihre Accounts vor Hackern in einem gewissen Maß zu schützen. Sicherlich bietet die Wahl des Passwortes keinen 100%igen Schutz, doch zählen trivial gewählte Passwörter zu den „Lieblingen“der Hacker. Dies ist der Nachlässigkeit der Kunden zu verdanken, sich bei der Wahl ihres persönlichen Passwortes auf leicht zu findende Passwörter, wie Namen von Kindern oder Tieren, ja sogar dem Benutzernamen, einzulassen, in der Hoffnung, eben jenes Passwort nicht vergessen respektive sich leichter merken zu können. Schon durch pures Ausprobieren lassen sich so einige Passwörter knacken, auch Listen mit häufig verwendeten Passwörtern oder Lexika kommen bei Hackern zum Einsatz. Um ein möglichst sicheres Passwort zu wählen, sollte man Buchstaben, Zahlen und Sonderzeichen kombinieren, und zwar so, dass sich eine logische Kombination ausschließen bzw. nicht nachvollziehen lässt.

Umsetzung

ricardo.ch Meldet man sich beim Auktionshaus Ricardo an, so wird ein zufallsgeneriertes Passwort an die e-mail-Adresse versandt, mit welchem man sich dann einloggen kann. Natürlich besteht die Möglichkeit, sein Passwort abzuändern. Tut man dies, so sind folgende Richtlinien bei der Wahl des Passworts einzuhalten:

- Länge des Passworts: mind. 6, max. 15 Zeichen
- Passwort muss Kombination aus Buchstaben und Zahlen (oder Sonderzeichen) sein (mind. eine Zahl oder ein Sonderzeichen muss benutzt werden)
- Passwort darf nicht identisch mit dem Benutzernamen sein

Hält man sich nicht an diese Richtlinien, ist eine Änderung/Anerkennung des Passworts nicht möglich.

ebay.de Bei eBay wählt man sich von Anfang an ein eigenes Passwort. Im Gegensatz zu Früher, als man sein Passwort ohne Einschränkungen frei wählen (und somit sehr unsicher gestalten) konnte, integriert eBay jetzt bei der Wahl von Passwörtern eine Sicherheitsprüfung, welche die Sicherheit des (neu) gewählten Passworts anzeigt (siehe Abb.). Erscheint dabei das Passwort zu unsicher oder ist es gar ungültig (bei der Wahl des Benutzernamens als Passwort z.B.), wird keine Änderung oder Anerkennung des Passwortes erwirkt.

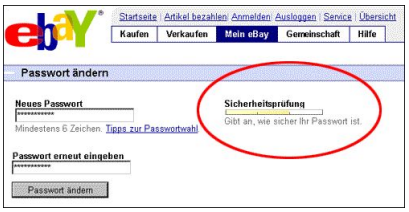


Abbildung 6.1: Sicherheitsprüfung des Passworts bei eBay

Auch bei eBay muss das Passwort mindestens 6 Zeichen lang sein, allerdings müssen keine Zahlen und Buchstaben kombiniert werden, um ein gültiges Passwort zu erhalten. In der Abbildung wurde ein Passwort bestehend aus 11 Buchstaben gewählt, welches zwar die Skala der Sicherheitsprüfung nicht füllt, dennoch aber gültig ist.

atrada.de Bei der Online-Auktionsplattform Atrada wird bzgl. der Wahl eines sicheren Passwortes lediglich ein Aspekt berücksichtigt: Die Länge des Passwortes, welches mindestens 6 Zeichen lang sein muss. Weitere Einschränkungen bei der Wahl des Passwortes gibt es nicht, so dass es möglich ist, triviale Passwörter nebst dem Benutzernamen zu wählen.

6.2.3 Phishing / Passwortklau

Beim Passwortklau handelt es sich um das Stehlen der Zugangsdaten eines Benutzers zu seinem Benutzerkonto. Hierfür werden nicht mehr nur simple Methoden, wie das einfache Ausprobieren von trivialen Passwörtern, benutzt. Das so genannte Phishing (Password Fishing) erlebt einen nie da gewesenen Boom und die Methoden des Phishings werden immer ausgereifter und vielfältiger.
Phishing ist eine Form des Trickbetrugs mit Methoden des Social Engineering und umfasst den illegalen, weitgestreuten Versuch Anwendern ihre Zugangsdaten für sicherheitsrelevante Bereiche zu entlocken. Die gängigste Methode einer Phishing-Attacke ist der Versand einer Phishing-e-mail, in der der Empfänger aufgefordert wird, über einen angegebenen Link eine offizielle Webseite zu besuchen, um dort seine Zugangsdaten einzugeben. Als Begründung für diese Dateneingabe werden oft Drohungen ausgesprochen, wie z.B. das Sperren des Benutzerkontos u.ä. Der o.g. Link führt allerdings auf eine gefälschte Webseite, welche dem Original oft täuschend echt nachempfunden wurde. Gibt der Benutzer nun auf dieser Seite seine Zugangsdaten ein, erhält der Urheber der Seite

diese Daten und kann sie nun missbrauchen. Um dem e-mail-Empfänger Echtheit vorzugaukeln, bedient man sich vieler Methoden, wie z.B. echt aussehende URL-Grafiken als Link, die Einbindung von Formularen und Skripten in die e-mail oder das Fälschen von Ziel-URLs, die sich optisch nicht von den Original-URLs unterscheiden.
Leider sind Online-Auktionshäuser machtlos bzgl. der Phishingmails, weswegen lediglich auf die Tatsache hingewiesen werden kann, dass vom Auktionshaus selbst nie solche Aufforderungen an die Benutzer gestellt werden. Dem kommt unter den drei genannten Beispiel-Auktionshäusern zumindest eBay nach.
Was allerdings sehr wohl von den Online-Auktionen beeinflusst werden kann, sind die Möglichkeiten von Phishing-Attacken aus der Plattform heraus. So können Verkäufer beim Einstellen eines Angebots den Artikel via HTML-Code beschreiben. HTML-Code bietet grundsätzlich auch u.a. die Einbettung von Skripten, mittels derer sich auch Phishing-Attacken durchführen lassen. Via HTML und Skripten können so Benutzerbewertungen und Elemente einer Angebotsseite insofern manipuliert werden, als dass zum einen das Bild des Verkäufers positiv verfälscht werden kann , zum Anderen kann der Käufer durch z.B. das Betätigen des Bieten-Buttons auf eine Pishing-Seite umgeleitet werden, um dort Benutzernamen und Passwort an den Verkäufer zu übermitteln.
Ein weiterer wichtiger Schritt zur Prävention vor Passwortklau ist das Integrieren von Software zur Erkennung von Passwortangriffen, z.B. Brute-Force-Angriffe, bei denen alle Buchstaben-, Zahlen- und Sonderzeichenkombinationen eines Passwortes systematisch durchprobiert werden.

Umsetzung

ricardo.ch Ricardo bietet die Möglichkeit, die Angebote via HTML-Code zu beschreiben, allerdings ist die Einbettung von Skripten und das Weiterleiten auf andere Seiten untersagt. Zu bemängeln ist der anscheinend fehlende Schutz vor Brute-Force-Angriffen, wodurch es Angreifern möglich ist, unter einem Benutzernamen vielfache Versuche, das Passwort herauszufinden, durchzuführen.

ebay.de Auch eBay bietet die Einstellung von Angeboten unter Verwendung von HTML-Code. eBay bietet zudem die Einrichtung einer so genannten „mich-Seite“, in der der Benutzer die Möglichkeit hat, sich selbst zu präsentieren.
Dabei dürfen auch Skriptsprachen verwendet werden. Da diese Optionen für betrügerische Machenschaften missbraucht werden können und auch wurden, sind mittlerweile die Einstellmöglichkeiten bzgl. des HTML-Codes insofern beschränkt, als dass einige ausgewählte HTML- und Skriptfunktionen nicht mehr gestattet sind (Pop-up-Fenster, Java-Script Includes, IFrames etc.).
eBay hat zum Thema „Phishing“diverse Hilfeseiten in ihr Portal eingefügt, die dem Benutzer die Gefahr und deren Abwehr näher bringen soll. Des Weiteren steht dem Benutzer eine kostenlose eBay-Toolbar zur Verfügung, die neben vielen Funktionen einen Sicherheitscheck integriert, der anhand eines Farbcodes zeigt, ob man sich auf einer von eBay, PayPal oder mobile.de geprüften Website befindet oder auf einer potenziell gefälschten. Allerdings wurde durch das Entwicklerteam Validome und Heise in einer Sendung von

„Stern TV“[pe], [he] schon einmal gezeigt, dass sich die Toolbar umgehen lässt. Diese bietet somit keinen sicheren Schutz. Des weiteren wird die Toolbar nur vom iExplorer unterstützt.
eBay integriert auch einen Schutz vor Brute-Force-Angriffen: Nach einer unbestimmten und zufälligen Anzahl von Anmeldefehlversuchen wird ein GIF-Bild im Login-Fenster eingeblendet, welches eine vierstellige Zahlenkombination beinhaltet. Diese Zahl wird bei jedem Login-Versuch neu generiert und mit wechselnder Schriftart, Farbe und wechselndem Hintergrund angezeigt. Der Nutzer muss zusätzlich zu seinen Login-Daten auch die vierstellige Zahl eingeben. Da es nicht so einfach möglich ist durch Programme die dargestellte Zahl aus dem GIF-Bild zu extrahieren, sollen so erschwerte Bedingungen für automatisierte Angriffe geschaffen werden.

atrada.de Atrada bietet ebenfalls die Möglichkeit, einen einzustellenden Artikel via HTML-Code zu beschreiben. Dabei werden aus Sicherheitsgründen einige HTML-Tags nicht erlaubt. Welche das sind und inwiefern Skriptsprachen erlaubt sind, war leider nicht zu eruieren. Die Einrichtung einer (wie bei eBay genannten) „mich-Seite“gibt es nicht, d.h. man bewegt sich für andere Benutzer anonym durch die Auktions-Plattform. Des Weiteren integriert Atrada einen Schutz vor Brute-Force-Attacken, der durch eine Login-Sperre von 5 Minuten nach fünfmaligem fehlgeschlagenen Login-Versuch realisiert wird.

6.2.4 Identitätsfeststellung

Um zu gewährleisten, dass sich hinter den persönlichen Angaben eines Benutzers einer Online-Auktion auch tatsächlich die beschriebene Person verbirgt, ist eine Verifikation der Angaben zur betreffenden Person notwendig. Es handelt sich also um die Zuordnung von Personalien (Identität) zu einer natürlichen Person. Diese Zuordnung hat bei Online-Auktionen eine große Bedeutung, da der hier abgewickelte elektronische Geschäftsverkehr ohne den persönlichen Kontakt zwischen Käufer und Verkäufer abgewickelt wird. Da der Diebstahl einer Identität bei Geldgeschäften großen Schaden verursachen kann, sind die Methoden, nach denen die Identität einer Person festgestellt wird, besonders wichtig und kritisch zu betrachten.

Verfahren zur Identitätsfeststellung

Sichere Verfahren

Erkennungsdienstliche Behandlung Hierbei werden, wie von der Polizei in aller Welt praktiziert, zur Personenfeststellung Fingerabdrücke abgenommen und ein Lichtbild angefertigt. Dieses Material kann dann mit amtlichen Aufzeichnungen verglichen werden. Die erkennungsdienstliche Behandlung gilt als sicherstes Verfahren zur Identitätskontrolle.

Postident Das von der Deutschen Post AG gegen Entgeld angebotene Postident-Verfahren realisiert die Identifikation einer Person durch die Übernahme der Ausweisdaten und die Einholung der Kundenunterschrift, wobei die Identifikation entweder direkt in der Filiale oder per Zusteller vorgenommen wird. Dabei genügt dieses Verfahren den Vorschriften des Geldwäschegesetzes und wurde vom TÜV IT als sicher beurteilt. Die Fehlerquote von Postident beträgt dabei ca. 1,1%. [po]

Unsichere Verfahren

Überprüfung der Kreditkarte Bei der Überprüfung der Identität einer Person durch das Einholen einer gültigen Kreditkartennummer wird davon ausgegangen, dass die Identität des Inhabers der Kreditkarte bei Eröffnung eines Neukontos in einem Bankunternehmen bereits vollständig verifiziert wurde. Ist die Kreditkarte gültig, wird davon ausgegangen, dass es sich um den richtigen Eigentümer der Kreditkarte, und somit um die richtige Person hinter dem Benutzernamen handelt.

SCHUFA Die SCHUFA Holding AG ist eine privatwirtschaftlich organisierte Auskunftei, welche nicht selbst Daten ermittelt, sondern sich diese von ihren Vertragspartnern liefern lässt. Auch hierbei wird von der SCHUFA keine eigene Identitätskontrolle durchgeführt. Durch eine SCHUFA-Auskunft wird lediglich die Kreditwürdigkeit von bekannt gegebenen Personalien eruiert, nicht aber die tatsächliche Übereinstimmung der Personalien mit einer Person. [sch]

Normale Briefsendung Um die postalische Anschrift einer Person zu bestätigen, wird oftmals ein postalischer Brief an die betreffende Person versandt, welche dann z.B. einen Freischaltcode o.ä. beinhaltet. So soll sichergestellt werden, dass die betreffende Person tatsächlich unter der angegebenen Adresse gemeldet ist und es sich hierbei nicht um falsche Daten zur Person handelt.

Umsetzung

ricardo.ch Ricardo führt bei neuen Mitgliedern eine Plausibilitätskontrolle durch. Dazu wird ein Brief nach dem ersten Auktionsgebot versendet, der einen Aktivierungscode beinhaltet, mittels dessen der Neukunde sein Benutzerkonto (und somit seine postalische Anschrift) bestätigen muss. Geschieht dies nicht innerhalb einer Frist von 30 Tagen, wird das Konto gesperrt.

ebay.de eBay verlässt sich bei der Verifikation einer Person auf eine SCHUFA-Auskunft. Um sich bei eBay anmelden zu können, bedarf es einer gültigen e-mail-Adresse. An diese Adresse wird ein Aktivierungslink verschickt, um das Benutzerkonto anzumelden. Normalerweise wird zusätzlich ein Aktivierungscode via Brief mit Passwort an die angegebene postalische Adresse versandt, um diese zu verifizieren. Dies geschieht aber nicht bei Kunden, deren e-mail-Adresse von bestimmten Providern, wie T-Online, AOL oder

MSN stammen, da davon ausgegangen wird, das besagte Provider die Korrektheit der Adressen bereits festgestellt haben. [wdr]
eBay bietet allerdings die freiwillige Möglichkeit, geprüftes Mitglied zu werden, wobei dann eine Verifikation der Person durch Postident vollzogen wird. Die Kosten sind vom Benutzer zu tragen.

atrada.de Die Identitätsfeststellung bei Atrada sieht eine telefonische Bestätigung der Benutzerdaten vor. Für die Anmeldung benötigt man eine gültige e-mail-Adresse. Laut Atrada werden Erstnutzer angerufen, um sich von ihnen die Korrektheit der Daten bestätigen zu lassen. [ia]

6.2.5 Bewertungssysteme

Das Bewerten von Käufern und Verkäufern nach Abwicklung eines Geschäftes dient der Selbstkontrolle zwischen den Mitgliedern einer Online-Auktionsplattform. Dabei können positive, neutrale oder negative Bewertungen nebst Begründung abgegeben werden. Dies soll helfen, das Gegenüber anhand der teils subjektiven, teils objektiven Erfahrungen und Bewertungen anderer Mitglieder einzuschätzen.

Abbildung 6.2: Bewertungsprofil bei eBay

Die Manipulation der Bewertungen bei Ricardo und Atrada lassen sich aufgrund des Verzichts von Skriptsprachen respektive des Verzichts auf persönliche Seite etc. wohl darauf beschränken, dass jemand durch getürkte Auktionen sein Bewertungsprofil aufbessert. Hier sollten aber interne Sicherheitsmechanismen greifen, um dieses zu unterbinden.
Bei eBay hatte man zumindest unter Verwendung von Skriptsprachen die Möglichkeit seine Bewertung so zu manipulieren, so dass dem Betrachter ein falsches Bild vorgeführt wurde. Inwiefern nach der Überarbeitung der Skript- und HTML-Möglichkeiten dies noch möglich ist, ist unklar. Da aber immer noch nicht auf Skriptsprachen und interne Verlinkung verzichtet wird, bestehen sicherlich immer noch Möglichkeiten der Manipulation.

6.2.6 Sicherheitsverbindung

eBay, Atrada und Ricardo bieten beim Anmelden eines Benutzers auf ihren Plattformen eine SSL-Verbindung zur Gewährleistung der Datensicherheit. SSL (Secure Sockets

Layer) ist eine Entwicklung der Netscape Communications Corp. und arbeitet auf Socket-Ebene zwischen Anwendungs- und Transportschicht. SSL unterstützt verschiedene kryptographische Verfahren mit variablen Schlüssellänge. Eine SSL-Verbindung ist anhand der URL zu erkennen, da sich dort das „http://“ in „https://“ ändert. [ssl] Bei Ricardo hat der Benutzer die Möglichkeit, eine SSL-Verbindung beim Einloggen zu aktivieren, d.h. wenn er sich über den Link „MyRicardo“ (äquivalent zu eBays „Mein eBay“) auf der Plattform einloggt. Bei Gebotsabgaben, bei denen ein vorheriges Einloggen nicht stattfand, wird auch keine SSL-Verbindung angeboten bzw. aktiviert. Dies geschieht bei eBay und Atrada automatisch, und zwar immer dann, wenn ein Benutzer Benutzernamen und Passwort eingeben muss, also nicht nur beim expliziten Einloggen (über den Link „Einloggen“ bei eBay bzw. „Mein Marktplatz“ bei Atrada).

6.2.7 Fazit

Der Benutzer einer Online-Auktion stellt mit der Wahl seines Passworts ein großes und nicht zu verachtendes Risiko für sich selbst dar (siehe Abschnitt „sichere Passwörter“). Um diesem Sicherheitsrisiko entgegenzuwirken, kann man leicht bei der Neuanmeldung von Benutzern (oder später bei der Änderung von Passwörtern) einen Sicherheitscheck integrieren, der das gewählte Passwort überprüft und gegebenenfalls ablehnt, falls dies zu unsicher erscheint. Diesem Prinzip folgen die Auktionsplattformen Ricardo und eBay bereits und bieten somit ihren Kunden den Service eines „sicheren“ Passwortes. Das Negativbeispiel kann hier durch das Auktionshaus Atrada angeführt werden, die bzgl. der Passwortsicherheit leider keine Überprüfung vorsieht, und somit dem Passwortklau nichts entgegenbringt. Generell (das gilt nicht nur für Online-Auktionen) sollte man als Benutzer auf Tools zurückgreifen, welche Passwortgenerator und -verwaltung zusammen realisieren (z.B. *1Password Pro 4.0* oder *Any Password 1.43*), um „schwache“ und mehrfach verwendete Passwörter zu vermeiden.
Das Engagement von eBay bzgl. der Aufklärung der Nutzer über Phishing ist beispielhaft und lässt zumindest hoffen, dass in Zukunft weniger Kunden auf solche Attacken hereinfallen. Warum eBay allerdings weiterhin nicht auf den Unsicherheitsfaktor Skript verzichtet, bleibt fraglich. Hierbei handelt Ricardo insofern sicher, als dass Skriptsprachen und weiterführende Links in Angebotsbeschreibungen komplett verboten sind. Mit Ausnahme von Ricardo wurden ebenfalls Sicherheitsmechanismen zur Abwehr respektive Einschränkung von Passwortangriffen vorgenommen. Allerdings ist zu berücksichtigen, dass diese nur greifen, wenn jemand „zu oft“ versucht, ein Passwort zu knacken. Die o.g. Maßnahmen zur Vorbeugung von Brute-Force-Angriffen lassen sich umgehen, indem nicht versucht wird, einen Account mit vielen Passwörtern zu knacken, sondern mittels weniger, leichter Passwörter irgendeinen Account. Unternimmt man dabei immer nur eine geringe Anzahl von Versuchen, und zwar so viele, wie zulässig sind, schlägt der Angriffsschutz nicht zu und die Attacke wird auf Serverseite nicht registriert. Hier müssen also andere Mechanismen her, wie z.B. das Überwachen und gegebenenfalls das Sperren von IP-Adressen. Dies könnte leider die Folge haben, dass man so eventuell ein ganzen Unternehmensnetz ausschließt, welches sich hinter einem Proxy verbirgt. Auch das Filtern von Angebotsseiten (wie es durch die Online-Auktionsplattformen auch rea-

lisiert wird), die via HTML-Code erstellt wurden, bietet Schutz vor Pishing-Angriffen. Allerdings ist ein Filter immer nur so gut wie der Programmierer, der ihn geschrieben hat. Es ist nicht davon auszugehen, dass sämtliche Tricks und Versuche von potentiellen Angreifern durch Filter ausgemacht werden können, was eine dynamische Anpassung der Filtermechanismen erfordert. Oft hat allerdings die Vergangenheit gezeigt, dass sich z.B. die Auktionsplattform eBay auf ihren Sicherheitsmechanismen ausruhte und potentielle Gefahren als „nur theoretisch“ deklassierte.
Zu guter letzt bleibt zu bemängeln, dass keine der 3 Auktionsplattformen eine sichere Identifikationskontrolle bei der Anmeldung eines Accounts realisiert. Lediglich bei eBay kann man sich durch das Postident-Verfahren identifizieren lassen, was allerdings keine Pflicht ist. Somit kann in keiner der Online-Auktionen mit relativ hoher Sicherheit die Identifikation einer Person garantiert werden. Es blieb z.B. auch der zu erwartende Telefonanruf von Atrada aus. Bei einem Versuch der Neuanmeldung wurden falsche Angaben zur Person gemacht, wobei das Benutzerkonto offiziell bestätigt und aktiviert wurde, ohne dass eine telefonische oder postalische Verifikation der Daten erfolgte. Hier sollten alle drei Auktionshäuser ihre Strategie überdenken. Schon ein einfaches Abfragen und Überprüfen der Kontodaten eines Benutzers bei der Anmeldung könnte das Verkaufen unter falscher Identität einschränken, da so Unterschiede zwischen Anmeldenamen und Kontoinhaber erkannt und unterbunden werden können. Auch die Verifikation der Identität durch Postident (welches als einziges, sicheres Verfahren zur Identitätsfeststellung bei Online-Auktionen in Frage kommen dürfte) sollte, nach Meinung der Autoren, mehr als nur freiwilliger Natur sein. Abschrecken dürften hierbei allerdings der Aufwand und die Kosten sein, die an die Benutzer entfallen.

6.3 Vertragliche Situation

Dieser Abschnitt befasst sich mit der rechtlichen Handhabung von Online-Auktionen. Dabei geht es vorrangig um die Problematiken, wie Online-Auktionen juristisch einzuordnen sind und welche Rechte und Pflichten für die beteiligten Parteien gelten. Hierzu werden in den einzelnen Teilabschnitten typische Fragen zum Thema „Versteigerung im Internet“behandelt, beispielsweise

- Sind Online-Auktionen Auktionen im klassischen Sinn?
- Welche Rechten und Pflichten haben die Plattformanbieter?
- Gibt es ein Widerrufsrecht bzw. Rücktrittsrecht?
- Welche Richtlinien gelten für Bewertungen?
- Wie ist die Beweislage beim Rechtsstreit?

6.3.1 Online-Auktionen vs. Klassische Auktionen

Bei dem Begriff „Auktion“denken viele Leute in erster Linie an den Zuschlag, den der Auktionator mittels des Hammers erteilt. Betrachtet man Auktionen allerdings genauer, geht es hierbei um einen Mechanismus der Preisfindung für den Verkauf von Waren. Ein Verkäufer gibt für einen Artikel ein Verkaufsangebot ab, indem er ihn mit einem Mindestgebotspreis zur Versteigerung freigibt. Der potentielle Käufer nimmt dieses Angebot an, indem er seinerseits ein Gebot für den Artikel abgibt. Wer letztendlich den Zuschlag für die Ware erhält, das entscheidet der Hammerschlag des Auktionators. Es wird deutlich, dass während dieses Prozesses eine Situation entsteht, bei der die Beteiligten einem hohen Stressfaktor ausgesetzt sind. Schließlich geht es für Versteigerer und Bieter darum, denn größtmöglichen Profit zu erzielen.
Die Rechtssprechung ist sich dieser Situation bewusst, und so werden klassische Auktionen im Artikel „Versteigerergewerbe“[GewO§34b] und in der Versteigerungsverordnung [VerstV] gesondert geregelt. Als wesentliches Merkmal einer klassischen Auktion wird die örtliche und zeitliche Begrenzung, in der die Versteigerung stattfindet, angesehen. Es gilt also zu beachten, dass die Beteiligten unter einem künstlich hergestellten Druck agieren. Um dabei voreiliges Handeln vorzubeugen, müssen bei Auktionen die Waren den Bietern im Voraus zugänglich gemacht werden. Somit haben diese Gelegenheit, sich vom Zustand und dem ungefähren Wert einen Eindruck zu verschaffen. Dabei ist die Versteigerung „ungebrauchter“Waren verboten, soweit man sie regelmäßig im Einzelhandel kaufen kann (§34b Abs. 6 Nr. 5b GewO), da sonst Auktionen in direkter Konkurrenz zum Einzelhandeln stehen könnten. Versteigerungen müssen mindestens 2 Wochen vorher bei der zuständigen Behörde angemeldet und durch diese genehmigt werden. Dabei gilt an Sonn- und Feiertagen grundsätzliches Auktionsverbot.
Zwar ähnelt der Ablauf der Preisfindung bei Online-Auktionen dem klassischer Auktionen, allerdings entfällt durch die weltweite Verbreitung des Internets eine örtliche Begrenzung. Auch der zeitliche Druck ist weniger verschärft, da sich Online-Auktionen gewöhnlich über mehrere Tage erstrecken und der Zeitpunkt des Zuschlags bereits beim Auktionsstart bekannt ist. Aufgrund dieser Tatsachen hat sich bei den Gerichten die Meinung durchgesetzt, Online-Auktionen nicht als klassische Auktionen, sondern als „Verkauf gegen Höchstgebot“einzustufen. Folglich entfällt für eine Online-Auktion die behördliche Anmeldepflicht, das Auktionsverbot an Sonn- und Feiertagen, sowie Verkaufsverbot von Neuwaren.

6.3.2 Vertragsverhältnisse bei Online-Auktionen

Bei einer erfolgreichen Versteigerung im Internet sind immer mindesten drei Parteien beteiligt, nämlich der Betreiber der Auktionsplattform, der Anbieter der Ware und der Höchstbietende. Der Betreiber erbringt gegenüber dem Anbieter und den einzelnen Bietern eine Dienstleistung, indem er ihnen die Möglichkeit gibt über seine Auktionsplattform zueinander zu finden. Somit entsteht ein Benutzerverhältnis zwischen ihm und den Nutzern der Plattform. Die Rechte und Pflichten dieses Verhältnisses sind in dem Teilnehmervertrag des jeweiligen Betreibers festgelegt, den jeder Nutzer bei der Regis-

trierung akzeptieren muss. Zwischen den Nutzern, die an einer Auktion beteiligt sind, besteht eine Art Marktverhältnis, denn hier findet der eigentliche Handel bzw. Leistungsaustausch statt. Nach Ablauf der Auktion kommt es zum Vertragsschluss zwischen beiden Parteien. Da es sich in den meisten Fällen um Kaufverträge handelt, wird lediglich auf diese im Folgenden eingegangen. Aber auch die Schließung anderer Verträge, wie Mietverträge und Leasingverträge, ist erdenklich.
Eine scheinbare Ausnahme bilden unternehmenseigene Auktionen der Betreiber. Zu Unterscheiden ist aber, dass man mit dem Unternehmen handelt welches ebenfalls die Dienstleistung anbietet. Der Betreiber als solcher tritt nicht als Händler über seine Auktionsplattformen in Erscheinung.

Das Teledienstgesetz (TDG)

Da grundsätzlich alle Gesetze der realen Welt auch im Internet ihre Anwendung finden, wären Anbieter von Internetdiensten schadensersatzpflichtig, wenn ihre Inhalte die Rechte Dritter verletzen. Das würde beispielsweise bedeuten, der Plattformbetreiber haftet in vollem Umfang für die Inhalte aller Artikelbeschreibungen auf seinen Webseiten. Der Gesetzgeber hat diese Haftbarkeit durch das TDG eingeschränkt, denn er sieht es als erwiesen an, dass durch die technischen Möglichkeiten der Vervielfachung eine Überwachung solcher Inhalte für die Dienstanbieter unzumutbar ist. Dabei unterteilt das TDG Inhalte der angebotenen Dienste in zwei Gruppen: Die eigenen Informationen der Dienstanbieter und fremden Informationen der Dienstnutzer, die durch den Anbieter lediglich bereitgestellt werden.
Für eigene Informationen liegt die volle Verantwortlichkeit nach §8 Abs.1 TDG beim Dienstanbieter. Das heißt, er kann für resultierende Schäden solcher Inhalte in vollem Umfang belangt werden. Dazu zählen auch Informationen Dritter, die sich der Dienstanbieter zueigen gemacht hat.
Für fremde Informationen sind Dienstanbieter generell nicht verantwortlich (§9 Abs.1 TDG). Sie sind auch nicht verpflichtet, Inhalte vor oder während der Bereitstellung auf Rechtverstöße zu prüfen bzw. nachzuforschen, ob diese Rechtsverstöße zur Folge haben können. Letztendlich sind Dienstanbieter nach §11 TDG nur dann zu einem Entfernen oder Sperren der Informationen verpflichtet, wenn sie durch Dritte auf gegebene Rechtswidrigkeiten hingewiesen werden. [TDG]

Haftbarkeit des Plattformbetreibers

Ob das TDG sich auf Online-Auktionen anwenden lässt, war lange Zeit umstritten. Bei unternehmenseigenen Auktionen ist der Fall klar, denn ähnlich dem Versandhandel werden eigene Waren auf der eigenen Webseite angeboten. Die Verantwortung für die Inhalte liegt also beim Betreiber, egal ob es sich dabei um einen Festpreishandel oder eine Auktion handelt.
Üblicherweise stammt bei Online-Auktionen die Beschreibung der Angebote jedoch nicht vom Betreiber, sondern von den Nutzern. Es scheint sich also generell um fremde Informationen zu handeln, womit sich der Betreiber jeglicher Verantwortung entziehen

kann. Fraglich ist, ob sich der Betreiber die Inhalte zueigen macht. Dafür würden die Abhängigkeit der Gebote nach der Artikelbeschreibung und die Berücksichtigung des Höchstgebots bezüglich der Prämienberechnung sprechen. Zudem stellen die Betreiber häufig Tools zur Verfügung die den Handel zusätzlich fördern sollen.
Der Bundesgerichtshof lehnte diese Umstände als Indiz einer Zueigenmachung ab. Im konkreten Rechtsstreit ging es um eine Schadensersatzklage des Uhrenherstellers „Rolex"gegenüber dem Plattformanbieter „eBay"wegen Markenverletzung (Urt. v. 11.03.2004, Az. I ZR 304/01, NJW2004, 3102 ff.).[III ZR 96/03] Die Richter zogen lediglich einen Unterlassungsanspruch in Erwägung, da die Markenverletzung erst die die Bereitstellung der Handelsplattform ermöglicht wurde. Allerdings setzt das voraus, dass eine Verletzung der Prüfpflichten vorliegt, die wiederum vom BGH nicht definiert wurden.
EBay ergriff darauf die Initiative und gründet mit VeRI (Verifizierte Rechte Inhaber) ein Programm zum Schutz von Markenrechten. Inhabern von Schutzrechten prüfen eigenständig Auktionen auf Markenrechtsverletzungen und melden diese ggf. an den Betreiber. Der Betreiber sperrt diese Auktionen mit sofortiger Wirkung und erklärt sich bereit, registrierten VeRI - Mitgliedern die Personendaten des Anbieters, wie Name und Anschrift, zugänglich zu machen. Ziel ist es also, die Überprüfung von Verstößen auf die Betroffenen zu verlagern und ihnen im Gegenzug rechtliche Maßnahmen gegen die Täter zu ermöglichen.

Kaufverträge der Nutzer

Wollen sich zwei Parteien zu gegenseitigen Tun und Unterlassen verpflichten, schließen sie einen Vertrag. Das gilt sowohl in der realen Welt wie auch in der Welt des Internets. Dazu gibt jeder der Beteiligten eine Willenserklärung ab, in Form eines Angebots und einer Annahme. Die Rechtsgrundlage solcher Verträge ist in den §§ des BGB gegeben. Die AGB der Betreiber spielt hier keine Rolle, denn wie bereits erwähnt nimmt dieser nicht am Handel zwischen dem Anbieter und dem Höchstbietenden teil. Sie werden aber oftmals zur Urteilsfindung hinzugezogen, um die Abläufe der Vertragsentstehung zu klären.
Strittig ist nun, wann eine Willenserklärung als solche zur Erkennen ist. Laut BGB bedarf es dazu keiner ausdrücklichen Erklärung seitens der Parteien. Es genügt, wenn eine Erklärung durch das Verhalten der Beteiligten ersichtlich wird. So können rechtswirksame Willenserklärungen auch durch Mausklicks und die daraus resultierende Übermittlung von Daten entstehen.
Des Weiteren ist klarzustellen, wie eine abgegebene Erklärung zu interpretieren ist. Zu könnte die Freischaltung der Webseite mit der Artikelbeschreibung als Angebot gelten und die abgegebenen Gebote darauf als Annahmen. Demzufolge würde aber schon mit dem ersten Gebot ein Vertrag zustande kommen. Betrachtet man wiederum die Gebote als Angebot zum Vertragsschluss, so dass nach Auktionsablauf die Annahme des Höchstgebots durch den Anbieter erfolgt, hätte dieser stets die Möglichkeit, die Annahme zu verweigern (zum Beispiel wegen eines zu niedrigen Preises).
Die Antwort auf diese Problematik gab der BGH im Falle einer Versteigerung, bei der ein VW Passat weit unter dem handelsüblichen Preis ersteigert wurde. [VIII ZR 13/01]

Für Online-Auktionen gilt somit, dass der Anbieter mit Freischalten des Artikels eine Annahmeerklärung abgibt, wobei er das Höchstgebot des Artikels akzeptiert. Die Bieter erklären mit ihren abgegeben Geboten ein Angebot, den Artikel zum jeweiligen Preis zu kaufen. Das bedeutet, dass bei Ablauf der Auktionsfrist automatisch ein Vertrag zustande kommt, einerseits durch das Angebot des Höchstbietenden und anderseits durch die Annahmeerklärung des Anbieters. Selbst wenn es dabei zu derart niedrigen Preisen kommt, die als sittenwidrig gelten, bleibt der Vertrag gültig. Die Preisfindung bei Auktionen (auch bei Online-Auktionen) wird dabei als idealtypischer Mechanismus zur Bildung von Marktpreisen angesehen.

Widerruf & Rücktritt vom Kauf

Zum Schutz der Verbraucher beim Handel über Fernkommunikationsmittel gibt es das Widerrufs- bzw. Rücktrittsrecht. Demnach besteht als Privatperson gegenüber einem gewerblichen Händler die Möglichkeit binnen 14 Tagen ohne jegliche Begründung den Kauf der Waren rückgängig zu machen (§§312b ff. BGB). Zwar ist dieses Recht für Auktionen ausgeschlossen [BGB§312d], allerdings bezieht sich dies auf Auktionen im klassischen Sinn.
Bei der Anonymität der Nutzer bei Online-Auktion stellt sich nun oft die Frage, ob es sich um einen Händler oder eine Privatperson handelt. Die Aufforderung der Plattformbetreiber, Händlertätigkeiten anzugeben, kann lediglich als Appell angesehen werden. Eine Verpflichtung zur Angabe besteht nicht.
Die Klärung, ob ein Nutzer als gewerblicher Händler zuzuordnen ist, kann mittels der Anzahl der Transaktionen binnen eines bestimmten Zeitraums nicht eindeutig erfolgen. Sollten Privatpersonen sich durch gegebene Anlässe (z.B. Entrümpeln des Speichers) dazu entschließen, mehre Versteigerungen per Online-Auktion zu starten, würden sie fälschlicherweise als Unternehmen angesehen. Da dieses Kriterium also nicht ausreicht, gelten weitere Indizien wie

- Die Regelmäßigkeit der Transaktionen über einen längeren Zeitraum
- Die hohe Anzahl der Verkäufe
- Das mehrfache Anbieten gleicher Artikel
- Das Anbieten von Neuwaren
- Das gleichzeitige Anbieten einer Vielzahl von Artikeln

Je mehr dieser Kriterien erfühlt sind, umso eindeutiger ist eine gewerbliche Tätigkeit erwiesen.[Uelzen2005]

6.3.3 Bewertungen bei Online-Auktionen

Da Bewertungen als wichtiger Anhaltspunkt für das Handlungsverhalten gelten, sind gerade Anbieter um eine markelose Bewertungsliste bestrebt. Sollte es vorkommen, dass

man eine negative Bewertung erhält, kann man diese zwar kommentieren, doch die Weste bleibt eben für zukünftige Transaktionen „befleckt“. Zumal solche Bewertung auch aus Revanche oder Missgunst abgegeben werden, besteht der Wunsch nach gänzlicher Entfernung.
Das AG Koblenz sah in einem Urteil (Urt. v. 2.4.2004, Az. 142 C 330/04, MMR 2004, 638f.) [142 C 330/04] das Bewertungsforum als Meinungsforum an, so dass ein Löschungsanspruch lediglich bei beleidigender Schmähkritik oder bei offensichtlichen unwahren Behauptungen bestünde. Hingegen meinte das AG Erlangen (Urt. v. 26.5.2004, Az. 1 C 457/04) [1 C 457/04], die Abgabe einer sachlich richtigen Bewertung sei vertragliche Nebenpflicht, so dass unbegründete Abwertung ohne sachliche Rechtfertigkeit einen Löschungsanspruch genügen.

6.3.4 Beweislast bei Vertragsschluss

Kommt es bei Abschluss eines Vertrages zum Streitfall, der eine gerichtliche Durchsetzung von Ansprüchen verlangt, ist die Frage der Beweislast von zentraler Bedeutung. Schließlich beruhen richterliche Entscheidungen auf Tatsachen, die für gewöhnlich seitens des Klägers zu beweisen sind. Klingt es nicht eine nachvollziehbare und begründete Beweisführung zu erbringen, ist die Klage als gescheitert zu betrachten.
Häufig geht es bei solchen Rechtsfällen um Zahlungsforderungen der Anbieter gegenüber dem Höchstbietenden. Doch welche Beweismöglichkeiten hat der Anbieter als Kläger hierbei, wenn der Bieter die Abgabe des Gebots bestreitet? Da die Abwicklung der Online-Auktionen gewöhnlich über den Versand von Emails geschieht, sind diese meist der einzige Ansatzpunkt. Allerdings handelt es sich meist um generierte Emails der Plattformbetreiber ohne jegliche Signatur. Die Beweisgültigkeit ist somit stark eingeschränkt, denn es kann lediglich der Versand der Email über den Nutzer-Account, aber nicht die eindeutig Identität des Nutzers bewiesen werden. Als weiteres Beweismittel bleibt letztlich nur die Angabe des Nutzer-Accounts samt Passwort um den vermeintlichen Bieter zu identifizieren. Aber auch ist die Eindeutigkeit als Beweis umstritten.
So gab es in der Vergangenheit mehrere Prozesse, die zwecks mangelnder bzw. mangelhafter Beweise verloren wurden. [2 O 450/00, 2 O 472/03] Die Aufführung des Email-Verkehrs und die Angabe von Nutzer-Account und Passwort reichten den Richtern für gewöhnlich nicht aus. Sie begründeten ihre Entscheidung mit der Unsicherheit der Email-Kommunikation und der Vielfältigkeit des „Identitätsdiebstahls“im Internet. Weiterhin sahen sie es als erwiesen an, dass ein Missbrauch von Nutzerzugängen und Email-Konten als reale Gefahr einzustufen sei, womit diese als Beweismittel nicht anzuführen sind.
Es wird deutlich, dass somit böswilligen Bietern Tür und Tor geöffnet werden. Schließlich können sie beim Abstreiten der Gebotsabgabe den Anbieter in eine nahezu aussichtlose Beweislage versetzen. Auch wenn die o. g. Urteile Einzelfallentscheidungen waren, setzen sie doch Richtwerte für die Zukunft. Um den generellen Missbrauch dennoch einzuschränken, ziehen die Gerichte auch folgende Umstände unter Betrachtung:

- Hat der Beklagte bereits negative Bewertungen wegen Nichterfüllung

- Gab bereits vorher Missbrauchsfälle des Beklagten, vorauf keine Änderung des Passworts erfolgte
- Kaufte der Beklagte vorher mehrere gleichartige Artikel
- War die Zeitspanne zwischen Gebotsabgabe und Auktionsende groß genug, um den Missbrauch festzustellen
- Hatte der Beklagte während der Auktion Kontakt zum Kläger

6.3.5 Fazit

Grundsätzlich gibt es keine Gesetze und Paragraphen, die den Handel über Online-Auktionen regeln. Es liegt also in den Entscheidungen der Gerichte wie die Normen der Versteigerung auf die Welt des Internets abzubilden sind. Positiv ist dabei die kritische Berücksichtigung der Sicherheitsmängel anzusehen, denen sich die Richter durchaus bewusst sind. Doch leider bleiben viele Fragen offen oder werden nicht genau beantwortet wie beispielsweise die Prüfungsvorschriften für Plattformbetreiber bezüglich ihrer bereitgestellten Webseiten. Letztendlich hat sich dennoch im Laufe der vergangenen Jahre ein Trend entwickelt, an dem die Betroffenen eine Antwort auf prinzipielle Fragen erhalten. Leider konnte in diesem Abschnitt nur ein grober Überblick über einige rechtliche Schwerpunkte gegeben werden. Es wurde versucht, mit der Einordnung der Online-Auktionen und der Klärung der Vertragsverhältnisse dem Leser einen Einstieg in die Problematik zu vermitteln. Schließlich bleiben tiefgründige Fragen offen, wie die Anfechtbarkeit von Verträgen und die Rücknahme von Geboten.
Buchtipp: Wer sich vertiefend mit der vertraglichen Situation bei Online-Auktionen beschäftigen möchte, dem sei an dieser Stelle das Buch „Internet-Auktionen bei eBay & Co.“(ISBN 3-423-50636-9) von Carsten Uelzen und Thomas Burmester empfohlen. Die Autoren setzten sich sehr gut mit der rechtlichen Situation der Online-Auktionen auseinander und bieten auch Tipps rund ums Ver- und Ersteigern.

6.4 Zusammenfassung

Online-Auktionen haben sich im Laufe der Zeit zu einem festen Bestandteil der Internetaktivität entwickelt und zählen neben Email-Kommunikation, Recherchen, Online-Banking, etc., zu einer seiner Hauptanwendungen. Jedoch stellt die Abwicklung von Geschäftsprozessen hierbei hohe Sicherheitsanforderungen, denn offensichtliche Sicherheitslücken und die daraus resultierenden Schäden können von schwerwiegendem Ausmaß für die Betroffenen sein. Im Interesse der Nutzer sind somit Sicherheitsmaßnahmen erforderlich, die den Ablauf der Online-Auktionen schützen. Mit „eBay“, „ricardo“und „atrada“haben sich drei Betreiber von Auktionsplattformen als Marktführer hervorgetan. Mit ihrer führenden Position auf diesem Gebiet über nehmen sie eine Beispielrolle zum Thema „Sicherheit bei Online-Auktionen“. Doch gerade das macht sie auch zur Zielscheibe illegaler Attacken.
Phishing und Passwortklau zählen dabei fast zur Tagesordnung und wie so oft, liegt das größte Sicherheitsrisiko beim Anwender selbst. Durch leichtfertiges Vertrauen und unüberlegtes Handeln ermöglichen viele User den Angreifern einfaches Spiel. Die Plattformbetreiber versuchen diesen Umstand ihren Kunden bewusst zu machen mittels Mechanismen zur Passwortvergabe und Benutzerregistrierung. Leider werden viele dieser Verfahren nur optional angeboten und sind nicht verpflichten, so dass auch hier keine umfassende Absicherung erfolgt. Die Anbieter müssen sich also den Vorwurf gefallen lassen, weitaus mehr zur Sicherheit ihrer Auktionen betragen zu können.
Auch an den Gerichten zählen Online-Auktionen zum festen Bestandteil des Alltags. Mit der gewerblichen Einordnung gegenüber der klassischen Auktion und der bisherigen Urteilssprechung wurde eine Grundlage für die juristische Handhabung geschaffen. Die Schwierigkeit der Abbildung der gesellschaftlichen Normen auf Online-Auktionen liegt dabei in den technischen Möglichkeiten des Internets und der generellen Brisants zum Thema „Sicherheit“. Dennoch scheint es den Richtern gelungen zu sein, einen Trend für zukünftige Rechtssprechungen aufzuzeigen, selbst wenn noch viele Fragen offen sind.

Literaturverzeichnis

[ebay] eBay Deutschland

[ricardo] Ricardo

[atrada] Atrada

[pe] @t-mix News zum Thema „eBay“

[he] Heise Artikel „eBay-Passwortklau“

[epr] Presse-Service-Center von eBay zum Thema „Sicherheit bei eBay“

[ct1] „Ohne Gewalt“ c’t-Ausgabe 15/04, Seite 214-215

[ct2] „Um den guten Ruf“ c’t-Ausgabe 07/04, Seite 80-81

[ct3] „Passwort-Diebstahl“ c’t-Ausgabe 01/05, Seite 28

[ia] Tecchannel Atrikel: „Test: Online-Auktionen“

[sch] SCHUFA

[po] Postident

[ssl] Informationen zu SSL

[wdr] Bericht von wdr.de über eBay-Sicherheit

[Uelzen2005] *Internet-Auktionen bei eBay & Co.* von C.Uelzen & T.Burmester, 2005

[irr] Internerrecht-Rostock.de

[er24] e-Recht24.de

[GewO§34b] GewO § 34b Versteigerergewerbe

[VerstV] Versteigererverordnung

[TDG] Gesetz über die Nutzung von Telediensten

[BGB§312d] Widerrufs- und Rückgaberecht bei Fernabsatzverträgen

[III ZR 96/03] Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr

[VIII ZR 13/01] Wirksamer Vertragsschluss bei Online-Auktionen

[142 C 330/04] Ebay - Entfernung missbräuchliche Bewertung

[1 C 457/04] Ebay - Entfernung missbräuchliche Bewertung

[2 O 450/00] Beweislastumkehr & Anscheinsbeweis

[2 O 472/03] Beweislastumkehr & Anscheinsbeweis

7 Elektronisches Publizieren

Kerstin Seidel, Maximilian Seifert

7.1 Einleitung

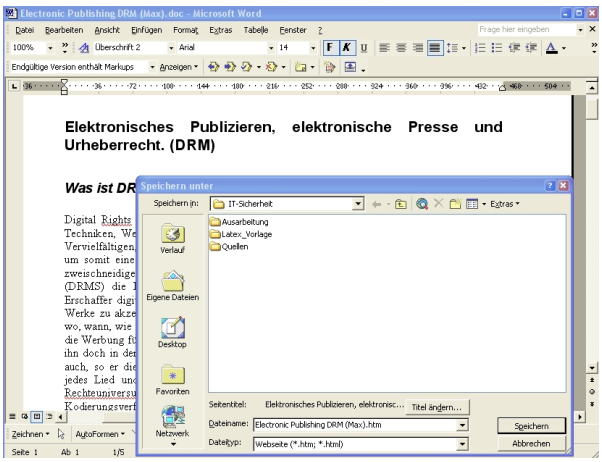
Diese Ausarbeitung entstand für das Seminar „Trust Management und Security Policy Enforcement“ an der Universität Potsdam und beschäftigt sich mit dem elektronischen Publizieren, der elektronische Presse und dem Urheberrecht. Zum Schutz dieser digitalen Inhalte werden die Grundlagen des Digital Rights Management (DRM) betrachtet. Dabei können wir jedoch (aufgrund des eingeschränkten Umfangs dieser Ausarbeitung) DRM nicht in seiner vollen Tiefe vorstellen sondern lediglich einen Überblick über die Standards und Verfahren geben.

7.2 Elektronisches Publizieren

Unter elektronischen Publikationen versteht man Veröffentlichungen, die zur Darstellung elektronische Medien verwenden. Zu unterscheiden sind dabei On- und Offline-Publikationen, also solche, die das Internet nutzen oder auf lokalen Datenträgern (CD-ROM, DVD, Diskette, ...) veröffentlicht werden.[1]
Es gibt eine Vielzahl an Möglichkeiten, Informationen für das elektronisch Publizieren aufzubereiten. Wir stellen hier kurz einige Möglichkeiten vor, ohne jedoch tiefer auf diese einzugehen. Dabei handelt es sich um Softwarelösungen, deren erstellte Inhalte sich für das Publizieren im Internet anbieten. Offline-Publikationen werden von uns nicht weiter betrachtet, da die für Online-Publikationen erstellten Inhalte ohne weiteres auch im Offline-Bereich eingesetzt werden können.

7.2.1 Microsoft Word

Die wohl einfachste Möglichkeit unter Microsoft Windows einen Text für eine Online-Publikation aufzubereiten, ist den Text unter Word zu schreiben und als Webseite abzuspeichern.



1. als Website unter Word speichern

```
</head>

<body lang=DE link=blue vlink=purple style='tab-interval:35.4pt'>

<div class=Section1>

<h1>Elektronisches Publizieren, elektronische Presse und Urheberrecht. (DRM)</h1>

<p class=MsoNormal><o:p> </o:p></p>

<h2>Was ist DRM?</h2>

<p class=MsoNormal><o:p> </o:p></p>

<p class=MsoNormal>Digital <span class=SpellE>Rights</span> Management (oder
kurz DRM) ist ein Oberbegriff für eine Sammlung von Techniken, Werkzeugen und
Formate, die den Zugriff, d.h. im Speziellen das Abspielen, Vervielfältigen,
Übertragen, Zitieren, etc. auf die digitale Werke bzw. Werte steuern sollen, um
somit eine sichere Verbreitung und Verwertung zu ermöglichen. Dabei ist DRM ein
zweischneidiges Schwert: Zum einen sind durch Digital <span class=SpellE>Rights</span>
Management Systeme (DRMS) die Rechteinhaber, also die großen Plattenfirmen,
Filmstudios, allgemein die Erschaffer digitaler Werte überhaupt erst bereit,
das Internet als Distributionskanal für ihre Werke zu akzeptieren. Durch
```

2. der automatisch generierte HTML-Quelltext

Die Informationen in der automatisch generierten Webseite können nun über einen Webserver im Internet publiziert werden.

7.2.2 Adobe FrameMaker

Adobe FrameMaker ist eine professionelle Authoring- und Publishing-Lösung für Unternehmen (Einzelpreis 1.599,64 EUR). Dank WYSIWYG-Unterstützung (What You See Is What You Get) und einer auf Schablonen basierenden Umgebung ermöglicht Adobe FrameMaker die Erstellung skalierbarer Dokumente aus einer einzigen Quelldatei. Es können beliebige Dokumente erstellen werden, von kurzen Texten bis hin zu mehrbändigen Büchern. Einmal erstellte Dateien können auf vielfältige Art und Weise veröffentlicht werden, z.B. als gedruckte Dokumente sowie im Adobe PDF-, HTML-, SGML- oder XML-Format. In diesen Formaten eignen sich die Dokumente hervorragend zum Publizieren im Internet oder auf Datenträgern. Adobe bietet mit dem FrameMaker 7.1 zusätzlich die Möglichkeit, elektronische Dokumente Sehbehinderten zugänglich zu machen und auf Handhelds anzuzeigen.

7.2.3 XSL-FO (XSL Formatting Objects)

XSL-FO ist Teil der Extensible Stylesheet Language (XSL), welche als allgemeine Stylesheet-Sprache für XML Dokumente erdacht worden ist. XSL besteht grundlegend aus zwei Teilen:

- einer Sprache, um XML Dokumente zu transformieren
- einen XML Vokabular, um die Semantiken der Formatierung zu spezifizieren

Ein XSL Stylesheet Processor ist in dem Zusammenhang ein Programm, welches ein Dokument oder Daten in XML und eine XSL Stylesheet entgegennimmt, um eine Darstellung der XML Quelle zu erzeugen. Dieser Darstellungsprozess lässt sich in zwei Schritte

untergliedern: die Umwandlung eines XML Quellbaumes in einen gewünschten Ergebnisbaum, sowie die anschließende Interpretation des Baumes. Die formatierten Ergebnisse sind dann für die jeweilige Darstellung auf beliebigen Medien geeignet.
Der erste Schritt nennt sich Tree Tranformation und wird von einem Formatter ausgeführt. Der zweite Schritt nennt sich Formatting und kann z.B. durch eine spezielle Rendering-Engine im Browser bewerkstelligt werden. Die Tree Transformation erlaubt die weitgehende Umformung der Struktur eines XML Dokumentes. So kann etwa ein Inhaltsverzeichnis erstellt werden oder nur Teile aus dem ursprünglichen Dokuments ausgewählt werden. Für das Formatting werden Formatierungssemantiken, die die Knoten des Quellbaumes annotieren ausgelesen. Das Ergebnis des Formatting ist ein Baum mit Formatting Objects als Knoten. Für die einzelnen Formatierungsklassen können sehr fein Attribute wie Zeileneinschub, Wort- und Buchstabenabstände etc. beschreiben werden.

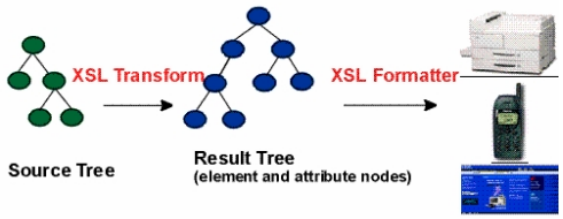


Abbildung 7.1: XSL Tree-Transformation

Vorteile von XSL:

Im Gegensatz zu HMTL haben die XML Elemente keine fest vorgegeben Darstellungssemantiken. Ohne ein Stylesheet ist ein XML Dokument nur eine Ansammlung von Daten, von denen ein Text Processor nicht wüsste, wie er sie darstellen sollte. Durch die XSL-Stylesheets steht ein umfangreiches Model und Vokabular zur Verfügung, um Darstellungsformen in XML selber zu beschreiben. Durch diesen Ansatz ist Inhalt von Layout getrennt und das elektronische Publizieren lässt sich aus einer Datenquelle in die verschiedensten Darstellungen überführen.

Bekannte Textformatierer:

- Apache FOP
- RenderX XEP

7.3 Elektronische Presse

Im Internet sind bereits einige Anbieter von elektronischer Presse zu finden. Aufgrund der Einschränkung im Umfang stellen wir hier nur zwei Anbieter vor.

7.3.1 Rhein Main Presse

Die Rhein Main Presse verfügt über eine elektronische Ausgabe ihrer Zeitung. Dabei handelt es sich um eine 1:1 Abbildung der aktuellen Tageszeitung. Für Kunden der Zeitschrift wird ein 4-Wochen Rückblick geboten. Die Seiten liegen im pdf-Format Einzelseiten oder gesamte Zeitung) vor und könenn mit einer Volltextsuche durchsucht werden. Für das Beziehen der Zeitung ist ein Abbonement notwendig (5 EUR/Monat), zum Schnuppern wird eine Demoausgabe bereitgestellt.

www.main-rheiner.de/eausgaben/mr/rmp/main.php

7.3.2 Füssener Internet Zeitung

Die Füssener Zeitung bietet ihre aktuelle Ausgabe kostenlos im Internet an. Die jeweilige Ausgabe liegt im .pdf-Format vor und kann abonniert werden. Das Abonnement wird dann per email zugestellt.

www.fuessener-zeitung.de/aktuelle_ausgabe.html

Rhein Main Presse

Fuessener Internet Zeitung

7.4 Großbaustelle Urheberrecht

Der folgende Abschnitt befasst sich mit den gesetzlichen Grundlagen zum Urheberrecht (Eigentum und elektronischen Publizieren bzw. Vervielfältigen). Dabei wird die aktuelle Gesetzeslage betrachtet sowie ein Ausblick auf die folgende Novelle des Urheberrechts gegeben.

Das Urheberrecht stellt einen Schutz konkreter Werke dar, etwa von Musikstücken, Büchern, Fotos, Bildern, aber auch von Software. In den meisten Ländern greift der Schutz automatisch mit dem Entstehen des Werkes. Dabei ist zu beachten, dass das Urheberrecht nur das eigentliche Werk und nicht die Idee dahinter schützt.

7.4.1 „Erster Korb“

Seit dem 13. September 2003 gilt das neue Urheberrecht (auch bekannt als „Erster Korb“), das die Vorgaben der sog. Informations-Richtlinie der EU umsetzt. Die Änderungen sind im Bundesgesetzblatt Nr. 46 vom 12. September 2003 (S. 1774-1788)[2] veröffentlicht. Wir konzentrieren uns speziell auf die geänderten Rechte für Musik, Filme, Software und Texte.

- Anfertigen von Privatkopien (Musik/Filme):
  Die Anfertigung von Kopien ist für private Zwecke erlaubt, wenn die Quelle über keinen Kopierschutz verfügt (§53, §95). Bis zu sieben Kopien für „private Zwecke“ sind derzeit erlaubt. Der Urheber wird für diese legalen Kopien über Geräteabgaben und Abgaben auf Tonträger entschädigt (§54).
  Die Formulierung in §53 „soweit nicht zur Vervielfältigung einer offensichtlich rechtswidrig hergestellte Vorlage verwendet wird“ soll jedoch klarstellen, dass Kopien nur zulässig sind, soweit der Nutzer auf das Original oder eine zulässige Kopie berechtigten Zugriff hat. Die Vervielfältigung von Raubkopien soll damit ausgeschlossen werden.
  Bei online angebotenen Dateien, wie bei Filesharingsystemen, kann man in der Regel davon ausgehen, dass es sich nicht um eine Privatkopie handelt, da diese nicht im privaten Bereich weitergegeben werden, sondern einem unüberschaubaren Benutzerkreis zur Verfügung gestellt wird. Derartige „Privatkopien“ waren und sind nicht erlaubt.

- Anfertigen von Privatkopien (Software):
  Eine Privatkopie von Software gibt es nicht. Bei Software ist gemäß §69 d) Abs. 2 lediglich eine Sicherungskopie erlaubt. Diese darf nur durch die Person, die zur Benutzung des Programms berechtigt ist, erstellt werden und muss für die Sicherung einer zukünftigen Benutzung erforderlich sein. Derzeit ist nur eine einzige Sicherheitskopie erlaubt. Software unterliegt den jeweiligen Lizenzbestimmungen, darf also, ohne ausdrückliche Erlaubnis durch den Urheber, in der Regel nicht für die Weitergabe kopiert werden. Der gesamte Bereich der Privatkopie gilt somit nicht für Computerprogramme, Betriebssysteme oder Spiele.

- Anbieten von Dateien in Internettauschbörsen(Musik):
  Das Bereitstellen von Musik (Upload) ist ebenso illegal wie der Download. §53 verbietet die Privatkopie, wenn eine „offensichtlich rechtwidrig hergestellte Vorlage verwendet wird“. Dies ist beim Download von Internettauschbörsen eindeutig der

Fall, da es keine mit dem Downloader verbundene Person ist, die das Musikstück anbietet (keine Vervielfältigung für nicht genau definierte Dritte).

- Anbieten von Dateien in Internettauschbörsen(Software):
  Das Bereitstellen oder downloaden von Software in Internettauschbörsen ist nicht gestattet. Nach §69 c) bedarf eine dauerhafte oder vorübergehende Vervielfältigung der Zustimmung des Rechtsinhabers.

- Download von Musik für den eigenen Gebrauch kostenlos aus dem Internet:
  Es ist kein Anfertigen von Kopien erlaubt, wenn es sich um offensichtlich rechtswidrige Vorlagen handelt (§53).

- Download von Software für den eigenen Gebrauch kostenlos aus dem Internet:
  Nur der Download von Freeware, Shareware oder kostenlosen Updates, der vom Urheber genehmigt ist, ist rechtlich erlaubt. Ein Download von kommerzieller Software über eine Tauschbörse ist nicht erlaubt (§69 c)).

- Knacken des Kopierschutzes um CDs oder DVDs zu kopieren:
  §95 sieht einen „Schutz technischer Maßnahmen“ vor. Gemäß §95 Abs. 1 dürfen technische Maßnahmen ohne Zustimmung des Rechtsinhabers nicht umgangen werden. Der Kopierschutz bei Audio-CDs oder DVDs darf somit auch zum Zwecke der Privatkopie nicht geknackt werden.
  Wird der Kopierschutz umgangen (nicht ausschließlich zum privaten Gebrauch), drohen nach §108 bis zu 3 Jahre Haft. Die Weitergabe von Kopierprogrammen kann mit einer Geldbuße von bis zu 50.000 Euro geahndet werden.

- Kopieren von Texten/Veröffentlichungen/Zitate:
  Nach §52a ist das Veröffentlichen kleiner Teile eines Werkes, Werke in geringem Unfang sowie einzelner Beiträge aus Zeitungen oder Zeitschriften im Unterricht an Schulen oder Hochschulen gestattet. Für „Tagesereignisse“ gilt das Recht zur Vervielfältigung, Verbreitung und öffentlichen Wiedergabe. Die Zitierfreiheit in §51 gilt für selbständige wissenschaftliche Werke (Großzitate). Darin dürfen einzelne andere Werke zur Erläuterung des Inhalts (zur Untermauerung der eigenen Aussage) aufgenommen werden. Es gilt jedoch der Grundsatz, dass die eigene Aussagen im Vordergrund stehen muss, nicht das Zitat. Nach §63 gilt zudem die Pflicht zur Offenlegung der Quelle.

7.4.2 „Zweiter Korb“

Im September 2004 wurde der Referentenentwurf zur zweite Reformstufe des Urheberrechts („Zweiten Korb“) vorgestellt. Geplant war die Fertigstellung des Gesetzes für Herbst 2005. Die Novelle wird jedoch nicht wie geplant umgesetzt werden können. Hauptursache ist der Streit um die Vergütungspauschale als Ausgleich für die prinzipiell weiterhin gestattete Privatkopie (vergl. 7.4.1). Die Vergütung soll dabei an die tatsächlich nennenswerte Nutzung der Gerätetypen oder der Typen von Speichermedien geknüpft

werden. Die Pauschalabgabe wird jedoch vom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) kritisiert, da bei PC-Systemen auch mehrfach auf einzelne Teile erhobene Belastungen sowie Wettbewerbsnachteil für hier ansässige Unternehmen und eine langsamere Verbreitung neuer Technologien zu befürchten sein. Die Geräteindustrie bemängelt außerdem, dass das Justizministerium keine klaren Regeln zur Abgabenhöhe einführen will. Die Verwertungsgesellschaften sehen ebenfalls in diesem Punkt Klärungsbedarf, denn sie befürchten bei Inkrafttreten des Gesetzes langwierige Verhandlungen mit den Herstellern und Importeuren von Geräten und Speichermedien über die Höhe der Vergütungssätze. Den Urhebervertretern könnte somit über Jahre hinaus ein erheblicher Teil an Erlösen fehlen.
Kritik kommt auch vom Aktionsbündnis „Urheberrecht für Bildung und Wissenschaft“. Dieses sieht eine „Gefahr für die wissenschaftliche Literaturversorgung“ durch zu rigide Vorschriften für den elektronischen Fachinformationsversand durch Bibliotheken. Die Regierung versucht der Wissenschaft entgegenzukommen: laut Kabinettsentwurf dürfen Bibliotheken künftig mehr Exemplare eines Werkes an elektronischen Leseplätzen gleichzeitig zugänglich machen, als der Bestand der Einrichtung umfasst.

Die größte Empörung kommt jedoch von Seiten der Filmindustrie, denn das Justizministerium hat im Referentenentwurf eine Bagatellklausel vorgeschlagen. Laut diesem soll der Download im geringfügigen Umfang strafffrei bleiben. Und diese Bagatellklausel soll sogar noch erweitert werden: wer Werke oder Bearbeitungen von Werken nicht nur in kleinen Mengen kopiert oder erstellt, sondern auch wer diese zum privaten Gebrauch vervielfältig, soll nicht bestraft werden. Gestattet wird somit die Versorgung von Freunden oder Bekannten. Aufgrund der Kritik wird auf Seiten der Regierung jedoch überlegt, neben Computerprogrammen auch Filme von der Bagatellregelung auszunehmen.
Die Kinos reagieren auf diese Entwicklung mit einer eigenen Kontrolle. In begründeten Verdachtsmomenten sollen künftig Nachtsichtgeräte einsetzen werden. Priorität sei dabei allerdings, „dass das Kino nicht zum Hochsicherheitstrakt wird“ und „dass der Kinobesucher sich nicht in seiner Intimsphäre gestört fühlt“[3]. Bei Einsatz der Nachtsichtgeräte würden die Zuschauer vorab informiert, zudem gehe es ja auch nur um „punktuelle Kontrollen“. Die Geschäftsführerin der Zukunft Kino Marketing GmbH (ZMK), Elke Esser sagte dazu: Es „haben sich mehrere Kinos zusammengeschlossen und prüfen die Bestellungen von circa 600 portablen Nachtsichtgeräten, mit denen wir in unregelmäßigen Intervallen und in begründeten Einzelfällen kontrollieren könnten.“ Für die Verbraucher findet sich in der Novelle so gut wie nichts Positives, denn das neue Urheberrecht entfernt sich immer weiter von einer fairen, ausgewogenen Regelung und muss sich deshalb auf eine sinkende allgemeine Akzeptanz einstellen.

7.5 Gefährdete Werte und Nutzungsrechte

Zu den gefährdeten Werten, die durch DRM Systeme geschützt werden sollen, gehören:

- Musikstücke

- Filme, TV-Material
- Bilder
- Texte
- Software

wobei vorrangig Audio- und Videodateien im Zentrum des Interesses stehen. Für digitale Medien ist es durch Nutzung von DRM-Lösungen möglich, unterschiedlichste Nutzungsrechte festzulegen, welche sich grob in drei Klassen einteilen lassen: Zugriffsrechte, Transportrechte und Bearbeitungsrechte.

Zugriffrechte:

Abspielen	Audio- und Videoinhalte, weitere Differenzierung nach Nutzungsrechten möglich: beliebig und unbegrenzt abgespielen, zeitliche Beschränkung, Beschränkung der Anzahl der Abspielvorgänge
Ansehen	Textdokumente und Bilder, Betrachtung erlaubt? Bei progressiven Bildformaten, d.h. die mit zunehmend nachgeladenen Daten feiner aufgelöst sind, ist die Angabe der Detailstufe bis zur das Bild zur Verfügung steht, denkbar.
Drucken	Textdokumente und Bilder, Ausdruck freigegeben/beschränken

Transportrechte:

Rechte auf Kopie	alle Medientypen, Vervielfältigung erlaubt/verboten.
Recht zum Transfer	alle Medientypen, regelt Transfer von digitalen Werke z.B. auf einen an den heimischen PC angeschlossenen portablen Medienplayer, wobei dieser Transfer in der Regel nur in einer Richtung möglich ist.
Recht auf Ausleihe	alle Medientypen, Beschränkung der Anzahl der Abspielmöglichkeiten oder eine zeitliche Begrenzung der Medienverfügbarkeit.

Bearbeitungsrechte:

Cut-&-Paste	alle Medientypen, erlaubt Weiterzuverarbeitung und Verwendung in eigenen Dokumenten/Medien.
Editieren	alle Medientypen, erlaubt Veränderung des ursprünglichen Mediums in begrenzter Weise.

Mit diesen unterschiedlichen Rechten, die für die verschiedenen Medientypen festgelegt werden können, unterstützen DRM-Anwendungen ein breites Spektrum an Kontrolle. In ihrer schwächsten Form regeln sie den Zugang zu digitalen Werken, in ihrer stärksten Form (im Falle von Abo-Modellen) ermöglichen sie eine individuelle Abrechnung innerhalb eines Bezahlsystems.

7.6 DRM-Referenzmodell

Das DRM Referenz Model besteht aus drei Komponenten. Der Server welche die Inhalte gespeichert hat *(Content Server)*, der Lizenz Server *(License Server)* und der Kunde *(Client)*.

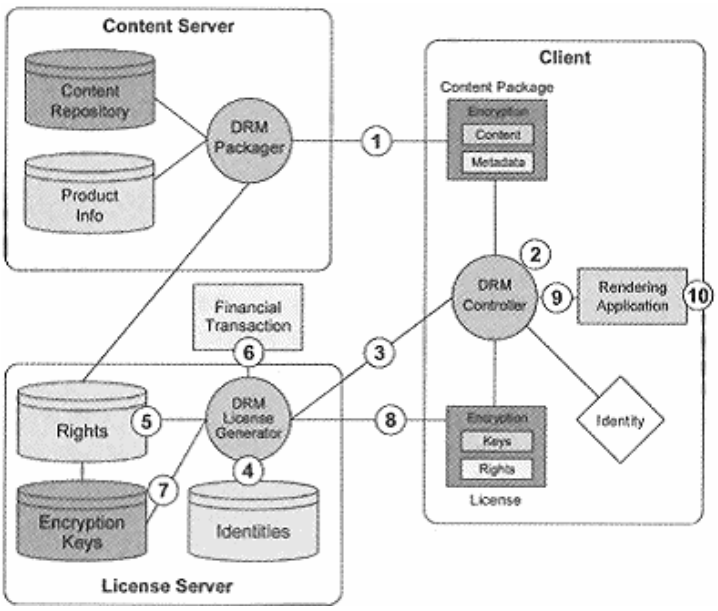


Abbildung 7.2: DRM-Referenzmodell, Quelle:Rosenblatt/Trippe/Mooney (2002)

1. Der Nutzer (Client) lädt - zum Beispiel von einer Web-Site, FTP Server, E-mail - die verschlüsselten digitalen Inhalte inklusive Metadaten auf seinen Computer hinunter (Content Package).

2. Durch Doppelklick wird eine automatische Anfrage gestartet. Diese aktiviert den DRM Controller. Einmal aktiviert, sucht der DRM Controller die nötigen Informationen um die gewünschte Lizenz ausstellen zu können.

3. Der DRM Controller sendet die Identität (Identity) des Nutzers und des digitalen Inhaltes (Content Package) zum Lizenz Server (License Server).
4. Der Lizenz Server identifiziert den Nutzer mit Hilfe der Identifications Datenbank (Identities).
5. Der Lizenz Server erfasst die Rechteinformationen gemäss der Anfrage des Nutzers (Rights).
6. Falls für den digitalen Inhalt eine Zahlung notwendig ist, wird auch eine finanzielle Transaktion gestartet (Financial Transaction).
7. Erstellung der Lizenz welche zugleich auch verschlüsselt (Encryption Keys) wird. Der DRM License Generator stellt die Rechte (Rights), die Nutzeridentität (Identity) und erstellt und verschlüsselt (Encryption Keys) die Lizenz.
8. Die Lizenz wird dem Nutzer geschickt.
9. Entschlüssselung des digitalen Inhaltes und "Freigabe"des Inhaltes an das Wiedergabegerät (Rendering Applications).
10. Das Wiedergabegerät spielt, druckt, zeigt, etc. den digitalen Inhalt dem Nutzer an.

7.7 DRM-Hardwareumsetzung (TPM/TCG/TCPA)

1999 schlossen sich die Unternehmen Compaq, HP, IBM, Intel und Microsoft zur „Trusted Computing Platform Alliance“ (TCPA) mit der Aufgabe zusammen, gemeinsame Standards zu erarbeiten. Die „Trusted Computing Group“ (TCG) ging am 8. April 2003 als eine Neugründung aus der TCPA hervor. Den zentralen Punkt der TCG bildet die Spezifikation eines neuen Bausteins, auf dem das gesamte Sicherheitskonzept aufbaut: das „Trusted Platform Module“ (TPM, auch Fritz-Chip genannt). Vier wesentliche Funktionen soll das TPM innerhalb einer sicheren Plattform übernehmen:

- Schützen und Generieren von geheimen Schlüsseln
- Sichere Ablage von als vertrauenswürdig eingestuften Systemkonfigurationen
- Bereitstellung eines speziellen Schlüssels, mit dem die Plattform von Dritten als vertrauenswürdig erkannt werden kann
- Verwaltungsfunktionen, mit denen u.a. das TPM von einem Benutzer ein- und ausgeschaltet werden kann

Das Trusted Platform Module ist ein Chip, der einer fest eingebauten Smartcard entspricht mit dem wichtigen Unterschied, dass er nicht an einen konkreten Benutzer, sondern an ein System gebunden ist.

Beim Hochfahren des Rechners wird zuerst das Core Root of Trust Measurement (CRTM) aufgerufen, das überprüft ob das TPM aktiviert ist. Ist das nicht der Fall, erfolgt ein normaler Bootvorgang wie er auf jedem Rechner abläuft. Ist das TPM hingegen aktiviert, dann wird beim Aktivieren jeder weiteren relevanten Komponente (festgelegte Hard- und Software) ein Hashwert gebildet. Wurden alle Komponenten aktiviert, wird ein Hashwert über die Gesamtkonfiguration gebildet und in einem sicheren Bereich des TPM abgelegt. Danach wird der normale Hochfahrvorgang fortgesetzt. Anschließend erfolgt eine Zustandsbewertung durch Vergleich mit Prüfsumme vom letzten Booten. Tritt dabei ein Unterschied auf, erfolgt ein Alarm und die Plattform ist nicht mehr TCPA-Konform und muss neu zertifiziert werden. (s. Abb. 7.7.2)

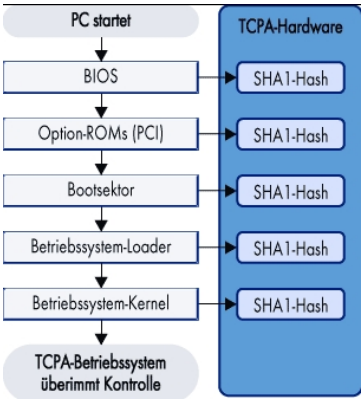
7.7.1 Kritik

Bisher kann der Benutzer eines PC, entsprechende Kenntnisse vorausgesetzt, seinen Rechner vollständig kontrollieren. Zukünftig könnten diese Möglichkeiten bei einer restriktiveren Plattform mit einem sicheren Betriebssystem wegfallen. Mit dem Argument „Sicherheit“ können Anwendungen gesperrt oder die Verwendung von Einsteckkarten abgelehnt werden. Die Konfiguration eines Rechners, die Lizenzierung der verwendeten Produkte und die Urheberrechte von gespeicherten Inhalten können jederzeit überprüft und an Dritte übermittelt werden. Der Benutzer muss sein Vertrauen in die Sicherheitskomponenten auf Schlüssel begründen, die er nicht selbst erzeugt hat. Ob die gespeicherten Schlüssel wirklich geheim und einmalig sind, ist nicht überprüfbar.

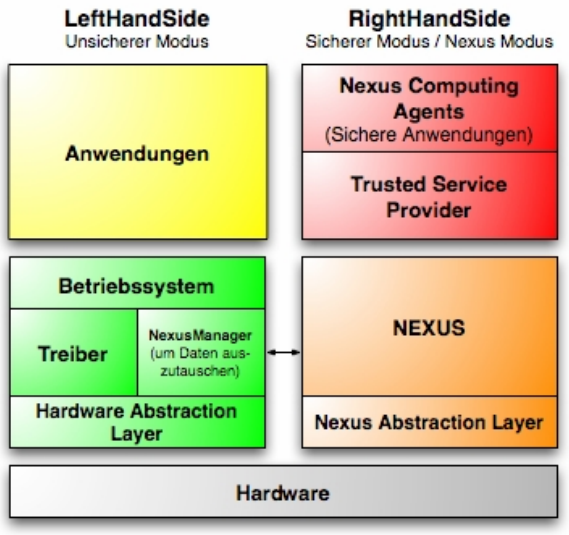
7.7.2 Next Generation Secure Computing Base (NGSCB)

Die Next Generation Secure Computing Base (NGSCB) ist eine Sicherheitsinitiative von Microsoft, die im Juni 2002 als Nachfolger von Palladium ins Leben gerufen wurde. Das Konzept der NGSCB, das erstmals in der nächsten Windows-Version Longhorn eingesetzt werden soll, ergibt sich durch einen Kompromiss den Microsoft bereit ist einzugehen: Zum einen soll Windows ein möglichst sicheres Betriebssystem werden, zum anderen soll „alte“ Software weiterhin lauffähig bleiben. Die Lösung bildet der Nexus, ein zweiter Kernel der zum bisherigen Windows „hinzugeladen“ wird. Auch ein Entladen des Nexus im laufenden Betrieb ist vorgesehen. Nach dem Laden des Nexus gibt es laut Microsoft zwei Einschränkungen: Computerprogramme dürfen nicht mehr beliebig auf den kompletten Speicher zugreifen und die CPU nicht mehr in den Real Mode versetzen.
In den vorhandenen Dokumenten unterscheidet Microsoft grundsätzlich zwischen der unsicheren Seite mit dem normalen Windows (LeftHandSide) und der sicheren Seite des Nexus (RightHandSide). Der Nexus verwaltet auf der gesicherten rechten Seite sichere Anwendungen (Agents) und TSPs (Trusted Service Provider), die ein (sicheres) Pendant zu den Diensten unter Windows darstellen. Dienste und Anwendungen laufen zwar in sicheren Speicherbereichen ab, bei beiden handelt es sich aber dennoch um ganz gewöhnliche Software. Der Nexus sieht sie einfach als sicher an und geht davon aus, dass

alles andere (also auf der LeftHandSide) unsicher ist. Wie dafür gesorgt wird, dass diese „sicheren“ Programme auch sicher sind, ist bis jetzt noch unklar. Denkbar wäre ein Zertifizierungssmodell, bei der sichere Anwendungen auf ihre Legitimität geprüft würden. Daten von dieser unsicheren linken Seite gelangen über einen speziellen Treiber auf dieser LeftHandSide, dem Nexus-Manager, auf die RightHandSide. Der Nexus prüft die Daten dann im NAL (Nexus Abstraction Layer), dem Gegenstück zum HAL (Hardware Abstraction Layer). Weichen die Daten von der Erwartungen ab, werden sie bereits hier verworfen. Außerdem muss der Nexus sich selbst und die gesamte RightHandSide vor direkten Speicherzugriffen (z.B. über Busmaster-fähige Geräte) schützen.
Abb. 7.7.2:



Funktionsweise des Fritzchip



Next Generation Secure Computing Base, Quelle:www.Wikipedia.org

7.8 DRM-Softwareumsetzung

Aufgrund der Einschränkungen im Umfang dieser Ausarbeitung stellen wir hier nur eine DRM-Lösung von Microsoft vor.

7.8.1 Microsoft Windows Media digital rights management

Die Microsoft DRM-Lösung Windows Media DRM ist seit April 1999 (Windows Media 1) auf dem Markt und wurde seit dem ersten Release stetig weiterentwickelt. Aktuell liegt die Version Window Media DRM 10 vor.

1. Digitale Inhalte werden mit Metainformaitionen angereichert und verschlüsselt. Das Ergebnis ist eine DRM-geschützte Datei (Protected Media).

2. Die geschützten Inhalte können zum Download oder für Streaming bereitgestellt werden.

3. Im Lizenzserver werden neue Lizenzen zugehörig zu den geschützten Inhalten abgelegt. Diese Lizenzen enthalten die Regeln und Rechte für die Inhalte.

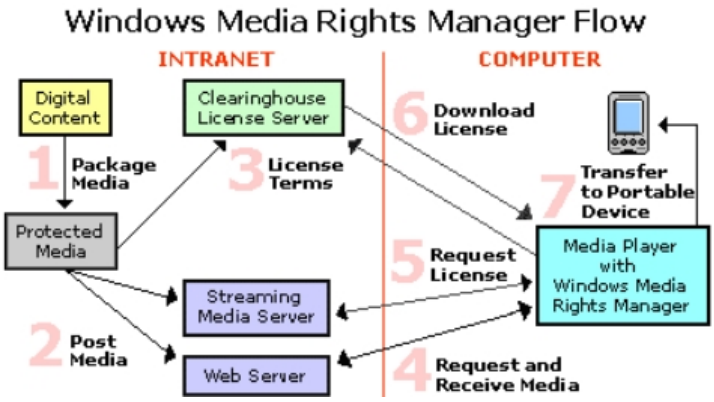


Abbildung 7.3: Windows Media Worklflow

4. Ein Client greift auf die geschützten Inhalte zu.

5. Je nach Vertriebstyp, muss vor dem Download oder Nutzen der Inhalte eine Lizenz erworben werden. Diese wird durch den Windows Media DRM unterstützenden Media Player des Nutzers vom Lizenzserver abgefragt.

6. Die Lizenz wird in das lokale Lizenzrepository des Clients geladen. Dieser kann die Inhalte nun nach den Bedingungen der Lizenz wiedergeben.

7. Die Inhalte können nun auch auf tragbare Geräte überspielt werden, wenn die Lizenz dies zulässt.

Literaturverzeichnis

[1] Begriffe aus dem Bereich „Elektronsiches Publizieren“, Uni München, www.zepl.uni-muenchen.de/glossar.htm

[2] Bundesministerium der Justiz, Bundesgesetzblatt Jahrgang 2003 Teil I Nr. 46, Bundesanzeiger Verlagsges.mbH, 2003, www.bmj.bund.de/files/e79860a4aef833e5de5933d86ef6003f/441/Bundesgesetzblatt_nr46.pdf

[3] Elke Esser, Geschäftsführerin der Zukunft Kino Marketing GmbH (ZMK), Spiegel Online, www.spiegel.de/netzwelt/politik/0,1518,354418,00.html

[4] C't, Magazin für Computertechnik, Ausgabe 11 (17.5.05), Heise Verlag, www.heise.de

[5] Wikipedia, www.wikipedia.de

[6] Internet-Rostock, Johannes Richard, www.internet-rostock.de

[7] XSL, w3.org, www.w3.org/TR/xsl/

[8] XML-FO, Apache, xml.apache.org/fop/

8 Elektronischer Vertragsabschluss

Steven Grigoleit

8.1 Zusammenfassung

In dieser Arbeit werden Grundlagen, Vorraussetzungen, sowie Probleme und Konsequenzen des elektronischen Vertragsabschlusses zusammengefasst.
Begonnen wird dabei mit einem Einblick in die Welt des „althergebrachten“ Vertragsabschlusses. Hier ist es wichtig, dass Zusammenspiel zwischen Antrag und Annahme als Grundkonstrukte eines Vertrages zu erläutern und darauf einzugehen, wann und unter welchen Bedingungen ein Vertrag rechtswirksam abgeschlossen wird.
Im darauf folgenden Teil werden technische Vorraussetzungen geklärt, die elektronische Vertragsabschlüsse erst ermöglichen. Dazu gehören in erster Linie die so genannte Elektronische Signatur sowie das Public-Key-Verfahren.
Um den Grundlagenteil zu vervollständigen, werden das Signaturgesetz und Begriffe zur Elektronischen Signatur vorgestellt.
Der letzte Teil der Arbeit beschäftigt sich abschließend mit elektronischen Vertragsabschlüssen und mit bestimmten Problemen, die damit einhergehen können.

8.2 Allgemeiner Vertragsabschluss

„Der Rechtsakt, der eine gewollte Rechtsfolge bewirkt, wird *Rechtsgeschäft* genannt.“[1]
Ein Vertrag (oder Kontrakt) ist ein „mehrseitiges Rechtsgeschäft zur Begründung, Aufhebung oder Änderung eines Rechtsverhältnisses, das durch übereinstimmende Willenserklärungen, nämlich Antrag und Annahme, zwischen zwei oder mehreren Personen (Vertragsparteien, Vertragsgegner) zustande kommt.“[2]
Von entscheidender Bedeutung ist also die abzugebende *Willenserklärung*.
Eine Willenserklärung „ist die Äußerung eines auf die Herbeiführung eines Rechtserfolges gerichteten Willens, setzt sich also aus dem äußeren Tatbestand der *Erklärung* und dem inneren Tatbestand des *Willens* zusammen.“[3]
Eine Erklärung kann nach dem Gesetz in den Formen Schreiben oder Sprechen verklausuliert werden. Das Gesetzt lässt aber auch andere Formen zu, die erfahrungsgemäß

[1] [01] S. 27
[2] [02] S. 471
[3] [01] S. 27

dem Erklären eines Willens dienen, wie zum Beispiel Kopfnicken oder auch weitere stillschweigende Verhaltensmuster.
Der Wille umfasst nach [01] den Handlungswillen, das Erklärungsbewusstsein und den Geschäftswillen. Hiermit meint man erstens, dass eine Handlung bewusst durchgeführt werden muss und nicht Folge z.B. eines Reflexes ist, zweitens, dass das Bewusstsein für eine rechtliche Tat (mit ihrer Konsequenzen) vorhanden ist und drittens, dass eine Absicht vorliegen muss, ein Rechtsgeschäft durchführen zu wollen.
Ein Vertrag kann über die verschiedensten Dinge oder Gegenstände abgeschlossen werden, da obige Definition keinerlei Einschränkungen bezüglich etwaiger Vertragsgegenstände vornimmt. Es gibt Verträge, die stillschweigend abgeschlossen werden (Beispiel: Taxi), es gibt aber auch in großer Vielzahl Verträge, die weitere gesonderte Maßnahmen zum Vertragsabschluss benötigen. Hier wird unterschieden, ob ein Rechtsgeschäft, bzw. die Willenserklärung, empfangsbedürftig oder nicht empfangsbedürftig ist (bei einseitigen Rechtsgeschäften). Die Form der Empfangsbedürftigkeit regelt dabei implizit die Frage, ab wann das Rechtsgeschäft wirksam ist. Eine weitere Unterscheidungsmöglichkeit untersucht die Tatsache, ob ein Vertrag gegenseitig oder nur einseitig verpflichtend ist (bei zweiseitigen Rechtsgeschäften).
In jedem Fall setzt ein gegenseitig verpflichtender Vertrag, bzw. der Abschluss eines gegenseitig verpflichtenden Vertrages das Vorhandensein von Willenserklärungen der Vertragspartner voraus. Diese Willenserklärungen müssen dabei konsequenterweise inhaltlich übereinstimmend sein, wobei die Willenserklärung des Antragenden von der Art einer Willenserklärung mit Empfangsbedürftigkeit ist. Darüber hinaus kann „das Zustandekommen eines wirksamen Vertrages von der Einhaltung einer bestimmten Form, der Zustimmung dritter Personen oder einer Behörde, der (konstitutiven) Eintragung in ein Register (z.B. Grundbuch) oder dem Eintritt einer Bedingung abhängig sein.“[4]
Nicht immer muss der Willen zwischen einander geographisch nah stehenden Personen erklärt werden. Das Gesetz unterscheidet darum zwischen Willenserklärungen zwischen Anwesenden und Abwesenden[5]. Eine Willenserklärung zwischen Anwesenden kann immer dann abgegeben werden, wenn sich die Vertragspartner z.B. im gleichen Raum befinden. Willenserklärungen, die im fernmündlichen Bereich (z.B. via Telefon) abgegeben werden, werden nach dem Gesetzgeber genauso behandelt, wie Willenserklärungen zwischen Anwesenden.[6] Zu diesem Zweck hat der Gesetzgeber allgemeingültig festgelegt, unter welchen Bedingungen die Willenserklärungen der Vertragspartner als Willenserklärungen zwischen Anwesenden oder Abwesenden zu behandeln sind. Kann, bzw. muss eine Willenserklärung verkörpert werden, stellt sie eine Willenserklärung zwischen Abwesenden dar. Verkörpert meint in diesem Zusammenhang, dass eine Willenserklärung auf einem gegenständlichen Träger festgehalten ist, dass heißt, dass die Willenserklärung beständig aufbewahrt werden muss, um sie dem abwesenden Vertragspartner zukommen zu lassen. Solche gegenständlichen Träger sind in der Regel Dokumente in Papierform.
Lassen es die technischen Vorraussetzungen zu, können auch mündliche Erklärungen

[4] [02] S. 471
[5] $ 130 [10]
[6] $ 147 [10]

zwischen anwesenden Vertragspartnern verkörpert werden. In diesem Fall muss ein geeignetes Aufnahmegerät verfügbar sein.
Geht man von der Annahme eines Vertragsabschlusses zwischen nicht anwesenden Vertragspartnern aus, muss genau geregelt werden, zu welchem Zeitpunkt der Vertrag rechtsgültig ist. Eine Willenserklärung gegenüber Abwesenden ist gültig, sobald sie dem Empfänger zugänglich ist[7]. Der Vertrag ist wirksam, sobald die Vertragsseiten den unterzeichneten Vertrag zugänglich haben. In diesem Fall sind die Willenserklärungen der Vertragspartner wirksam.
Geht man von der Annahme eines Vertragsabschlusses zwischen anwesenden Vertragspartnern aus, so ist eine nicht verkörperte Willenserklärung dann gültig, sobald der Empfänger sie wahrgenommen hat, zuerst ohne Beachtung der Frage, ob der Empfänger sie lediglich optisch oder visuell, oder auch inhaltlich wahrgenommen haben muss.
In jedem Fall regelt das BGB für bestimmte Arten von Verträgen bestimmte Formvorschriften, die zur Erreichung einer Wirksamkeit eingehalten werden müssen. Dazu gehört z.B. die eigenhändige Unterschrift zur Erklärung des eigenen Willens.
Zusammenfassend kann man also sagen, dass ein Vertrag ein Rechtsgeschäft ist und „aus zwei übereinstimmenden Willenserklärungen zweier Personen“ besteht. „Die beiden Willenserklärungen sind *Antrag* und *Annahme*. Jeder Vertrag kommt zustande durch die Annahme des Antrags. Das *Angebot* ist eine empfangsbedürftige Willenserklärung, die inhaltlich so bestimmt sein muss, dass sie durch ein ‚Ja' des Empfängers angenommen werden kann.“ Grundsätzlich hat ein Antragender sein Angebot an einem bestimmten Empfänger zu richten, wobei es natürliche Ausnahmen gibt. Diese Ausnahmen stellen beispielsweise ein Getränkeautomat oder ein Schaufenster dar.[8]

8.3 Technische Grundlagen

Nachdem im letzten Abschnitt die Begriffe Vertrag, Vertragsabschluss und Willenserklärung geklärt wurden, die natürlicher Weise grundlegend für einen elektronischen Vertragsabschluss sind, sollen in diesem Abschnitt technische Grundlagen, die zum elektronischen Vertragsabschluss notwendig sind, eingeführt werden. Dazu gehört vornehmlich das Erklären des Verfahrens der Elektronischen Signatur.

8.3.1 Public-Key-Verfahren

Die elektronische Signatur basiert in der Regel auf asymmetrische Kryptosysteme.[9] Das gesamte Verfahren kann auch *Public-Key-Verfahren* genannt werden. Public-Key deshalb, weil mit öffentlichen, also bekannten Schlüsseln gearbeitet wird.
Allerdings müssen auch private, also allgemein unbekannte Schlüssel verwendet werden. Nachfolgend soll das Verfahren der Ver- und Entschlüsselung vorgestellt werden.

[7] $ 130 [10]
[8] aus [01] S. 32
[9] [03]

Ein Unterzeichner muss einen öffentlichen Schlüssel haben, den jeder einsehen kann. Darüber hinaus hat er einen privaten Schlüssel, den nur er kennen darf.
Abbildung 1 zeigt, welche Syntax nachfolgend verwendet werden soll: (in Anlehnung an [10])

Tabelle 8.1: : Public-Key-Verfahren: Verwendete Syntax

P1	Person 1 (Sender)
P2	Person 2 (Empfänger)
K_{Pu}(P1)	Der öffentliche Schlüssel von P1
K_{Pr} (P1)	Der private Schlüssel von P1
$\{x\}$ _K	Das Verschlüsseln von x mit dem Schlüssel K
N	Eine Nachricht
h(N)	Der Hashwert von N berechnet mit der Hasfunktion h
S	Die Signatur

Betrachtet wird jetzt das Übermitteln einer Nachricht von P1 an P2. Dabei muss sichergestellt werden, dass P2 K_{Pu}(P1) kennt. Dies kann über verschiedene Wege erreicht werden. Entweder teilt P1 P2 K_{Pu}(P1) (auch über einen unsicheren Kanal) mit oder P2 informiert sich in entsprechenden Verzeichnissen.
In der Abbildung 2: *Ablauf eines Nachrichtenaustausches mit Signierung (Ablaufdiagramm in Form eines Petri-Netzes) sind die Personen 1 und 2 als Sender bzw. Empfänger gekennzeichnet. Jetzt will P2 von P1 ein von P1 signiertes Dokument, welches zum Beispiel für einen Vertragsgegenstand von größter Bedeutung ist oder eine Willenserklärung von P1 darstellt, welche zur Folge hat, dass ein Vertrag zwischen P1 und P2 rechtswirksam wird.*

[10] [03]

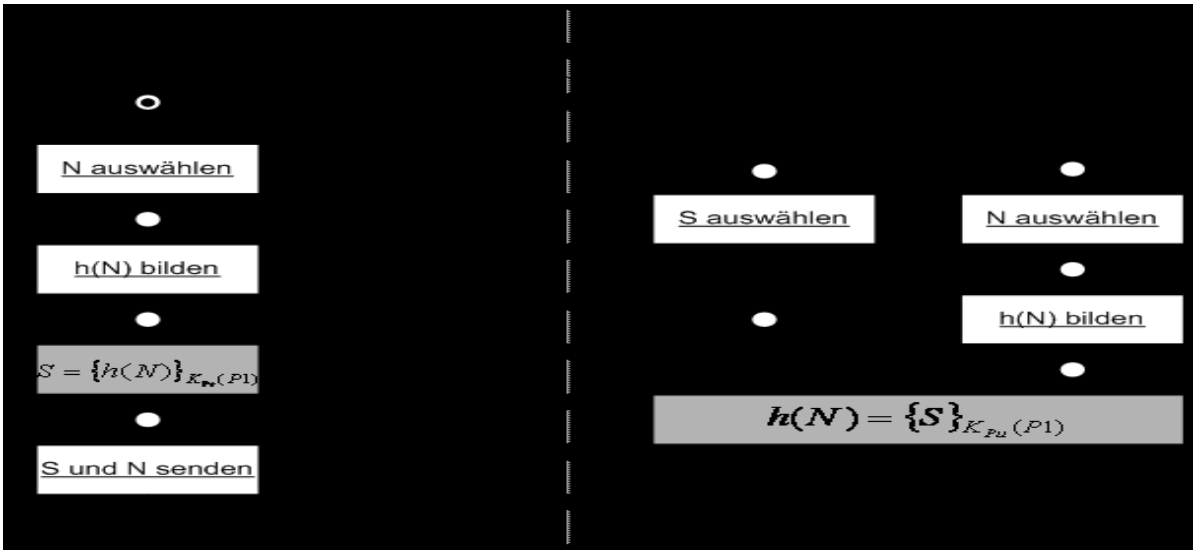


Abbildung 8.1: : Ablauf eines Nachrichtenaustausches mit Signierung

Dazu bildet P1 h(N). Dieser Hashwert (kurze Zeichenfolge) soll sicherstellen, dass erkannt werden kann, ob N (lange Zeichenfolge) manipuliert wurde. Wird N auch nur in einem Bit verändert, so verändert sich auch h(N). Der Weg zurück, also das Erstellen von N aus h(N) ist nur theoretisch mit quasi unrealisierbarem Aufwand möglich. P1 übermittelt jetzt nicht N und h(N) im Klartext, sondern verschlüsselt h(N) mit K_{Pr} (P1), was S ergibt:

$$S = \{h(N)\}_{K_{\mathrm{Pr}}(P1)}$$

P1 sendet jetzt N und S an P2. P2 ermittelt jetzt seinerseits mit der gleichen Hash-Funktion den Hashwert von N und versucht mittels K_{Pu}(P1) S zu entschlüsseln. Wenn

$$h(N) = \{S\}_{K_{Pu}(P1)}$$

gilt, kann P2 sicher sein, dass ihm N korrekt vorliegt und P1 ordnungsgemäß signiert hat. Damit könnte zum Beispiel ein Vertrag auf elektronischem Wege abgeschlossen worden sein.
Gilt letzteres nicht, ist das ein Hinweis darauf, dass entweder das Dokument, nach dem es signiert und bevor es P2 erreicht hat, manipuliert wurde oder das K_{Pr} (P1) nicht der

korrekte private Schlüssel von P1 war. Welcher der beiden Fälle eingetreten ist, kann nicht nachvollzogen werden. Muss es aber auch nicht, da es völlig gleichgültig ist, welcher der beiden Fälle eingetreten ist: in jedem Fall ist die elektronische Signatur ungültig und es existiert keine Grundlage mehr, auf Basis von S ein Rechtsgeschäft abzuschließen. Die grau hinterlegten Transitionen zeigen die Aktionen, in denen der privaten bzw. der öffentliche Schlüssel von P1 Verwendung finden.

8.3.2 Algorithmen und Standards

Wie im letzten Abschnitt gesehen, liegen die Schwierigkeiten und damit die Güte der verwendeten Verfahren zum einen in der Hashfunktion und zum anderen in der Verschlüsselungs- oder Signierfunktion.
Als mögliche Algorithmen für die Hashfunktion haben sich nach [11] der RIPEMD (Reseaux IP Europeens Message Digest) und der SHA-1 (Secure Hash Algorithm 1) durchgesetzt:

- RIPEMD gilt in der 160-Bit-Variante zurzeit als sicherer Algorithmus, wenngleich auch Varianten mit 256 Bit und 320 Bit denkbar sind. Er baut auf dem MD4[12]-Algorithmus auf.
- SHA-1 beruht auf ähnliche Prinzipien wie der bekannte MD5[13]-Algorithmus, ist mit einer Wortlänge von 160 Bits aber sicherer.

Für die Signierung gelten nach [14] der RSA (Rivest, Shamir, Adleman)-Algorithmus und der DAS (Digital Security Algorithm) als sicher:

- Bei RSA beruhen öffentliche und private Schlüssel auf einem Paar sehr großer Primzahlen. Für die Signatur werden mindest Schlüssellängen von 1024 Bits benötigt, um von einer momentanen Sicherheit sprechen zu können, da beispielsweise Schlüssellängen von 512 Bits schon geknackt wurden.
- Die Sicherheit des DAS ist auch von der verwendeten Hashfunktion abhängig und basiert auf dem Problem der diskreten Logarithmen. Heutzutage gelten Schlüssellängen von 1024 Bits als sicher.

Es existieren nach [15] so genannte PGP-Systeme und zertifikatsbasierte Systeme. PGP steht für Pretty-Good-Privacy und stellt in dem Sinne keine Algorithmen zur Verschlüsselung bereit. Vielmehr werden hier verschiedenste Verschlüsselungsverfahren unter einer

[11] aus [12]
[12] MD-4 (1990 entwickelt) ist ein Verfahren zur Errechnung einer eindeutigen Prüfsumme und erzeugt Hashwerte der Länge 128 Bit. Gilt heutzutage aufgrund von Mängel im Design als überholt und unsicher.
[13] MD-5 (1991 entwickelt) soll die Mängel vom MD-4 verbessern, nachdem schnell bekannt wurde, dass MD-4 wahrscheinlich unsicher ist, was heutzutage bewiesen wurde. Ebenfalls 128 Bit.
[14] aus [12]
[15] aus [03]

Umgebung zusammengefasst. „PGP-Systeme basieren auf dem Gedanken, dass sich jeder Kommunikationspartner jederzeit ein Schlüsselpaar erzeugen kann. Das Vertrauen in die Zuordnung der Schlüssel zu einer Person wird durch gegenseitige Beglaubigungen realisiert.“ Hier wird schnell deutlich, dass PGP-Systeme vor Gericht kaum Beweiskraft erlangen dürften.
Eine andere und weitaus beweiskräftigere Möglichkeit bieten die zertifikatsbasierten Systeme, die im Grunde Gegenstand dieser Arbeit sind. Wie noch detaillierter gezeigt wird, „erhält jeder Benutzer ein digitales Zertifikat, welches seine Identität beschreibt und die öffentlichen Schlüssel enthält. Jedes Zertifikat ist von einer ausgebenden Stelle beglaubigt, [...].“
Da der Standard S/MIME auf digitalen Zertifikaten aufbaut, spielt er demzufolge auch eine große Rolle bei der elektronischen Signatur.

8.3.3 Elektronische Signatur

In diesem Abschnitt wird die Fragestellung erläutert, was eine elektronische Signatur ist und wie jede Privatperson an eine Elektronische Signatur gelangen kann und welche Schritte von Antrag bis Auslieferung durchgeführt werden.
„Elektronische Signaturen sind durch Personen elektrisch erstellte Willenserklärungen oder Bestätigungen.“ Diese elektronische Signatur ist immer personengebunden, ermöglicht das Erkennen einer Veränderung an Dokumenten und ist eindeutig einer bestimmten Person zugeordnet. Willenserklärungen können in diesem Zusammenhang Bestellungen, Verträge, Anträge und Aufträge sein. Bestätigungen sind beispielsweise Empfangsbescheinigungen oder Quittungen.[16]
Wenn der Kunde eine so genannte Signaturkarte in Besitz nehmen will, so muss er, wie in Abbildung 3: *Beteiligte Instanzen auf dem Weg zu einer elektronischen Signatur ersichtlich, im ersten Schritt einen Antrag stellen. Will er eine qualifizierte elektronische Signatur, welche nach heutigem Stand alleinig die Funktion als rechtliches Äquivalent zur handschriftlichen Unterschrift innehat, so muss er sich mit einem offiziellen Dokument (Ausweis oder Reisepass) bei einem so genannten Trust Center vorstellen. Dort werden dann seine persönlichen Daten aufgenommen. Jedes Trust Center betreibt einen so genannten Schlüsselgenerator, der zuerst einen personengebunden privaten Schlüssel für den Antragssteller erzeugt. Beides, die persönlichen Daten und der private Schlüssel stellen dann das Zertifikat dar, welches beispielsweise auf eine Chipkarte gepresst werden könnte. In der Abbildung 2 wird dieser Arbeitsschritt von einem nicht weiter benannten Akteur erledigt.*
Der Schlüsselgenerator muss auch einen korrespondierenden öffentlichen Schlüssel erzeugen und in ein allgemein zugängliches öffentliches Verzeichnis gemeinsam mit den persönlichen Daten des Antragsstellers einstellen.
Die fertige Chip-Karte kann dann dem Antragsteller ausgehändigt werden.
Weitere Aufgaben des Trust-Centers sind dann die Überprüfung von Zertifikaten, das Sperren von Zertifikaten sowie ein so genannter Zeitstempeldienst, welcher nachprüfen

[16] aus [09]

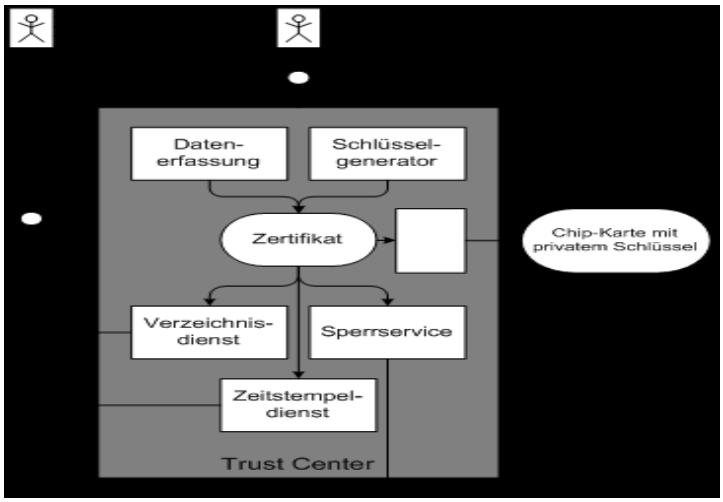


Abbildung 8.2: Beteiligte Instanzen auf dem Weg zu einer elektronischen Signatur

kann, ob ein Dokument zu einem gegebenen Datum noch gültig signiert war. Wie zu sehen ist, kann jeder diese Dienste in Anspruch nehmen.
Benötigt jetzt der Antragsteller eine Signierung, so kann er mit seiner Chip-Karte, seinem Lesegerät und weiterer Software, die beispielsweise den PIN-Zugriffsschutz auf die Chip-Karte überwacht oder den privaten Schlüssel ausliest, die Signierung einer Datei vornehmen.
Dieser Vorgang wird dabei weitgehend von Software erledigt. Es genügt die entsprechende Datei auszuwählen.
Heutzutage ist die Signierung auch in gängige Mail-Programme integriert. Dies geschieht teilweise „von Werk“, oder durch zugängliche weitere Plug-Ins. Diese Mail-Programme übernehmen dann die Aufgabe der Signierung beispielsweise von Mail-Anhängen und sorgen für das Übermitteln des signierten Dokuments.

8.4 Signaturgesetz

Viele rechtliche Vorgänge, die theoretisch elektronisch abgewickelt werden könnten, leiden unter bestimmten Formerfordernissen, wie sie im BGB festgeschrieben sind. Dazu gehört das Definieren von Unterschriften, Urkunden und Zertifikaten, bzw. in welchen Vorgängen diese erforderlich sind.
Aus diesem Grund wurde 2001 ein Signaturgesetz (SigG) verabschiedet, welches im genauen Wortlaut „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“ heißt. Ziel des SigG war es einerseits, eine erhöhte Rechtssicherheit für das E-Commerce zu erhalten und andererseits, eine elektronische Willenserklärung, welche Grundlage für den Abschluss bestimmter elektronischer Verträge ist, in ihrer rechtlichen Stellung und Beweiskraft der ursprünglichen handschriftlichen Unterschrift gleichzustellen. Dazu wurde eingangs festgehalten, dass das SigG „Rahmenbedingungen für elektronische Signaturen“ einrichten soll. Bewusst wurde dabei die Wortwahl ‚elektronisch’ und nicht nur ‚digital’ eingesetzt, um mit diesem Gesetz auch zukünftige Entwicklungen möglichst abdecken zu können, soweit diese vorhersehbar waren.

8.4.1 Begriffsbestimmungen

Das SigG grenzt im $ 2 – Begriffsbestimmungen ein, was im Sinne des SigG eine elektronische Signatur darstellt: „*Elektronische Signaturen* [sind] Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.“[17]
Wie in Kapitel 2 gesehen wurde, erfüllt S die Bedingungen an eine elektronische Signatur. Um die notwendigen Begriffe der fortgeschrittenen und qualifizierten elektronischen Signatur klären zu können, muss man weitere Begriffe einführend betrachten.
Nach SigG „sind *Signaturschlüssel* einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden.“

[17] § 2 (Nr. 1) [11]

Dagegen definiert das SigG *Signaturprüfschlüssel* als „elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.“[18]
Zusammenfassend lässt sich also festhalten, dass die Signaturschlüssel die privaten Schlüssel und die Signaturprüfschlüssel die öffentlichen Schlüssel eines Anwenders sind.
Das SigG beschreibt im § 2 (Nr. 8) Zertifizierungsdiensteanbieter und meint damit „natürliche oder juristische Personen, die qualifizierte Zertifikate [...] ausstellen.“
Wichtig ist der Begriff des Zertifikats. *Zertifikate* im Sinne des SigG sind „elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird.“ [19]
Ein Zertifikat fasst also personengebundene allgemeine Daten und den personengebundenen öffentlichen Schlüssel in einer geeigneten Form zusammen.
Weithaus enger wird dann der Begriff des *qualifizierten Zertifikats* gefasst. Nach dem SigG ist ein Zertifikat ein qualifiziertes Zertifikat, wenn es neben der allgemeinen Zertifikats-Eigenschaft auch noch § 7 SigG (Inhalt von qualifizierten Zertifikaten) genügt und darüber hinaus „von Zertifizierungsdiensteanbietern ausgestellt wurde, die mindestens die Anforderungen nach den §§ 4 bis 14 oder § 23 dieses Gesetzes [SigG] und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen.“[20]
Nachdem die wichtigsten Begriffe eingeführt wurden, kann nochmals spezieller auf die elektronische Signatur eingegangen werden.
Um weitere Rechtssicherheit zu erlangen, muss die allgemeine Definition einer elektronischen Signatur enger gefasst werden. Hierzu führt der Gesetzgeber im nächsten Schritt die *fortgeschrittene elektronische Signatur* ein. Fortgeschrittene elektronische Signaturen sind nach SigG § 2 (Nr. 2) elektronische Signaturen, die

1. ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
2. die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
3. mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
4. mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Eine fortgeschrittene elektronische Signatur ist qualifiziert, wenn sie zusätzlich „auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht“ und „mit einer sicheren Signaturerstellungseinheit erzeugt wurde.“
Sichere Signaturerstellungseinheiten sind „Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, [...] die für qualifizierte elektronische Signaturen bestimmt sind.“[21]

[18] § 2 (Nr. 4) und § 2 (Nr. 5) [11]
[19] § 2 (Nr. 6) [11]
[20] § 2 (Nr. 7) [11]
[21] § 2 (Nr. 3) [11]

In der Regel sind solche Signaturerstellungseinheiten heutzutage Karten-Lesegeräte und Chip-Karten, auf denen die privaten Schlüssel gespeichert sind. Der private Schlüssel wird auf dieser Chip-Karte nicht im Klartext gespeichert, sondern erzeugt. Dazu muss eine geeignete Chip-Karte, deren Anforderungen durch DIN V 66291-1 spezifiziert werden, einen eigenen Prozessor besitzen und PIN-geschützt sein.
Zusammenfassend hier nun eine Übersicht der möglichen Signatur-Varianten:
Warning: TRIAL RESTRICTION – Table omitted!
Die einfache elektronische Signatur wie auch die fortgeschrittene elektronische Signatur werden in der EU-Richtlinie[22] und im SigG nur definiert. Nähere rechtliche Anforderungen und damit verbundene Rechtswirkungen werden nur an die beiden letzten Signaturen (qualifizierte elektronische Signatur und qualifizierte elektronische Signatur mit Anbieter-Akkreditierung) gestellt. (nach [23])
Letzteres hat zur Folge, dass im Allgemeinen nur qualifizierte elektronische Signaturen rechtlich als Äquivalent zur eigenhändigen Unterschrift anerkannt werden. Vertragspartner können aber trotzdem auch eine andere Form vereinbaren (BGB § 127) und sich damit insbesondere auf vereinfachte elektronische Signaturen verständigen.
Die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung bietet heutzutage das höchste Maß an Sicherheit. Anbieter-Akkreditierung meint (in Deutschland), dass sich der Anbieter von qualifizierten Zertifikaten besonderen Prüfungsmechanismen durch Dritte (z.B. TÜV) unterziehen muss. In Deutschland ist diese besondere Form des Anbietens eines Zertifizierungsdienstes freiwillig. Anders zum Beispiel in der Schweiz wo die EU-Richtlinie in der Form umgesetzt wurde, dass es nur besonders akkreditierte Zertifizierungsdiensteanbieter gibt.
Das SigG in der Fassung vom Mai 2001 ist bis heute weiteren Änderungen ausgesetzt worden. Diese Änderungen wurden teilweise von der Wirtschaft (vornehmlich Banken) gewünscht bzw. von der politischen Opposition gefordert.

8.5 Elektronischer Vertragsabschluss

Vorraussetzungen für das Durchführen elektronischer Vertragsabschlüsse waren einige Gesetze und Verordnungen, die in den letzten Jahren verabschiedet wurden, um den Menschen die Möglichkeit der Nutzung der neuen Medien zu ermöglichen. Mehr und mehr nimmt dabei das Medium Internet eine dominierende Rolle ein, wenn es um den wirtschaftlichen Handel und damit auch um die rechtliche Stellung des wirtschaftlichen Handels geht.
Folgende Gesetze und Verordnungen wurden dazu verabschiedet oder verändert[24]:

- Signaturgesetz SigG
- Signaturverordnung SigV („Die Signaturverordnung ergänzt das SigG um Einzelregelungen zu den Anforderungen an die Zertifizierungsdiensteanbieter sowie an

[22] [05]
[23] [04]
[24] nach [03]

die bei der Zertifikats- und Signaturerstellung einzusetzenden Produkte und Verfahren. Sie konkretisiert darüber hinaus die Kostenregelung in § 22 SigG. In der Anlage 1 macht sie zudem detaillierte Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen."[25])

- Bürgerliches Gesetzbuch BGB
- Verwaltungsverfahrensgesetz (§ 3a zur elektronischen Kommunikation und § 37 zum elektronischen Verwaltungsakt)
- Formanpassungsgesetz (regelte die Änderung unzähliger weiterer Rechtsvorschriften; z.B. wurde im BGB der Wortlaut „schriftlich" durch „in Textform" ersetzt um damit der Gleichstellung der schriftlichen und elektronischen Dokumente Rechnung zu tragen)
- Weitere EU-Vorschriften und EU-Richtlinien

Viele Dinge aus der vorherigen allgemeinen Betrachtung über Vertragsabschlüsse lassen sich sofort auf elektronische Vertragsabschlüsse übertragen.
Auch ein elektronischer Vertrag kann nur dann abgeschlossen werden, wenn die gemeinschaftlichen Willenserklärungen der Vertragspartner vorliegen. Im Grunde stellt ein elektronisch abgeschlossener Vertrag lediglich eine „Spezialform" eines althergebrachten Vertragsabschlusses dar.
Der Unterschied liegt in der Art und Weise der Erklärung des Willens bzw. in der Übermittlung des Willens.
Zuerst muss die Frage geklärt werden, ob es sich um Willenserklärungen anwesender oder abwesender Vertragspartner handelt. Anwesend sind die Vertragspartner nur dann, wenn sie über das Internet direkt verbunden sind, z.B. in Form eines Chats oder einer Videokonferenz. Rein rechtlich nehmen diese Übertragungsmedien dann die Position einer fernmündlichen Übertragung ein, die vergleichbar mit althergebrachter Telephonie ist.
Werden die Willenserklärungen der Vertragspartner jeweils an die (virtuelle) Mail-Box via E-Mail versand, kann nicht mehr von Willenserklärungen zwischen Anwesenden gesprochen werden. Es liegt demnach ein Abwesendheitsverhältnis vor. Dieses Abwesendheitsverhältnis hat zur Folge, dass die für die Rechtswirksamkeit eines Vertrages unter Abwesenden notwenige Verkörperung von einer externen Software übernommen werden muss. Dies geschieht entweder auf Seiten des E-Mail-Providers oder direkt auf dem Rechner des jeweiligen Vertragspartners, indem dort die Nachricht bzw. das Dokument persistent auf einem nicht-flüchtigen Speichermedium festgehalten wird. Das Aufbewahren auf Speichermedien, wie der Festplatte, erfüllt die Vorrausetzungen der Verkörperung.
Zwischen einem elektronischen Postfach (Mail-Box) und dem gewöhnlichen Postfach an jeder Tür lassen sich in jedem Fall gewisse Parallelen ziehen: Rechtlich hat das elektronische Postfach ähnliche Eigenschaften wie das gewöhnliche Postfach. So bedarf es nach

[25] aus [06]

wie vor keiner genaueren Prüfung, ob ein Adressat seine Post aus dem Briefkasten entfernt hat, bzw. ob er die Post gelesen oder ungelesen entfernt und vernichtet hat. Diese und weitere denkbare Abläufe mit der Post im Briefkasten finden im realen wie auch im virtuellen Postfach gleichermaßen statt. Ob elektronisch oder nicht, in jedem Fall hat der Sender sein Mögliches getan, sobald seine Willenserklärung im Hoheitsbereich des Empfängers liegt, also im elektronischen oder im gewöhnlichen Postfach.

8.5.1 Elektronischer Vertragsabschluss ohne Signatur

Dieser Abschnitt zeigt am Beispiel eines Online-Shops, dass es heutzutage gängige Praxis ist, Verträge auf elektronischer Basis abzuschließen, die keiner gesonderten elektronischen Signatur bedürfen.
In der „realen“ Welt, wie auch in der digitalen Welt, ist die Frage nach dem Antragenden und dem Annehmenden für den Abschluss eines Vertrages über einen bestimmten Gegenstand von großer Bedeutung. Gerade in der elektronischen Welt des Internets kann diese Frage nicht immer eindeutig geklärt werden. Es ist also wichtig, möglichst genau den Antragssteller zu identifizieren, denn nur das Zusammenspiel zwischen Antragssteller auf der einen Seite und Annehmer dieses Antrages auf der anderen Seite bildet die Grundlage für das Zustandskommen und Abschließen von wirksamen Verträgen.
Beispielsweise gibt es heutzutage unterschiedliche Auffassungen, ob der Betreiber eines Online-Shops die Rolle des Antragenden oder die des Annehmenden ausübt. Im Allgemeinen wird jedoch davon ausgegangen, dass der Kunde, der den Online-Shop besucht, dem Händler ein Angebot macht, daher also die Rolle des Antragenden übernimmt. Durch das Ausfüllen eines elektronischen Bestellformulars erklärt er seinen Willen, die aufgeführten Produkte käuflich erwerben zu wollen. Ist der Händler in der Lage zu liefern, so muss er in der Regel per Mail dem Kunden eine Empfangsbestätigung zukommen lassen. Diese Empfangsbestätigung wird nach heutiger Rechtsaufassung als Willenserklärung des Händlers verstanden, muss aber dem Kunden die Möglichkeit eines Rücktrittes (Widerruf) von der Bestellung einräumen. Durch die Verwendung so genannter Allgemeiner Geschäftsbedingungen (AGB) kann der Händler seinen Willen teilweise im Vorfeld verklausulieren. Sie können dann wirksamer Bestandteil eines Vertrages werden, allerdings nur dann, wenn es dem Kunden zumutbar ist, diese auch in angemessener Zeit lesen zu können und wenn sie direkt in den Vertrag eingebunden werden. Dazu werden im Falle des Online-Shops die AGB in der Regel direkt per Link eingebunden und ihre Kenntnisnahme muss explizit bestätigt werden, bevor der Kunde seinen Willen erklären kann. Damit will man unter anderem auch vermeiden, dass Kunden nicht als Folge eines Reflexes einen ungewollten Antrag abgeben können, da der subjektive Handlungswille Vorraussetzung einer wirksamen Willenserklärung ist. Inwieweit man hier als Antragender erklären kann, „aus Versehen“ einen damit nichtigen Willen erklärt zu haben, bleibt freilich fraglich.
Anders liegt der Fall, wenn beispielsweise der Betreiber eines Online-Shops seinen Internet Auftritt derart unübersichtlich gestaltet, dass der Kunde im Bewusstsein des Erhaltens weiterer Informationen zu einem Artikel einen Bestellvorgang auslöst. Aus Betreibersicht ist es allerdings auch jetzt nicht nachvollziehbar, ob der Kunde ordnungs-

gemäß seinen Willen erklärt hat oder „Opfer“ irreführenden Designs geworden ist. Aus Kundensicht ist es dann sicher einfacher, von dem Recht des Widerrufs gebrauch zu machen.

8.5.2 Elektronischer Vertragsabschluss mit Signatur

Die elektronische Signatur als Äquivalent zur eigenhändigen Unterschrift soll in Zukunft (fast[26]) überall dort eingesetzt werden, wo heutzutage Vertragsabschlüsse mit eigenhändiger Unterschrift erforderlich sind.
Nachfolgend werden einige Beispiele bzw. Einsatzgebiete vorgestellt.
Viele Vorgänge, die heutzutage zwingend auf einem öffentlichen Amt erledigt werden müssen, beispielsweise das Antragen von Bafög- oder Wohngeld könnte in Zukunft von zu Hause aus mit einer qualifizierten elektronischen Signatur durchgeführt werden. Dazu bräuchten lediglich entsprechende Dokumente vom Antragssteller elektronisch signiert werden, womit dem Amt ein rechtswirksamer Antrag vorliegen würde.
Es existieren darüber hinaus im Geldgeschäft noch Erfordernisse, die den Weg zur Bank und damit die eigenhändige Unterschrift nach sich ziehen – trotz Online Banking.
Auch andere Abläufe, wie das Abgeben eines Angebots zu einer öffentlichen Ausschreibung (Verdingungswesen) sollen in Zukunft elektronisch signiert werden können.
Seitens der Bundesregierung wurden weitere Projekte ins Leben gerufen, die quasi als Vorreiter der elektronischen Signierung dienen sollen: die Gesundheitskarte, die Jobcard und der digitale Personalausweis.
Die Gesundheitskarte soll nach dem Willen der Regierung einerseits als „Speicher für elektronische Rezepte“ dienen und andererseits „Informationen für eine Notfallversorgung, Arzneimitteldokumentationen, den elektronischen Arztbrief und die elektronische Patientenakte“ beinhalten.[27]
„Die Jobcard soll Zugriff auf die Daten aller Arbeitnehmer zu den Beschäftigungszeiten, zur Höhe von Entgeltzahlungen sowie zur Auflösung des Beschäftigungsverhältnisses ermöglichen.“[28] Das hat zur Folge, dass bestimmte Vorgänge beispielsweise in den Arbeitsämtern schneller und effizienter gestaltet werden können.
Im Abschnitt 3.2 Elektronische Signatur wurde im Zusammenhang der Definition Elektronische Signatur auf mögliche weitere Einsatzfelder hingewiesen.

8.6 Probleme der Elektronischen Signatur

In den bisherigen Kapiteln der Arbeit wurden Grundlagen im Vertragsrecht und für die elektronische Signatur erläutert. Dann wurde das Verfahren der elektronischen Signatur eingeführt, um elektronische Vertragsabschlüsse durchführen zu können.

[26] Ausnahmen bilden beispielsweise notarielle Einträge, Eheschließungen oder das eigene Testament. Diese Vorgänge müssen weiterhin handschriftlich signiert werden.
[27] [07]
[28] [07]

Im letzten Abschnitt sollen nun bestimmte Probleme vorgestellt werden, die insbesondere mit der Verwendung der elektronischen Signatur auftreten.

8.6.1 Aufwand

Von circa 3800 Rechtsvorschriften müssen ein Großteil der Vorschriften überarbeitet werden, damit der Einsatz der elektronischen Signatur Realität werden kann.[29]

8.6.2 Gültigkeit einer Signatur – Nachsignierung

Zertifizierungsdiensteanbieter ohne besondere Akkreditierung haben die Auflage, öffentliche Schlüssel über den Zeitraum von 5 Jahren aufzubewahren. Zertifizierungsdiensteanbieter mit Akkreditierung müssen ihrerseits die Zertifikate 30 Jahre zugänglich halten. Ob so oder so, es gibt immer Verträge, die beispielsweise ein gesamtes Menschenleber oder auch darüber hinaus gültig sein sollen.
Was dann nach Ablauf der Frist erfolgen muss, ist eine Nachsignierung. Damit ist eine Auffrischung der elektronischen Signatur gemeint, damit diese weiterhin ihre Gültigkeit hat. Es ist leicht vorzustellen, dass diese Nachsignierung in der Zukunft ein relativ komplexes Problem darstellen wird.

8.6.3 Sicherheit der elektronischen Signatur

Der elektronischen (auch der qualifizierten elektronischen) Signatur ist nicht anzusehen, ob sie möglicherweise von einer nicht-autorisierten Person stammt. Dieser Fall könnte vorliegen, wenn jemand in den Besitz der Chipkarte einer zweiten Person gelangt ist. Mit dieser Chip-Karte gelangt der Betrüger auch in den Besitz des privaten Schlüssels. Diese Chip-Karte ist zwar PIN-geschützt, doch kann davon ausgegangen werden, dass das Vorhandensein dieser PIN keinen ausreichenden Schutz gewährleisten kann, da sie ausgespäht werden könnte. Kennt der Betrüger auch noch die persönlichen Angaben des Bestohlenen, so kann er damit auch in den Besitz des öffentlichen Schlüssels kommen. Damit verfügt er über alle Mittel, um im Namen der geschädigten Person signierte Dokumente zu verschicken, mit allen daraus denkbaren Konsequenzen.
Dieser Fall ist vergleichbar mit dem Verlust der EC-Karte. Merkt man den Verlust nicht rechtzeitig, wird der Betrüger unter Umständen (falls er ebenfalls in den Besitz der PIN gelangt ist) unrechtmäßig Geld abheben können.

8.6.4 Rechtliche Fragestellungen

Bei der qualifizierten elektronischen Signatur bleibt offen, ob das Eintippen einer PIN als echte Willenserklärung gelten kann. Um an seinen privaten Schlüssel zu gelangen, muss man mittels der Chip-Karte und des Kartenlesegerätes diesen Schlüssel von der Chip-Karte auslesen. Das Auslesen ist durch eine PIN geschützt. Nachdem man die PIN

[29] [08]

eingetippt hat, wird der private Schlüssel ausgelesen und die Signatur erzeugt, die mit dem Dokument unter Umständen sofort und automatisch verschickt wird. Das Erstellen der Signatur wird dazu z.B. in ein Mail-Client integriert.
Weiterhin ist es unklar, „wo unterschrieben“ werden soll. Bei einem Papierdokument wird immer unterhalb des Textes unterschrieben. Unterschriften oberhalb eines Dokuments sind rechtlich nicht verbindlich. Gilt dies auch für die elektronische Signatur?
Wird die elektronische Signatur Dokument-extern erstellt, also in einer externen Signaturdatei, lässt es die menschliche Vorstellungen eigentlich nicht mehr zu, von einem elektronischen Adäquat zur menschlichen Unterschrift zu sprechen, da man dann mindestens zwei Dateien erhält. Ein weiteres Problem ergibt sich, wenn man nur Teile eines Dokumentes signieren will. Darum kann man die elektronische Signatur auch in das zu signierende Dokument einbetten. In diesem Zusammenhang spricht man von einer Content-Signatur[30] Jetzt hat man die Möglichkeit, Einfluss darauf zu nehmen, welche Teile des Dokumentes signiert werden sollen und eben welche nicht. Dazu kann man so genannte Mehrfachsignaturen benutzen. Die Frage welche der beiden Varianten für den betrachten Rechtsfall ausschlaggebend und gültig ist, muss dann immer im Detail geklärt werden, was nicht selten ein umfangreiches Studium der (neueren) Gesetzestexte zur Folge hat. In den meisten Fällen sollte man sich wohl für eine eingebettete Signierung entscheiden, wenn es der Typ des Dokuments zulässt.
Eine weitere Fragestellung lässt sich aufgrund der Eigenschaften elektronischer Texte ableiten. Ist jemand gezwungen, ein Dokument zu signieren, so muss er sich fragen. welcher Text überhaupt „zur Unterschrift“ vorliegt. Ist es der Text, den die Person sehen kann? Oder verbirgt sich dahinter weitaus mehr? Letzteres wird möglich, wenn man sich vorstellt, dass jemand vor dem Signierungsprozess ein Dokument derart manipuliert hat, dass gewisse Textpassagen „etwa durch entsprechend gewählte Farbgebung ausgeblendet“[31] wurden.
Seitens der Wirtschaft (hier vornehmlich die Banken, die ebenfalls als Zertifizierungsdiensteanbieter fungieren) wurde auf eine Entschärfung des Signaturgesetzes gedrängt, um dadurch den Kunden leichter eine Signaturkarte aushändigen zu können, da die persönlichen Daten der Kunden vorliegen würden.

8.6.5 Allgemeine Akzeptanz

Der Einsatz von elektronischen Signaturen würde in vielen Bereichen des öffentlichen Lebens gewisse Ersparnisse einbringen. Diese Ersparnisse müssten im Umkehrschluss wieder an den Endverbraucher sei es über Steuervergünstigungen oder Preissenkungen abgegeben werden. Nur so kann dem Verbraucher die Signaturkarte „schmackhaft“ gemacht werden. Denn das Besorgen der qualifizierten elektronischen Signatur, der Signaturkarte und des Lesegerätes ist für die meisten Normalbürger schlichtweg zu teuer. (Nutzen-Aufwand-Verhältnis)
Doch bis jetzt scheitert es nicht nur an den Verbrauchern. Selbst von Seiten der Industrie

[30] nach [03]
[31] aus [03]

wird das gesamte Projekt Elektronische Signatur nicht ausreichend getragen. Gründe dafür liegen vor allem in einem großen Verwaltungs- und Administrationsaufwand, gerade in der Einrichtungsphase. (Stichwort Public-Key-Infrastructure PKI)
Ein weiterer Punkt, der der allgemeinen Akzeptanz nicht gerade förderlich ist, ist die Tatsache, dass es zur Zeit immer noch unterschiedliche Standards gibt und es nicht abzusehen ist, welche Standards sich letztlich durchsetzen werden.

8.7 Fazit

Die vorliegende Arbeit hat mögliche Einsatz- sowie Problemfelder der elektronischen Signatur als grundlegendes Beweismittel beim Abschluss elektronischer Verträge zusammengefasst.
Der Knappheit des Umfanges ist es verschuldet, dass einige Bereiche nicht mit der nötigen Detailtiefe bearbeitet wurden. Dem Gesamtverständnis ist dies jedoch nicht hinderlich.

Literaturverzeichnis

[1] *Brockhaus Lexikon in drei Bänden.*

[2] *Bürgerliches Gesetzbuch.*

[3] *EU-Richtlinie 2000/31/EG, Richtlinie über den elektronischen Geschäftsverkehr.*

[4] *Informationen zur Teilnahme am Public Key Service.*

[5] *Leitfaden Elektronische Signaturen.*

[6] *Signaturgesetzt SigG.*

[7] *Verfahren der elektronischen Signatur.* http://www.izn.niedersachsen.de/master/C5833088_N5676755_L20_D0_I3654280.html.

[8] *Wikipedia.* http://de.wikipedia.org/wiki/Digitale_Signatur.

[9] *Wikipedia.* http://de.wikipedia.org/wiki/Signaturverordnung.

[10] S. 32 c't 10/2004. Signaturbündnis, gesundheitskarte, jobcard. http://www.heise.de.

[11] S. 58 c't 1/1999. Digitale signatur. http://www.heise.de.

[12] Dr. Hermann Fahse, uberarbeitet von Dr. Justus Woydt. *Grundzüge des Zivilrechts für Ingenieure.* 2005.

9 Social Engineering

Stephan Müller, Christian Tinnefeld

9.1 Einleitung

Informationssicherheit ist ein wichtiges Thema bei Unternehmen, da Information ein Produktionsfaktor ist und somit über den finanziellen Erfolg einer Unternehmung entscheidet. Da heutzutage Informationen fast ausschließlich unter Zuhilfenahme von IT-Systemen erfasst, verarbeitet und übermittelt werden, versuchen Unternehmen ihre IT-Systeme und die damit verbundene Infrastruktur bestmöglich zu schützen. Im Jahr 2004 gaben Unternehmen weltweit 3,7 Milliarden USD für Netzwerksicherheit aus [15], für 2007 wird ein weltweiter Umsatz mit Antiviren-Software von 4,4 Milliarden USD projiziert [8].
Diese Maßnahmen etablieren einen gewissen Schutz vor technischen Angriffen. Allerdings bieten Sie keinen Schutz vor der Manipulation von Mitarbeitern. Da Mitarbeiter natürlich Zugriff auf die Daten ihres Unternehmens haben müssen, nützen die besten Firewalls und die komplexesten Verschlüsselungsmechanismen nichts, wenn ein Angreifer es schafft, dass ihm ein Mitarbeiter direkt die gewünschten Informationen aushändigt. Jedoch wird ein Mitarbeiter nicht direkt auf Anfrage beliebige Firmeninformationen preisgeben. Deshalb ist es notwendig den Mitarbeiter zu täuschen und ihn unter der Vorgabe falscher Tatsachen zur Informationspreisgabe zu bewegen. Diese Methodik bezeichnet man als Social Engineering.
Nach einer Einführung im ersten Kapitel werden in diesem Bericht im zweiten Kapitel die Vorgehensweise und die angewandten Techniken eines Social Engineers beschrieben. Im dritten Kapitel werden Gegenmaßnahmen vorgestellt und evaluiert, das vierte Kapitel bietet eine Zusammenfassung.

9.1.1 Risikofaktor Mensch - psychologische Grundlagen

Die Basis von Social Engineering ist die gezielte Manipulation von anderen Menschen. Der Erfolg dieser Manipulation beruht auf psychologischen Effekten [6]. Um ein tief greifendes Verständnis von Social Engineering zu erhalten, und um mögliche Gegenmaßnahmen bewerten zu können, ist es notwendig diese psychologischen Grundlagen zu verstehen.

Handlung im Affekt

Man spricht von einer Handlung im Affekt, wenn eine Person ein starkes Gefühl der Überraschung, Anteilnahme oder Wut empfindet und davon sein weiteres Handeln beeinflusst wird. Dieses Gefühl kann hervorgerufen werden, wenn zum Beispiel die Reaktion oder die Aussage eines anderen Menschen weit außerhalb des erwarteten Spektrums liegt. Diese Gefühle reduzieren den Anteil der logischen und rationalen Gedanken bei der Entscheidungsfindung für nachfolgende Handlungen. Dieses kontrafaktische Denken bezeichnet man auch als Handlung im Affekt [11].

Informationsüberladung

Gezielte Fehlinformationen bleiben unentdeckt, wenn sie im Rahmen bekannter Wahrheiten und in einer Informationsflut präsentiert werden, die eine Evaluierung von einzelnen Aussagen unmöglich macht. Wenn Menschen zu viel Informationen verarbeiten müssen, werden sie *"mental passiv und absorbieren Informationen, anstatt sie zu verarbeiten"*[2]. Auch die Argumentation aus einer unerwarteten Perspektive kann zu einer Informationsüberladung führen. Durch diese Konfrontation bleibt nicht genügend Zeit um die neuen Argumente zu evaluieren [10].

Reziprokation

Eine Regel des sozialen Verhaltens besagt, dass man einen Gefallen mit einer Gegenleistung quittiert. Dies trifft sogar zu, wenn der initiale Gefallen gar nicht gefordert worden war oder wenn die Gegenleistung wesentlich umfangreicher ist. Dieses Verhalten wird als Reziprokation bezeichnet [11].
Eine weitere Form der Reziprokation wird durch Verhaltensexperimente belegt, in denen zwei Personen ein Streitgespräch führen. Lenkt nun einer der beiden Gesprächspartner bei einem Diskussionspunkt ein, fühlt sich die andere Person ebenfalls verpflichtet einzulenken [3].

Autorität

Die meisten Menschen sind so erzogen worden, dass sie eine Autoritätsperson respektieren und ihre Anweisungen befolgen. Das kann sogar soweit gehen, dass sie auch dann den Befehlen einer Autoritätsperson gehorchen, wenn sie die Befehle nicht nachvollziehen können oder sie sogar für falsch erachten.
Ein berühmtes Beispiel hierfür ist das Milgram-Experiment [13], bei dem Probanden unter dem Einfluss einer Autoritätsperson bereit waren, anderen Probanden ernsthafte gesundheitliche Schänden zuzufügen [14].

Verantwortlichkeit und Gewissen

Menschen vernachlässigen bei Ihrer Entscheidungsfindung die Beachtung von Richtlinien, wenn man sie darauf aufmerksam macht, dass ihre Entscheidung direkte Konse-

quenzen trägt, für die sie voll verantwortlich sind. Sowohl die Aussicht auf persönliche Nachteile in gesellschaftlicher oder finanzieller Form, aber auch die Möglichkeit durch die eigene Entscheidung einem anderen Menschen zu schaden, beeinflusst einen Menschen so zu handeln, dass die möglichen negativen Konsequenzen nicht eintreten.

Etablierung einer Beziehung

Menschen stehen mit anderen Menschen in einer sozialen Beziehung. Die verschiedenen Beziehungen können dadurch klassifiziert werden, in welchem Kontext oder zu welchem Zweck sie etabliert worden sind (Geschäftspartner, Freunde, Kommilitonen etc). Die Tatsache, dass einem andere Menschen sympathisch sind oder man sie eventuell nicht leiden kann, lässt eine emotionale Bewertung der einzelnen Beziehung zu.
Bei der Etablierung einer Beziehung zu einem anderen Menschen spielt die Identifikation mit dem anderen Menschen eine große Rolle: kann man sich mit der Situation, der Persönlichkeit oder mit den Problemen von einem anderen Menschen identifizieren, erscheint einem die andere Person meistens sympathisch [11].

9.2 Social Engineering

Wie schon die psychologischen Grundlagen andeuten, ist Social Engineering keine Technik, die man sich nach einem vorgegebenen Schema aneignen kann. Ein erfolgreicher Social Engineer benötigt nicht nur zwischenmenschliches Feingefühl, sondern auch reichhaltige Erfahrungen im Umgang mit anderen Menschen. Ein berühmter Social Engineer ist Kevin Mitnick. Mitnick gilt als einer der bekanntesten Hacker, der sich im Laufe seiner Karriere nicht nur in zahlreiche Großunternehmen hackte, sondern auch Zugriff zu Rechnern von Behörden und Militär erlangte. Mitnick wurde 1995 vom FBI festgenommen und zu fünf Jahren Haft verurteilt. Nach seiner Haftstrafe hat er ein Buch mit dem Titel *Die Kunst der Täuschung* [9] verfasst, in dem er beschreibt, dass er die meisten sensitiven und geheimen Informationen nicht durch die Ausnutzung von technischen Schwachstellen erlangt hat, sondern durch das Anwenden von Social Engineering.
Kevin Mitnick definiert den Begriff Social Engineering wie folgt:

> Social Engineering benutzt Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, über die sich ein Social Engineer eine gefälschte Identität aneignet. Damit kann der Social Engineer andere zu seinem Vorteil ausbeuten, um mit oder ohne Verwendung von technischen Hilfsmitteln an Informationen zu gelangen [9].

9.2.1 Phasen des Social Engineering

Ein Social Engineering Angriff lässt sich in vier Phasen unterteilen: in der ersten Phase recherchiert der Angreifer und beschafft sich alle für seinen Angriff relevanten Informationen. Diese nutzt er in der zweiten Phase, um zu seinem Opfer ein Vertrauensverhältnis aufzubauen. Dieses Vertrauensverhältnis missbraucht der Angreifer in der dritten Phase,

in dem er sein Opfer zur Informationspreisgabe verleitet. In der vierten Phase kann er die gewonnenen Informationen beliebig missbrauchen.

Recherche

Bei der Recherche kann man zwischen zwei Kategorien unterscheiden: zum einen welche Informationen benötigt werden und zum anderen wie man an diese Informationen gelangen kann.
Die wichtigsten Informationen, die man bei einem Social Engineering Angriff benötigt, werden als Domainwissen bezeichnet. Zum Domainwissen gehören zum Beispiel Sprachcodes. Gibt sich ein Angreifer bei einem Telefonat mit einem Bankmitarbeiter als Kollege aus, darf er nicht ins Stocken geraten, wenn er mit Begriffen konfrontiert wird, die in der Bankenbranche allgemein üblich sind. Auch die Gewohnheiten einer Person, bzw. der Workflow in einem Unternehmen sind wichtige Informationen bei der Vorbereitung. Durch die Analyse von Arbeitsabläufen lassen sich zum einen Schwachstellen identifizieren und zum anderen haben Angriffe eine höhere Erfolgschance, wenn sie für das Opfer als normaler Arbeitsalltag dargestellt werden können. Die Identifzierung von relevanten Personen ist ein weiterer Schlüsselfaktor, da sie nicht nur eine Liste von möglichen Angriffspunkten darstellt, sondern auch eine Auswahl von Identitäten ist, die man sich bei dem Angriff aneignen kann.
Bei der Art der Informationsbeschaffung gibt es mehrere Alternativen. Durch die Brille eines Social Engineers ist es erstaunlich wie viele wertvolle Informationen Unternehmen einfach so preisgeben: im Geschäftsbericht finden sich Mitarbeiter-Organigramme, direkte Durchwahlnummern sind auf der Unternehmenshomepage hinterlegt und Mitarbeiter eines Unternehmens klagen in Internetforen über ihre Probleme unter Angabe der Firmen-Emailadresse. Doch die Kreativität eines Social Engineers bei der Informationsbeschaffung geht über die Mittel der klassischen Recherche hinaus: unter Dumpster Diving versteht man die Suche nach Informationen im Müll eines Unternehmens. Dies ist aus strafrechtlicher Sicht besonders interessant, da Müll nicht mehr unter das Datenschutzgesetz fällt und sich der Angreifer bei dieser Art der Recherche nicht einmal strafbar macht. Es gibt sogar Berichte, laut denen Oracle Dumpster Diving bei Microsoft betrieben haben soll, um an geheime Informationen zu gelangen [12].

Entwicklung von Beziehung und Vertrauen

Nachdem der Angreifer die benötigten Informationen zusammengetragen hat, kann er mit dem eigentlichen Angriff beginnen. Nun versucht er eine Beziehung zu seinem Opfer aufzubauen. Dabei ist die Aneignung einer falschen Identität von großer Hilfe, denn man misstraut einem Fremdem eher als einem vermeintlichen Kollegen oder Bekannten. Die Aneignung der fremden Identität kann durch so einfache Maßnahmen erfolgen, wie das Melden am Telefon mit einem fremden Namen bis hin zu einer Verkleidung mit Blaumann und Werkzeugkasten. Auch wenn der Auftritt als Handwerker beim Opfer nicht die Zuordnung zu einem bekannten Namen bewerkstelligt, ist dennoch davon auszugehen, dass kein Misstrauen auftritt, da man mit der Rolle des Handwerkers automatisch

die Zutrittsberechtigung zu Räumlichkeiten assoziiert.
Weitere Möglichkeiten um eine Beziehung oder sogar ein Vertrauensverhältnis herzustellen, basieren auf den in der Einleitung erwähnten psychologischen Grundlagen: schafft es ein Angreifer, sich zum Beispiel gegenüber einem Systemadministrator ebenfalls als Systemadministrator auszugeben, der die gleichen Probleme beim Einspielen eines aktuellen Sicherheitsupdates hat, identifiziert sich das Opfer mit dem Angreifer und befolgt eventuell Anweisungen, die zur Lösung des "gemeinsamen" Problems führen. Auch der Respekt vor Autorität kann zur Etablierung einer Beziehung genutzt werden: gibt sich der Angreifer bei einem Angestellten als Autoritätsperson aus, ist es weniger wahrscheinlich, dass dieser kritische Rückfragen stellt. Der Appell an die Hilfsbereitschaft ist eine wirkungsvolle Methode: kein Kollege wird einem vermeintlich anderen Kollegen einen Gefallen abschlagen oder möchte für den Misserfolg eines Projektes innerhalb des Unternehmens verantwortlich gemacht werden können.
Ein beliebter Trick beim Aufbau einer Beziehung ist das so genannte Namedropping [9]. Dabei lässt der Angreifer im Gespräch mit seinem Opfer beiläufig Namen fallen von Personen, die das Opfer kennt. Dadurch suggeriert der Angreifer, dass er mit dem betreffenden Personenkreis vertraut ist.
Reverse Social Engineering beschreibt eine besonders gewiefte Methode zur Vertrauensschaffung. Hierbei verursacht der Angreifer ein Problem, welches das Opfer betrifft. Dann kontaktiert er das Opfer, gibt sich als Hilfe zu dem bestehenden Problem aus und behebt sein selbst verursachtes Problem innerhalb einiger Zeit. Danach vertraut ihm das Opfer und wird weitere Anweisungen vom Angreifer befolgen. Hierzu ein kleines Beispiel: ein Angreifer ist in der Lage die Netzwerkverbindung seines Opfers zu stören (zum Beispiel durch Denial of Service). Er ruft das Opfer an, gibt sich am Telefon als Netzwerkadministrator aus und erklärt dem Opfer, dass es momentan ein Problem im Netzwerk gibt, welches er aber gerade behebt. Nach einiger Zeit unterbricht der Angreifer seine selbst verursachte Störung, kontaktiert wieder sein Opfer und berichtet, dass die Störung behoben sei. Das Opfer ist nun davon überzeugt, dass der Anrufer der Netzwerkadministrator ist und folgt seinen weiteren Anweisungen.

Ausbeutung von Vertrauen

Nach der Etablierung eines Vertrauensverhältnisses wird dieses ausgebeutet, um an die gewünschten Informationen zu gelangen. Je nach der Art der etablierten Beziehung kann sich die Ausbeutung unterschiedlich schwierig gestalten. Hat sich der Angreifer glaubwürdig als Autoritätsperson ausgegeben, dürfte ihm das Opfer alle gewünschten Informationen liefern.
Doch auch in dieser Phase sind die psychologischen Tricks eine wertvolle Hilfe: möchte der Angreifer sein Opfer nur zu einer Handlung bewegen, konfrontiert er es mit mehreren Anfragen und lenkt bei den für ihn unwichtigen Punkten ein. Dadurch wird das Opfer unter Druck gesetzt bei dem verbleibenden Punkt selbst einzulenken (Reziprokation). Die Vorgabe eines falschen Szenarios (zum Beispiel ein schwerer Unfall hat sich ereignet) macht das Opfer empfänglich für Handlungsanweisungen (Handlung im Affekt) [11].
Wenn es der Angreifer bewerkstelligt, seine Attacke im Arbeitsalltag seines Opfers zu

maskieren, bleibt der Angriff an sich vollkommen unbemerkt. Dadurch kann es sogar zu einer Stärkung der Beziehung zwischen Angreifer und Opfer kommen und das Opfer kann wiederholt zur Informationsbeschaffung genutzt werden.

Missbrauch der Information

Die Art und Weise des Missbrauchs der Information hängt von der Art der erbeuteten Information ab. Da Social Engineering in allen Gebieten angewandt werden kann, kann sich demzufolge der Missbrauch auch beliebig gestalten. Die Information kann Teil einer Vorbereitung für einen Hackerangriff sein oder zur Sabotage dienen. Auch ein finanzieller Vorteil durch die Information oder die Möglichkeit zum Identitätsraub sind denkbar.

9.2.2 Kombination von Social Engineering und Technologie

Die Kombination von Social Engineering und Technologie ermöglicht dem Angreifer neue Szenarien: die Täuschung von Menschen ist einfacher, da eine andere Identität zum Beispiel im Internet wesentlich einfacher angenommen werden kann als im richtigen Leben. Durch die automatisierte Manipulation können mehr Opfer kontaktiert werden[9]. Vermutlich jeder Internetnutzer ist schon einmal Opfer einer Social Engineering Attacke geworden. Spam-Emails, die Viren oder Würmer in sich tragen, werden unter anderem als Email von einer netten, jungen Damen verpackt, die dummerweise ihre aktuellen Fotos aus dem Badeurlaub an eine falsche Adresse geschickt hat. Diese Art der Täuschung ist ein klassisches Beispiel für Social Engineering.
Eine besonders clevere Kombination von Technologie und Social Engineering haben Hacker entwickelt, die möglichst viele anonyme Emailkonten erhalten möchten. Freemail Provider haben mittlerweile Sicherheitsabfragen in ihrer Anmeldeprozedur, die nur von Menschen problemlos und fehlerfrei bewerkstelligt werden können (zum Beispiel das Erkennen einer Zahl in einem vorgegebenen Muster). Daher haben die Hacker einen automatisierten Prozeß entwickelt, der diese Abfrage an eine beliebige Anzahl von Emailadressen schickt und dem Empfänger mitteilt, er würde Zugang zu einer Seite mit erotischem Inhalt erhalten, wenn er lediglich die angefügte "Sicherheitsabfrage" löst. Durch das Verschicken an viele Empfänger konnten die Hacker sicher stellen, dass zumindest einer auf den Trick herein fällt und sie weiterhin ohne ihr eigenes Zutun automatisiert Emailaccounts erstellen können.
Auch das Prinzip von trojanischen Pferden basiert auf Social Engineering: das Opfer erhält beispielsweise kostenlos ein Programm, das für ihn einen Mehrwert darstellt und das in seinen Augen auch fehlerfrei funktioniert. Dieses Programm kann ein Tool sein, dass die zum Onlinebanking benötigten Tan-Nummern verschlüsselt auf dem Rechner speichert, damit das Opfer nicht immer die Tan-Liste mit sich führen muss. In Wirklichkeit aber verschickt das Programm die gespeicherten Tan-Nummern an eine vorgegebene Email-Adresse, ohne das das Opfer davon weiß.

Phishing

Das zuletzt beschriebene Exempel ist ein Beispiel für eine Methode die als *Phishing* bekannt ist. Unter Phishing versteht man die Möglichkeit einem Opfer unter Zuhilfenahme der Kombination von Social Engineering und Technologie Daten zu entlocken, die einen Identitätsklau ermöglichen. Dazu können nicht nur trojanische Pferde benutzt werden, sondern auch Emails, die auf die Webseiten der Angreifer verweisen. Diese Webseiten sehen den Webseiten von Organisationen oder Unternehmen, dem das Opfer vertraut ähnlich oder sind sogar identisch. Daher schöpft das Opfer keinen Verdacht und gibt dort seine persönlichen Daten ein oder, falls vorhanden, seinen bestehenden Benutzernamen samt Password. Ein aktuelles Beispiel dafür beschreibt [4], indem Angreifer Opfer auf eine vermeintliche Mastercard-Webseite gelockt haben. Um die Gefahr dieser Attacken einzudämmen, wurde die *Anti-Phishing Working Group* [7] etabliert, die Phishing Webseiten registriert. An Hand dieser Statistik wurde nachfolgende Grafik erstellt.

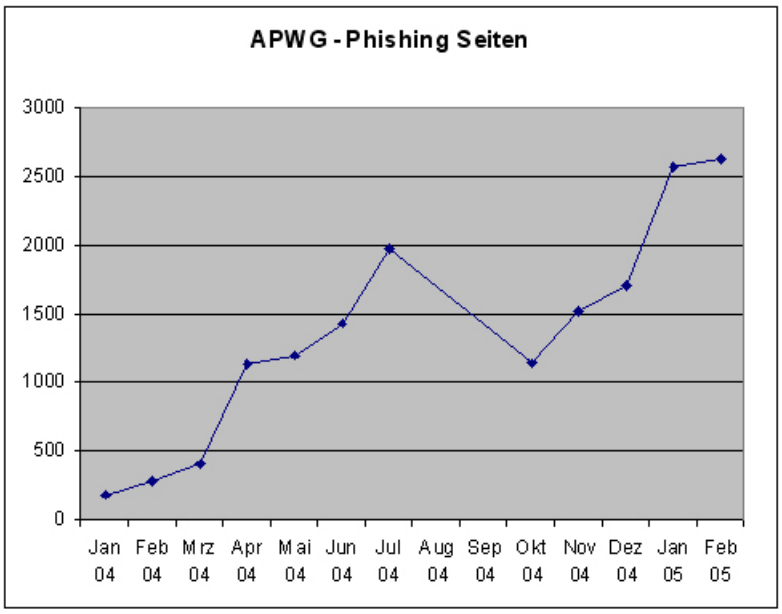


Abbildung 9.1: Phishing Webseiten

Die Grafik lässt erkennen, dass es im letzten Jahr zu einem massiven Anstieg von Phishing Attacken gekommen ist. Die Aussagekraft der absoluten Zahlen muss kritisch betrachtet werden, da längst nicht alle Phishing Versuche auch werden. Dennoch sind sie in Korrelation zueinander bzw. als Indikator aussagekräftig.

9.2.3 Covert Channel

Der primäre Einsatzzweck von Social Engineering ist die Informationsbeschaffung. Eine weitere Möglichkeit der Informationsbeschaffung ist die Nutzung von Covert Channels. Diese Methodik wird nicht primär mit dem Themengebiet Social Engineering assoziiert,

ist aber auf Grund ihrer Charakteristika in diesem Zusammenhang äußerst erwähnenswert.
Unter einem Covert Channel versteht man einen verdeckten Kommunikationskanal [5], der zustande kommt, indem *ein Computermechanisums in einer unerwarteten Weise genutzt wird, um ein Mittel zur Verfügung zu stellen, durch das Information zu einem nicht autorisierten Individuum fließen kann* [1].
Ein konkretes Beispiel für einen Covert Channel kann mit der UNIX-Anmeldeprozedur erklärt werden. Gibt man einen gültigen Benutzernamen ein und ein beliebiges Password, dauert die Überprüfung einige Zeit, da das eingegebene Password gehasht wird und mit dem hinterlegten gehashten Passwordwert verglichen wird. Danach erfolgt eine Meldung, ob die Anmeldung erfolgreich war oder nicht. Gibt man hingegen einen ungültigen Benutzernamen ein, kann dieser Vergleich nicht erfolgen und die Meldung über die gescheiterte Anmeldung erscheint sofort. Auf Grund dieser zeitlichen Verzögerung kann man, sofern das Login-Programm über keine künstliche Verzögerung verfügt, überprüfen ob ein bestimmter Benutzername gültig ist.

9.3 Abwehr von Social Engineering

Nachdem die Social Engineering Attacke und ihre Grundlagen erläutert worden sind, wird nun die Abwehr von solchen Angriffen betrachtet.

9.3.1 Warnzeichen für einen Social Engineering Angriff

Damit eine Person überhaupt bemerken kann, dass sie gerade Opfer einer Social Engineering Attacke ist, muss sie die Warnzeichen eines solchen Angriffs kennen.
Weigert sich ein Anrufer seine Rückrufnummer zu hinterlassen oder lässt er beiläufig bekannte Namen während des Gespräches fallen, sind das eindeutige Hinweise, dass es sich um eine Attacke handeln könnte. Auch das Ausspielen von Autorität bzw. die Vorgabe einer hohen Dringlichkeit sollten die Aufmerksamkeit genauso wecken, wie das Empfangen ständiger Komplimente [9].

9.3.2 Gegenmaßnahmen

Bei den möglichen Gegenmaßnahmen finden sich in der Literatur die verschiedensten Konzepte und Empfehlungen. David Gragg hat in seinem Paper *A Multi-Level Defense Against Social Engineering* [6] die verschiedenen Konzepte zusammengefasst und in fünf Leveln strukturiert.

Foundational Level

Als Basis für die Verteidigung sieht er das so genannte *Foundational Level*. Die Basis dieses Levels ist eine umfassende Sicherheits-Policy. In dieser Policy werden alle sicherheitsrelevanten Aspekte erfasst und reglementiert: die Klassifikation von Informationen

in verschiedenen Stufen, die Zuordnung von Mitarbeitern zu Sicherheitsstufen, die Identifikation und Autorisierung, Richtlinien bei der Erstellung und Änderung von Passwörtern, die Vernichtung von Informationen bis hin zur Begleitung von Besuchern im Unternehmen. Darüber hinaus müssen die Mitarbeiter informiert werden, welche Informationen sie überhaupt nach außen weitergeben dürfen.

Parameter-Level

Im darauf folgenden *Parameter-Level* müssen die Mitarbeiter über Social Engineering aufgeklärt werden und die erstellten Policies verinnerlichen. Auch die Vermittlung von den bereits erwähnten Warnzeichen findet in diesem Level statt. Da viele Mitarbeiter die Risiken einer solchen Attacke unterschätzen bzw. davon ausgehen, dass sie zu clever sind, um hinters Licht geführt zu werden, wird mit ihnen ein so genannter Reality Check unternommen. Dabei werden nicht nur Beispiele bekannter Attacken durchgesprochen, sondern auch die Aneignung einer gewissen paranoiden Haltung empfohlen, um Social Engineering Attacken rechtzeitig zu bemerken.

Persistence-Level

Im dritten Level, dem *Persistence-Level*, geht es darum, dass die Mitarbeiter in kurzen Zeitintervallen an die im zweiten Level erarbeiteten Sachverhalte erinnert werden.

Gotcha-Level

Schon der Name des vierten Levels, nämlich *Gotcha-Level*, deutet an, dass hier der Arbeitsablauf abgeändert wird, um Social Engineering Attacken aufzudecken. Dies geschieht unter Verwendung von so genannten *Social Engineering Land Mines (SELM)*: eine Möglichkeit für das Opfer einen Angreifer zu enttarnen, ist das Stellen einer *Bogus Question*. Dabei konfrontiert er einen Angreifer mit einer irrsinnigen Frage, von der der Angreifer meint, er müsse die Antwort kennen und gibt demnach eine Antwort. Hierzu ein Beispiel: Ein Angreifer ruft sein Opfer an und identifiziert sich als Herr Meier. Das Opfer schöpft Verdacht und stellt Herrn Meier die ausgedachte Frage, wie es denn seiner Tochter gehe, die ja letzte Woche einen schweren Autounfall hatte. Wenn der vermeintliche Herr Meier nun auf die Frage eingeht und berichtet seiner Tochter gehe es schon wieder besser oder ähnliches, kann sich das Opfer sicher sein, dass es nicht mit dem echten Herrn Meier spricht.
Eine weitere Möglichkeit besteht in der Verwendung der *Bitte-Warten Policy*, wonach bei jedem Anruf der Anrufer nach einiger Zeit in eine Warteschleife geschickt wird, damit der Mitarbeiter genügend Zeit hat über die aktuelle Anfrage nachzudenken und ggf. einen Kollegen um Rat fragen kann. Auch die *Call-Back Policy* kann genutzt werden um den Erfolg eines telefonbasierten Angriffs zu mindern, in dem prinzipiell jeder Anrufer zurückgerufen wird, bevor sein eigentliches Anliegen bearbeitet wird. Das Einführen einer *Drei-Fragen Policy* sieht eine geheime Absprache zwischen allen Mitarbeitern vor, in der auf drei unauffällige Standardfragen besondere Antworten festgelegt werden, die im Zweifelsfall einen legitimen Mitarbeiter verifizieren können.

Offensive Level

Unter dem Offensive Level versteht man das Melden von Zwischenfällen. Nur durch das Melden von Zwischenfällen kann das Profil eines Social Engineers festgestellt werden. Werden diese Meldungen nicht gemacht, muss jeder Mitarbeiter selbst und ohne Vorwarnung auf den Angreifer eingehen. Dieser kann die fehlende Korrespondenz zwischen Mitarbeitern nutzen, um gezielt seine Anfragen zu optimieren.

9.3.3 Evaluierung von Gegenmaßnahmen

Nachdem verschiedene Möglichkeiten zur Verteidigung von und zur Prophylaxe für Social Engineering Attacken vorgestellt worden sind, möchten wir diese jetzt bewerten. Prinzipiell gilt auch hier, dass wie bei fast jeder sicherheitsrelevanten Lösung ein Trade-Off zwischen Sicherheit und Usability fokussiert werden muss.
Ein ständiges Rückrufen oder die zwanghafte Einbindung von Warteschleifen mag zwar die Erfolgsquote von Social Engineering Attacken reduzieren, ist aber im Arbeitsalltag eines normalen Unternehmens nicht praktikabel. Auch das Stellen von *Bogus Questions* führt im Extremfall eher zu verunsicherten Kunden und Konflikten, als das es eine sicherheitsbringende Maßnahme ist. Des Weiteren kann nicht jede Information klassifiziert werden, geschweige denn eine ständige Evaluierung durch den Mitarbeiter stattfinden, in wie weit er die aktuelle Information weitergeben darf. Die Auswirkung einer paranoiden Haltung auf das Arbeitsklima und die Produktivität kann sich sicherlich jeder vorstellen.
Im zweiten Kapitel haben wir erläutert, dass die Analyse des Workflows in einem Unternehmen eine gute Vorlage für die Konzeption einer Social Engineering Attacke ist. Doch das Stellen von bestimmten Fragen oder sonstige Maßnahmen sind nichts anderes als festgelegte Abläufe, die erforscht und umgangen werden können. Dadurch kann im Extremfall die Arbeit eines Social Engineers erleichtert werden bzw. durch das Passieren dieser Mechanismen beim Angriff ein äußerst starkes Vertrauensverhältnis zwischen Angreifer und Opfer hergestellt werden.
Auch die Klassifikation von Daten und das Einpauken dieser Klassifikationen und diverser Richtlinien durch Mitarbeiter bietet nur äußerst begrenzten Schutz vor Angriffen. Hierdurch wird lediglich ein Katz-und-Maus Spiel initiiert, da bei allen Richtlinien Schwachstellen enthalten sind. Darüber hinaus übersehen diese Methoden unserer Meinung nach den eigentlichen Kern von Social Engineering Attacken: den Risikofaktor Mensch. Menschen kann man nicht durch die Erteilung von Richtlinien zu intuitiv richtig handelnden und selbstsicheren Mitarbeitern machen. Dies kann nur durch das Durchleben von solchen Situationen bzw. durch konkrete Gesprächstrainings erfolgen, in denen Mitarbeitern gezielt beigebracht wird, nicht nur die bekannten psychologischen Fallstricke zu umgehen, sondern auch zukünftig in neuen Situationen intuitiv richtig zu handeln. Dabei ist die Etablierung eines Selbstvertrauens, durch die Zusicherung auch bei vermeintlich falscher Handlung nicht belangt zu werden, enorm wichtig.
Ein optimaler Schutz vor Social Engineering Angriffen ist ein intaktes und ausgeprägtes soziales Netz innerhalb des Unternehmens. Dennoch ist es fragwürdig ob dieses, in Anbetracht der verschiedenen Mentalitäten von Menschen, immer etabliert werden kann.

9.4 Zusammenfassung

Social Engineering ist ein mächtiges Werkzeug. Es kann in allen Bereichen angewandt werden, die einzige Voraussetzung ist die Möglichkeit in irgendeiner Weise mit einem anderen Menschen zu kommunizieren.
Aus der Sicht des Angreifers ist Social Engineering eine sehr effiziente Methode: beherrscht er diese Kunst der Manipulation, hat er gute Chancen erfolgreich zu sein und das bei einem für ihn minimalem Risiko.
Aus der Perspektive des Opfers ergibt sich ein differenziertes Bild: es ist schwierig eine sorgfältig vorbereitete Attacke zu erkennen. Die menschliche Fehlbarkeit kann in so verschiedenen Variationen missbraucht werden, dass auch hier der Grundsatz gilt, dass es keine perfekte Sicherheit gibt. Dennoch gibt es eine gute Nachricht: selbst Kevin Mitnick wurde gefasst.

Literaturverzeichnis

[1] Edward G Amoroso. *Fundamentals of Computer Security Technology.* Prentice-Hall, Inc., 1994.

[2] William Kent Burtner. Hidden pressures. *Notre Dame Magazine*, pages 29–32, Winter 1991-1992.

[3] Robert B Cialdini, Beth L Grenn, and Anthony J Rusch. When tactical pronouncements of change become real change: The case of reciprocal persuasion. *Journal of Personality and Social Psychology*, 62:30–40, 1992.

[4] Presse die. Phishing bei mastercard.com. *http://www.diepresse.com/Artikel.aspx?channel=h\&ressort=ho\&id=490308*, 06.2005.

[5] Hans-Georg Eßer. Ausnutzung verdeckter kanäle am beispiel eines web-servers. Master's thesis, RWTH Aachen, 2005.

[6] David Gragg. A multi-level defense against social engineering. *SANS Institue - Informations Security Readings*, 2003.

[7] Anti-Phishing Working Group. The anti-phishing working group statistics. *http://www.antiphishing.org/*, 2005.

[8] John Leyden. The trouble with anti-virus. *The Register - http://www.theregister.co.uk/2003/09/05/the_trouble_with_antivirus*, 2003.

[9] Kevin Mitnick and William Simon. *Die Kunst der Täuschung.* mitp-Verlag, 2003.

[10] Richard E Petty, Monique A Fleming, Joseph R Priester, and Amy Harasty Feinstein. Individual versus group interest violation: Surprise as a determinant of argument scrutiny and persuasion. *Social Cognition*, 19:418–442, Aug. 2001.

[11] Jonathan J Rusch. The social engineering of internet fraud. *United States Department of Justice*, pages 4–6, 1999.

[12] Hilmar Schmundt. Katz-und-maus-spiel. *Der Spiegel*, 22:144, 2005.

[13] Milgram Stanley. Behavioral study of obedience. *Journal of abnormal and social psychology*, 67:371–378, 1963.

[14] Wikipedia. Milgram-experiment. *http://de.wikipedia.org/wiki/Milgram-Experiment*, 2005.

[15] Jeff Wilson. Network security market. *Infonetics Research* - *http://www.infonetics.com/resources/purple.shtml?ms05.sec.4q.nr.shtml*, 2005.

10 Kombinierte Angriffe

Sascha Jütterschenke und Björn Knuth

10.1 Abstract

Moderne Netzwerke ermöglichen es, wichtige Informationen und Dienste an eine stetig wachsende Gruppe von Benutzern zu verteilen. Der steigende Bedarf des Zugangs zu solchen Dienstleistungen hat zur Entwicklung redundanter Kommunikationsverbindungen, drahtloser Netzwerke, mobiler Notebooks, etc. geführt. Diese neuen Zugangstechnologien und Verbindungen steigern zwar den Wert, der von ihnen unterstützten Informationssysteme, aber gleichzeitig ebnen sie Angreifern und Hackern neue Wege.
Diese Arbeit soll einen kurzen Überblick über technische und organisatorische Angriffsmöglichkeiten auf moderne IT-Infrastrukturen geben. Im Fokus stehen dabei neuere Entwicklungen von hybriden Angriffen, die mit Hilfe mehrerer Vektoren in die Sicherheitsinfrastruktur eindringen und dort erheblichen Schaden verursachen können. Eine vereinfachende Kategorisierung der Gefahrenpotentiale heutiger IT-Infrastrukturen und der grundlegenden technischen Angriffsmethoden bildet die Basis für die Erläuterung einiger Beispiele von kombinierten Angriffen. Sie beschreibt sozusagen das Angriffsrepertoire, aus dem moderne Angriffe ihre Waffen schöpfen. Eine Analyse und Bewertung von Konzepten zur Abwehr solcher Gefahren bildet einen weiteren Schwerpunkt dieser Arbeit und zeigt einen Querschnitt heutiger Verteidigungsstrategien. Zur genaueren Untersuchung des organisatorischen Aspekts kombinierter Angriffe wird im Besonderen auf das Thema Social Engineering und Phishing eingegangen, da hier der menschliche Faktor eine entscheidende Rolle spielt - wie bei praktisch allen kombinierten Angriffen. Abschließend soll ein zusammenfassender Ausblick die Tendenz der aktuellen Entwicklungen im Bereich der Angriffe und deren Verteidigung aufzeigen.

10.2 Einleitung

Nach einem Artikel [1] von IT SecCity [2] zum aktuellen Viren-Report 2004 von TrendMicro TrendMicro habe die Infektionsrate von Informationssystemen mit schadhaftem

[1] vgl. [11]
[2] IT SecCity ist ein sehr ertragreiches Portal, wenn man nach Informationen zum Thema IT-Sicherheit sucht

Code (*malicious code/Malware*) zum ersten Mal 3 **Millionen-Pro-Monat** überschritten. Ein Grossteil dieses schadhaften Codes (55 Prozent) zähle zur Klasse der *Trojaner und Backdoors* - wesentlichen Werkzeugen bei der Durchführung kombinierter Angriffe. Ebenfalls habe es einen enormen Anstieg bei so genannten *Phishing-Attacken* gegeben - Phishing-Attacken stellen eine besondere Klasse hybrider Angriffe dar, da sie in vielfältiger und ungewöhnlicher Weise den menschlichen Faktor berücksichtigen. Im Kapitel 10.7 und 10.8 soll näher auf dieses neuartige Angriffsphänomen eingegangen werden. Als dritten Bereich, der verhältnismäßig starken Zuwachs bei bekannten Angriffsmustern erfuhr, identifizierte TrendMicro die Gruppe der *Bot-Programme*, die es Angreifern ermöglichen, unbemerkt die komplette Kontrolle über infizierte Systeme zu erlangen und über den Zusammenschluss mehrerer solch ferngesteuerter Systeme, so genannte *Zombienetzwerke (Botnets)* aufzubauen. Auf die technischen Angriffsvarianten (*Trjoaner, Backdoors, Bots, u.a.*) wird zur kurzen Erläuterung im Kapitel 10.4 näher eingegangen.

Durch die zunehmende "Bösartigkeit" heutiger Angriffe hat die Vertrauenswürdigkeit, Integrität und Erreichbarkeit vieler Unternehmen katastrophalen Schaden genommen. Innerhalb weniger Minuten erleiden Weltkonzerne Verluste in Millionenhöhe infolge von Angriffen durch *Malware und Hackern*. Die Schäden werden als direkte Folgen der Schadensfunktionen der Attacken (Datenverlust, Netzausfall, Maßnahmen zur Wiederinstandsetzung, usw.) und den Folgeschäden (Störungen im Arbeitsablauf, verminderte Produktivität, Auftragsverlust, Image-Einbuße, Kundenunzufriedenheit, etwaige Rechtsansprüche, etc.) verursacht.

Abbildung 10.1 verdeutlicht die finanzielle Brisanz dieses Themas auf der monetären Ebene, die bereits volkswirtschaftliche Ausmaße erreicht hat.

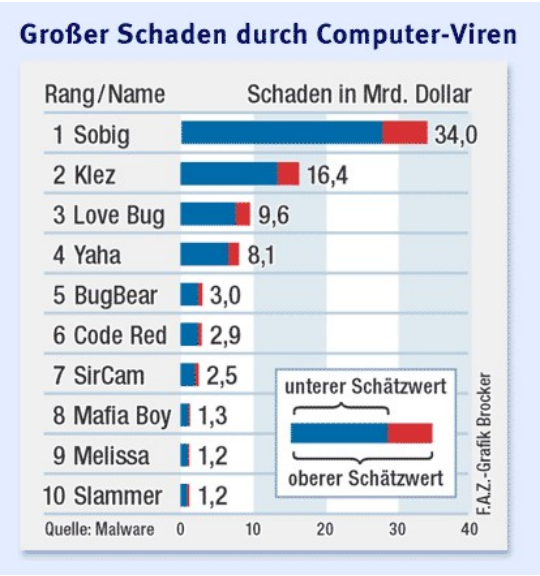


Abbildung 10.1: PC-Viren 2004

10.3 Ursachen der Bedrohungen von IT-Infrastukturen

Im Folgenden soll geklärt werden, welche Motivationen Angreifer haben, sich unberechtigt Zugriff auf Informationssysteme und Netzwerkressourcen zu verschaffen und welche Faktoren ihnen Angriffe überhaupt erst ermöglichen.

10.3.1 Motivation der Angreifer

Wie unterschiedliche Untersuchungen zeigen (BKA [3] Symantec [4]) hat die Kriminalität im Internet in den letzten Jahren zunehmend wirtschaftlichen Hintergrund bekommen. Abbildung 10.2 unterstreicht diese Aussage anschaulich. 16 Prozent aller Angriffe zielen demnach auf Unternehmen aus dem Bereich E-Commerce ab (400 Prozent Zuwachs! [6]) - denjenigen Unternehmen, die Werte direkt aus der Nutzung von IT-Infrastrukturen schöpfen. Waren die Triebfiedern des "Hackens" in den Anfängen noch Spieltrieb, Geltungsdrang und Neugierde, werden heute zunehmend Angreifer mit kriminellen Absichten wie Bereicherung, Rache oder Spionage zum Problem. Angriffe werden dabei sowohl von außerhalb (*Hacker, Spione, Datendiebe*) als auch aus den internen Strukturen gefahren (*interne Mitarbeiter, Personen mit unberechtigtem* physischem *Zugriff* auf Systemkomponenten). Dem Kapitel Gegenmaßnahmen 10.5 vorgreifend soll hier schon erwähnt sein, dass viele Unternehmen ihre Sicherheitsbemühungen zumeist auf das Feld der externen Angriffe konzentrieren und die internen Gefahren (*physische Zugänge zu Systemkomponenten, allgemeine Sicherheitsrichtlinien, Personal und Organisation*) meist zu sehr vernachlässigen.

Eine vom Gefahrenpotential ebenfalls nicht zu unterschätzende Personengruppe sind so genannte Script-Kiddies. Dies ist eine Bezeichnung für Jugendliche, die Systeme - teils aus purem Vandalismus - mit *Virengeneratoren* oder *Hacker-Tools* angreifen, ohne dabei ein tieferes Verständnis über die Techniken und Mechanismen hinter diesen Angriffen und damit den Folgen ihres Handelns zu haben. Mit ihren unbedarften Aktionen verursachen sie meist erheblichen Schaden und werden auf Grund der Tatsache, dass die Hacker-Skills der breiten Angreifermasse im Vergleich zum Anstieg der Komplexität der Hacker-Tools an sich sinken (siehe Abbildung 10.3), zunehmend zum wirtschaftlichen Problem .

10.3.2 Technische und Organisatorische Schwachstellen heutiger IT-Systeme

Welche Gegebenheiten, technischer und organisatorischer Natur, machen sich nun Angreifer zu Nutze, um unberechtigten Zugriff auf Daten und Systemressourcen zu erlangen?

[3] vgl. [10], Kapitel „Typologie von Hackern" bzw. BKA-Kriminalstatistik 2000
[4] vgl. [6]

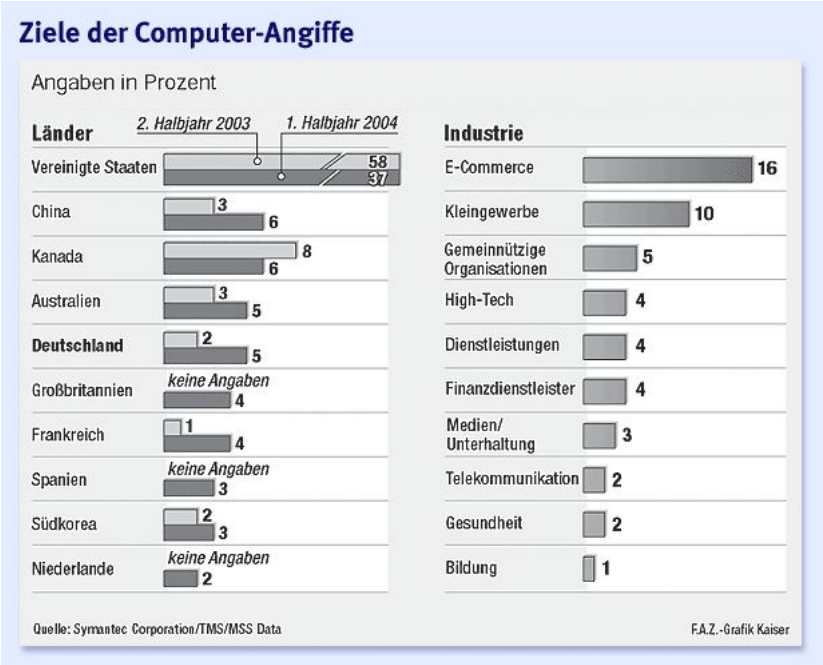


Abbildung 10.2: Internet-Kriminalität erreicht Europa

Technische Bedrohungen

Technische Bedrohungen erwachsen vorrangig aus *Schwächen, der* in der IT-Infrastruktur eingesetzten *Software*, wie z.B. *Fehler oder Sicherheitslücken* in Programmen, die dazu führen, dass ein Angreifer die Software dazu missbrauchen kann, um Attacken diverser Art gegen das gesamte System zu fahren. Computerprogramme, die auf diese Weise spezifische Schwächen anderer Computerprogramme ausnutzen, werden *Exploits* genannt (oft wird auch nur die theoretische Beschreibung eines Exploits als Exploit bezeichnet [3]). Eine Weiterführung dieses Prinzip stellen *Viren, Würmer und Trojaner* dar, auf die im Besonderen im Kapitel 10.4 eingegangen wird. Ihre Funktionsprinzipien bilden die Grundlage für viele kombinierte Angriffe und sind deshalb essentiell für deren Verständnis. Da die Zeit zwischen dem Erkennen einer neuen Schwachstele und dem Ausnutzen durch Exploits u.a. immer geringer wird, haben Privatnutzer und Unternehmen immer weniger Zeit, um angemessen darauf zu reagieren (z.B. installieren von Sicherheits-Patches/Viren-Signatur-Updates). Ein Weg zur effizienten IT-Sicherheit mittels *proaktiver Maßnahmen* soll im Kapitel 10.5.2 aufgezeigt werden.

Technische Bedrohungen entstehen weiterhin auf Grund der Ausnutzung besonderer *technischer Details bzw. systemimmanenten Mängeln von Kommunikationsprotokollen* (z.B. SMTP, ICMP) und *Websprachen* (z.B. ActiveX, Java). Sie setzen allerdings beim Angreifer fundierte technische Kenntnisse über Kommunikationsprotokolle und die Möglichkeiten, über *aktive Inhalte* auf Systeminterna zuzugreifen, voraus. Laut dem Artikel der FAZ [6], werden nach einer Studie von Symantec immer häufiger Computer

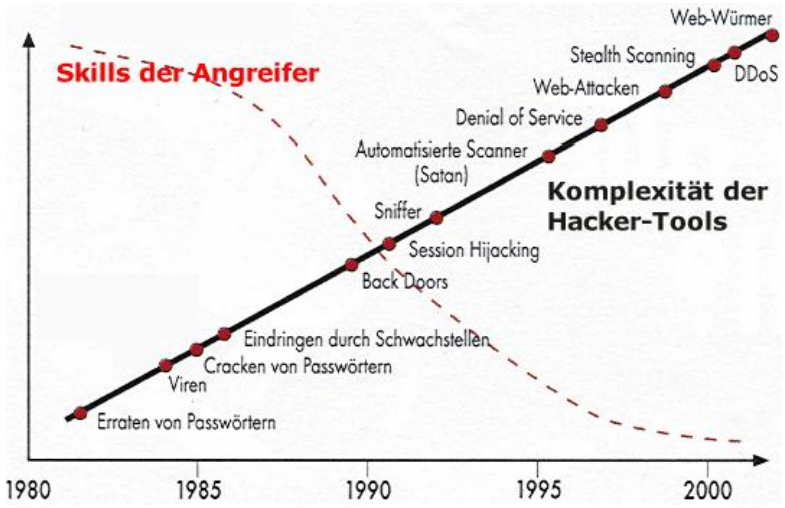


Abbildung 10.3: Komplexität von Hackertools - Skills der Angreifer

von Endanwendern von Angreifern benutzt („Einfallstor Endanwender“), um über Web-Anwendungen übliche Sicherheitseinrichtungen zu umgehen und größere Systeme anzugreifen - 82 Prozent der dokumentierten Schwachstellen wurden als leicht ausnutzbar eingestuft. Angriffe über solche so genannte *Brückenkopf-Hosts* spielen im Bereich der blended threads insbesondere bei *distributed-denial-of-service-Attacken (dDoS-Threats)* mittels so genannter *Zombienetzwerke (Botnets)* eine wichtige Rolle.

Nicht zu unterschätzende Gefahrenpotentiale für die Sicherheit von IT-Infrastrukturen stellen *Fehler in der Konzeption und Konfiguration* dar. Netzwerke von mittleren und großen Unternehmen sind durch eine hohe Dynamik gekennzeichnet: Reorganisation, Zukäufe von neuen oder Abstoßen von ertragsschwachen Unternehmenseinheiten sind oft die Ursachen für Schwachstellen, die - unbeabsichtigt - in die Infrastruktur eingebaut werden. Nichtbeachtung von Sicherheitseigenschaften bei der Planung und Anpassung der IT-Infrastruktur (z.B. fehlerhafte Einbindung neuer Rechner in die Sicherheitsstruktur) und falsche bzw. nicht vollständige Einstellungen von Parametern und Optionen von verwendeten Programmen und Systemen (z.B. fehlende Benutzerrechte-Einschränkung, nicht angepasste Standard-Passworte in Hard- und Software) sind hier die Hauptquellen für mögliche Attacken, die sich auch neuere Viren-Mischformen zu Nutze machen. Neuartige Bedrohungen haben es gerade auf das Überlisten der vorherrschenden Sicherheitsstandards abgesehen und der herkömmliche Schutz über Antiviren-Software und Firewall ist schon lange nicht mehr ausreichend, um adäquat auf die neuen Bedrohungen zu reagieren. Im Kapitel 10.5 soll sich dem konzeptionellen Schutz gegen die künftigen (unbekannten) Bedrohungen genähert werden.

Organisatorische Bedrohungen

Spezifische Bedrohungen für IT-Systeme kommen, wie weiter oben schon angedeutet, häufig auch aus dem *organisatorischen Umfeld*. Private Disketten von Mitarbeitern, die mit Viren verseucht sind, können ganze Unternehmensnetze lahm legen. Der *nachlässige Umgang mit Passworten und physisch zugänglichen Systemteilen* führt dazu, das unbefugte Dritte Zugriff auf geschützte Daten und Systemressourcen erhalten und diese manipulieren können. Das *Fehlen sicherheitsrelevanter organisatorischer Vorgaben* (z.B. Zutrittsbeschränkungen, Berechtigungskonzepte), die *lückenhafte Schulung von Mitarbeitern, menschliches Versagen und vor allem* ***mangelndes Sicherheitsbewusstsein*** öffnen Angreifern schon auf organisatorischer Ebene Tür und Tor. Ein kritischer Punkt, der besonders bei so genannten Phishing-Attacken zum Tragen kommt. Kapitel 10.8 wird das weite Feld der Phishing-Attacken, die sich auf Grund der in diesem Kapitel beschriebenen technischen und organisatorischen Schwachstellen ergeben, näher beleuchten. Phishing hat sich innerhalb der letzten Jahren als das "Parade-Konzept" hybrider Angriffe etabliert (vgl. Abbildung 10.2 - Angriffe auf eCommerce-Unternehmen) und wird deshalb einen weiteren Schwerpunkt dieser Arbeit bilden.

10.4 Klassen von Schadenssoftware (Malware)

Automatisierte technische Abläufe, die das Ziel haben, auf fremden Rechnern für dessen Besitzer unerwünschte Effekte hervorzurufen, und/oder die es einem Angreifer ermöglichen, unberechtigt Zugriff auf fremden Rechnern zu erlangen, um dort Daten und Prozesse auszuspähen, zu verändern und zu gefährden, bezeichnet man als Sabotagesoftware (*Malware*) oder schädlichen Code (*malicious code*). Geläufiger ist hier der Begriff *Virus*, der allgemein für verschiedene Klassen von Sabotagesoftware verwendet werden kann. Dabei lassen sich folgende Kategorien von Viren anhand ihres Schadenspotentials identifizieren: Viren im eigentlichen Sinn, Trojanische Pferde und Würmer.

Viren im eigentlichen Sinn

Viren im eigentlichen Sinn sind kleine Programme, die sich in anderen Programmen einnisten (infizieren) und dort unerwünschte Effekte hervorrufen. Im Wesentlichen unterteilen sie sich dabei in einen Reproduktionsteil, der für die Weiterverbreitung (Infizierung anderer Programme) des Viruses zuständig ist und einen Aktionsteil, in dem die vom Angreifer beabsichtigten, schädigenden Aktionen ausgeführt werden. Die Auswirkungen solcher Aktionen reichen dabei von harmlosen Veränderungen an Ausgabegeräten (Bildschirmanzeige wird verändert, Meldungen angezeigt, Lautsprecher aktiviert, usw.) bis hin zu zerstörerischen Sabotageaktionen wie Reduktion der Verarbeitungsgeschwindigkeit, permanenter Warmstart oder Manipulationen an Daten (Löschen/Ändern von Dateiverzeichnissen, Zerstörung von Daten, Formatierung der Festplatte, etc.).

Trojanische Pferde

Trojaner arbeiten nach einem ähnlichen Prinzip wie Viren. Sie nisten sich ebenfalls in anderen Programmen ein, besitzen aber keinen Reproduktionsteil. Ihr Ziel ist es, durch die im nicht dokumentierten Aktionsteil angestoßenen Aktionen, für den Nutzer unbekannte und unerwartete Zusatz- und Schadensfunktionen ins System einzuschleusen. Dabei gibt es grundsätzlich zwei verschiedene Methoden, wie Angreifer dabei versuchen, die Existenz solcher Trojaner zu verschleiern, um sie ins System einzuschleusen. Nach dem Prinzip der Namensvetter (*companions*) wird der Aktionsteil an Programme gehängt, die im Namen mit dem Nutzer bekannten Programme identisch sind und/oder nur eine andere Dateiendung (z.B. .com statt .exe) besitzen. Mit der Methode der Geschenke (*gifts*) wird der Nutzer dazu gebracht, ihm unbekannte Programme (z.B. Freeware, Public-Domain-Software, „must have seen"-Mail-Attachements) entgegenzunehmen und auszuführen. Intention des Gebrauchs von Trojanern ist meist nicht, die Zerstörung oder die Manipulation von Daten, sondern das Ausspionieren und Beeinflussen von Nutzerverhalten (*Adware*), das Stehlen persönlicher und personenbezogener Daten (*Spyware, Keylogger*) oder gar die (komplette) Fernkontrolle des Computer über nicht sichtbare Kommunikationskanäle (*Bots*).

Würmer

Im Unterschied zu Viren und Trojanern benötigen Würmer kein Wirtsprogramm, sondern sind selbstständige Programme, die reproduktionsfähig sind. Sie entfalten meist nicht direkt schädigende Wirkungen an Daten und Programmteilen, sondern produzieren Fehlfunktion im infizierten System bzw. am gesamten Systemumfeld durch Speicher- bzw. Netzüberlastung oder Geräteblockierung auf Grund ihrer permanenten Reproduktionstätigkeit.

Hoaxes

Virenhoaxes sind Falschmeldung über nicht existierende Viren, die häufig Dinge behaupten, die überhaupt nicht möglich bzw. wahr sind und auf deren Basis Maßnahmen ergriffen werden, die eigentlich unnötig sind (z.B. das voreilige Herunterfahren des Netzwerks). Auch Kettenbriefe, die per E-Mail weitergeleitet werden, können zu den Hoaxes gezählt werden, da ja meist kein realer Hintergrund, der die Verbreitung rechtfertigen würde, besteht.

10.5 Gegenmaßnahmen zur Gefahrenabwehr

Die Gruppe der Maßnahmen zur Gefahrenabwehr lässt sich grundlegend in reaktive und proaktive Maßnahmen unterteilen. Die traditionelle (reaktive) IT-Sicherheit ist bemüht, das Schadensausmaß von Angriffen mit peripheren Sicherheitsmaßnahmen, wie z.B. *Antiviren-Software, Firewalls* und *Intrusion Detection/Prevention Systemen*, zu begrenzen. Proaktive Maßnahmen basieren auf Lösungen und Konzepten, die es ermögli-

chen die relevanten Werte und Prozesse von IT-Systemen durch geeignete Lenkungsmaßnahmen bereits im Vorfeld zu schützen (z.B. Vulnerability/Exposure Risk Management). Hier geht es nicht um Schadensbegrenzung, sondern vielmehr um das Vermeiden und Vermindern von Risiken.

10.5.1 Reaktive Maßnahmen

Antiviren-Software

Antiviren-Software ist zunächst die effektivste Methode *bekannte Viren* auf infizierten Systemen zu entdecken und wenn möglich zu entfernen (*Viren-Scanner*) und auf der anderen Seite prophylaktisch dafür zu sorgen, dass über Datei-Erstell, -Kopier bzw. -Ladevorgänge keine Viren auf den geschützen Rechner gelangen können (Viren-Wächter). Das Problem von Antiviren-Programm besteht allerdings darin, dass sie nur bekannte und sichtbare Viren aufspüren und eliminieren können. Moderne Angriffsvarianten zielen aber darauf ab, bekannte Sicherheitsmaßnahmen zu umgehen und ihre Aktivitäten zu verschleiern, um eine maximale Infektionsrate zu erzielen. Auch bei so genannten polymorphen Viren, die ihren Code nach jeder Infektion ändern oder Stealth-Viren, die ihre Existenz vor Virenschutz-Programmen verbergen können, stößt diese Abwehrmaßnahme bereits an ihre Grenzen. Außerdem ist es notwendig, dass die Antiviren-Software regelmäßig in kurzen Intervallen aktualisiert wird, da sie sonst neue Viren nicht erkennen und abwehren kann. Hier kommt auch das schon angesprochene Patching-Problem der Zeitspanne zwischen bekannt werden einer Schwachstelle, dem ersten Auftreten eines diese Schwachstelle ausnutzenden, schadhaften Programms und dem Erkennen und Bereitstellen von Gegenmaßnahmen durch die Antiviren-Hersteller zum Tragen (vgl. Kapitel 10.3.2). Die Zeitspanne kann unter Umständen schon so groß sein, dass bereits erheblicher Schaden entstanden ist.

Firewalls

Firewalls bestehen aus Netzwerkkomponenten (Hard- und Software) an der Schnittstelle zwischen zwei Netzen (z.B. zwischen Intranet und Internet), die sie passierende Datenpakete kontrollieren. Die Firewall untersucht den Datenverkehr und lässt nur unverdächtige bzw. erwünschte Daten passieren (*Paketfilter* für zugelassene Ports/Dienste). Damit die Firewall diese Kontrolle leisten kann, muss allerdings der gesamte Datenverkehr über diese Station laufen. *Application Gateways* (z.B. E-Mail-Filter) und *Proxy Server* (z.B. HTTP-Proxys), so genannte *Gateway-Firewalls*, können dazu benutzt werden, direkten Datenverkehr zwischen Quell- und Zielrechner zu verhindern und über Analyse des über die Gateways laufenden Datenverkehrs, bestimmte Daten (ausführbare eMail-Attachements, unerwünschte Website-Inhalte) herauszufiltern bzw. zu blocken (Viren u.a.). Als Nachteil fällt dabei sofort der Performanceverlust auf Grund der, unter Umständen, aufwendigen Datenanalysen ins Gewicht. Außerdem muss die Firewall selbst immun gegen Angriffe sein: Gelingt es einem Angreifer sie zu überwinden, kann sie auch keinen Schutz mehr bieten - z.B. kann mittels *Spoofing*, also dem Vortäuschen von

falschen Adressen und Absendern und dem Umlenken von Datenpaketen an zugängliche Ports (z.B. Port 80) die Schutzfunktion von Firewalls leicht ausgehebelt und schädlicher Code ins Zielnetz eingeschleust werden.

Intrusion Detection Systeme

Intrusion Detection Systeme (*IDS*) wurden entwickelt, um Angriffe zu identifizieren (musterbasiert/anomaliebasiert) und sie den IT-Sicherheitsbeauftragten von Unternehmen zu melden, damit diese entsprechende Gegenmaßnahmen einleiten können. Herkömmliche IDS stoppen Angriffe nicht, sondern erkennen lediglich feindlichen Datenverkehr und geben Warnmeldungen aus. Da jedoch die Anzahl der Bedrohungen stetig steigt (siehe z.B. Script-Kiddies in 10.3.1: etwa 90 Prozent der in Logfiles erfassten Hackerattacken werden von Script-Kiddies verursacht [5]) stellt es sich zeitlich wie personell schnell als viel zu aufwendig heraus, die vielen Meldungen der IDS-Systeme zu analysieren und auf sie zu reagieren.

Intrusion Prevention Systeme

Intrusion Preventionen Systeme (*IPS*) sollen Gefahren nicht nur erkennen und sie melden, sondern auch auf sie reagieren bevor Schaden entsteht. Dies sind in der Regel IDS-Erweiterungen von Firewalls. Sie entscheiden mit ähnlichen Mechanismen wie Firewalls, ob Datenpakete passieren dürfen oder nicht und reagieren bei einer entsprechenden Wahrscheinlichkeit eines Angriffs mit Gegenmaßnahmen. Der wegen Passivität der IDS noch harmlose Fall von *False-Positives* (versehentlich als schädlich identifizierter, regulärer Verkehr) kann bei IPS jedoch dramatisch Auswirkungen haben, weil eine aktive und automatisierte Reaktion erfolgt. Durch Konfigurationsfehler (siehe Kapitel 10.3.2) kann ein IPS ein Netzwerk schlimmstenfalls komplett abschotten. Durch gezielte Ausnutzung der Eigenschaften von IPS können Angreifer bei *Denial-of-Service-Attacken (DoS-Attacken)* versuchen genau einen solchen Effekt zu erzielen, um die Erreichbarkeit des Netzwerks, das durch das IPS geschützt werden soll, zu beeinträchtigen. Eine sorgfältige Konfiguration des IPS ist demnach essentiell für dessen Wirksamkeit.

10.5.2 Proaktive Maßnahmen

Offenbar reichen reine Maßnahmen des Vorfall-getriebenen Reagierens angesichts neuartiger Bedrohungen zum Schutz relevanter Werte und Prozesse nicht mehr aus. Traditionelle Sicherheitsmechanismen (Antiviren-Programme, Firewalls, IDS, IPS, Access Management) werden durch moderne Angriffe bewusst umgangen, ausgehebelt oder gar deren immanente Eigenschaften ausgenutzt, um neue Angriffsformen zu etablieren (siehe 10.3.2 und IPS). Vorbeugende Maßnahmen, die das Risiko von Angriffen mindern oder gar vermeiden müssen die reaktiven Maßnahmen in geeigneter Weise ergänzen, um eine umfassende Sicherheit innerhalb der IT-Infrastrukturen - auf organisatorischer und technischer Ebene - zu ermöglichen.

[5] vgl. [12], Artikel: „Hacker im Visier: Aktion statt Resignation“

Security Awareness und Organisation

Die wohl wirkungsvollste Maßnahme auf organisatorischer Ebene ist die Steigerung der Security Awareness am System beteiligter Personen (z.B. durch Schulungen): „Denn wer sich bewusst ist, dass sämtliche Informationen einen Wert haben, welche im Web, im Gespräch oder auf dem Schreibtisch liegend aktiv oder passiv an andere weitergegeben werden, der überlegt sich, ob, wem und vor allem was er an andere kommuniziert.“ [6]

So können manch geplante Attacken bereits in einer frühen Phase abgewehrt, die in besonderer Weise den menschlichen Faktor berücksichtigen (siehe auch Kapitel 10.8). Für viele automatisierte Angriffe ist es notwendig, dass der Anwender die Schadenssoftware initial startet bzw. aufruft, z.B. schadhaften Code enthaltene Dateien aus dem Anhang einer Email öffnet, innerhalb einer Webanwendung dem Download von potentiell gefährlichen Daten (z.B. Scripte für aktive Inhalte, Dialer-Programmen, usw.) zustimmt oder ihm unbekannte Programme ausführt (vgl. Trojaner/Gifts - 10.4). Durch Sensibilisierung der Mitarbeiter für potentielle Angriffe können große Teile der potentiellen Gefahren bereits im Vorfeld eingeschränkt werden.

Sicherheitsmaßnahmen müssen weiterhin in übergeordnete (organisatorische) Prozesse integriert werden, so dass Mängeln im Security Management durch fehlerhafte oder mangelhafte organisatorische Vorgaben für die tägliche Praxis zur Planung, Steuerung, Durchführung und Kontrolle erforderlicher Sicherheitsaktivitäten entgegengewirkt werden kann. Konkret bedeutet dies die Erstellung genauer Richtlinien, wie bei einem sicherheitsrelevanten Vorfall vorzugehen und wer zu informieren ist (*Policies, Prozesse, Rollen*). Die Erstellung von Vorgehensplänen (*Alarm-, Notfall- und Wartungsplänen, Security Checks*) und einige weitere organisatorischer Maßnahmen, die hier aber nicht weiter Gegenstand der Untersuchung sein sollen gehören hier ebenso dazu. Angemerkt sei nur, dass ein kompetentes und konsistentes Sicherheitsmanagement personelle und funktionelle Aspekte integrieren muss, wobei technische Maßnahmen die organisatorischen Rahmenbedingungen auskleiden sollten und nicht den alleinigen Fokus umfassender IT-Sicherheit bilden dürfen.

Vulnerability Management/ Exposure Risk Management

Das so genannte Schwachstellen- oder Risikomanagement wird den nächsten Jahren zu den zentralen Sicherheitsthemen gehören. [7] Aufgrund der Vielzahl bekannt werdender, neuer Schwachstellen in Softwaresystemen (und Hardwaresystemen!) - 2004 gab es laut CERT 3600 (das sind fast 10 pro Tag!) - ist es notwendig, Verfahren zu finden, die automatisch Schwachstellenanalysen durchführen (Vulnerability Management Tools) und identifizierte Schwachstellen bewerten können (Exposure Risk Management Tools). Re-

[6] Zitat, Christoph Baumgartner, Geschäftsführer und Senior Conultant der OneConsult GmbH, aus: [12]

[7] vgl. [12], Artikel: „Ein Weg zur effizienten IT-Sicherheit“

gelmäßige *Security Audits* (betriebsweite Sicherheitsprüfungen) allein reichen nicht mehr aus, da die Periode zwischen den einzelnen Audits meist zu lang ist (siehe 10.3.2) und die limitierten Ressourcen (personell, zeitlich, finanziell) der Unternehmen kaum ausreichen, um umfassende Analysen und Maßnahmen durchzuführen.

Vulnerability Management Tools (z.B. eTrust Vulnerability Manager von CA oder Symantec Vulnerability Assessment von Symantec) ermitteln nun automatisch Schwachstellen der Infrastruktur durch bestimmte Analyseverfahren, auf deren Basis Gegenmaßnahmen geplant werden können. Die Durchführung dieses Maßnahmen kann durch integrierte Ticket-Systeme, die den Behebungsprozess steuern und verwalten, überwacht werden. Der Nachteil solcher Vulnerability Management Systeme ist die Masse an Informationen, die sie generieren und die es abzuarbeiten gilt.

Exposure Risk Management Systeme (z.B. Skybox View von Skybox Security) können die von Vulnerability Management Systemen identifizierten Schwachstellen im Kontext der Netzwerkarchitektur, der IT-Assets und Security Controls bewerten und damit die kritischen Schwachstellen (nur ein bis zwei Prozent identifizierter Schwachstellen sind wirklich kritisch!) herausfiltern. Durch automatische Analyseverfahren und oben beschriebene Ticket-Systeme, werden Sicherheitsverantwortliche und Riskmanager dabei unterstützt, Maßnahmen zur Behebung der Schwachstellen und Reduktion der relevanten IT-Risiken zu evaluieren, zu planen und erfolgsorientiert durchzuführen. [8]

10.6 Beispielhafte Blended Threats

Betrachtet man in der heutigen Zeit Schadenssoftware, so muss man feststellen, dass diese nicht mehr in ihrer Reinform existieren. Es treten zunehmend Viren auf, die mehrere Methoden nutzen, um Systeme zu infizieren und somit mehrere Sicherheitslücken nutzen. Viren dieser Art werden als Blended Threats, gemischte Bedrohung, bezeichnet. Hier treffen Eigenschaften von Viren, Trojanern, Würmern und des Social Engineerings aufeinander.

10.6.1 Nimda

Der Wurm Nimda befällt Computer mit dem Windows Betriebssystem. Das interessante an dem Virus ist, dass er mehrere Techniken für seine Verbreitung nutzt, ein eigenes Programm zur Verbreitung mitbringt und Systeme für Angriffe schwächt. Er soll hier dazu dienen, verschiedene Verbreitungswege zu zeigen, die in der Abbildung 10.4 zusammengefasst werden.

Der Virus verschickt sich per E-Mail, die die Datei readme.exe oder .doc als Anhang besitzt. Der Anwender muss nicht auf den Anhang Doppelklicken, um den Virus zu Aktivieren. Es genügt hier das Betrachten der Mail, um die Datei auszuführen. Für diese

[8] vgl. [12], Artikel: „Ein Weg zur effizienten IT-Sicherheit“

Eigenschaft nutzt der Virus eine MIME-Schwachstelle von einigen Versionen von Microsoft Outlook, Microsoft Outlook Express und Internet Explorer. Hat der Virus das System befallen, versucht er sich an alle E-Mail-Adressen weiterzuleiten, die er auf dem Rechner findet. Dafür nutzt der Virus seine eigene SMTP-Engine.

Der Virus versucht sich über Netzwerkfreigaben auf andere Anwender zu übertragen. Dafür kopiert er mehrere versteckte Dateien in das Windows-Verzeichnis. Um diese Verbreitungsart zu fördern, gibt der Virus alle Netzlaufwerke frei und gibt dem GAST-Account Admin-Rechte.

Des Weiteren verbreitet sich der Virus über infizierte Webseiten. Von einem infizierten System aus sucht er IIS-Webserver, die von der Schwachstelle im Unicode Directory Traversal betroffen sind. Anschließend sucht er dort nach Dateien wie index.html, default.html und main.html, die er mit schädlichem JavaScript Code infiziert. Mit dem Ausführen der Datei, wird die Datei readme.eml heruntergeladen, was eine erneute Weiterverbreitung zur Folge hat. Ein interessanter Aspekt ist hierbei, dass der Nimda Virus Sicherheitslücken ausnutzt, die vom Befall der Viren CodeRed2 oder Sandmin entstanden sind.

Zum Schutz sind hier mehrere Maßnahmen nötig. Zum einen gilt es auch hier, Mailanhänge mit .exe Erweiterung zu unterbinden. Um die Sicherheitslücken der Microsoft-Produkte zu stopfen, hat Microsoft Updates zur Verfügung gestellt. Infizierten Webseiten kann man wie in diesem Fall aus dem Weg gehen, indem JavaScript bei den Browsern deaktiviert wird. Das hat jedoch den Nachteil, dass viele Webseiten nicht mehr funktionieren.

10.6.2 JS Scob

JS Scob ist ein Trojaner, der in JavaScript programmiert wurde. Er bringt gleich drei verschiedene Risiken mit sich. Zum einen nutzt er Schwachstellen des Microsoft Internet Information Servers IIS und des Internet Explorers, indem er Webseiten infiziert. Dabei wird das Virenskript nicht an die Grafik-Dateien selbst gehängt, sondern an die Fußzeileninfos des IIS. Beim Betreten der Seite, wird ein Keystroke-Logger installiert, womit Eingaben persönlicher (finanzieller) Daten mitgelesen werden. Durch die Erstellung eines Cookies, verbindet sich der infizierte Rechner wöchentlich mit einer entfernten Webseite, an die die gesammelten Daten übermittelt werden. Damit besitzt der Hacker, ähnlich wie bei Spyware, die Kontrolle über den PC.

JS Scob war zwar in seiner Verbreitung und seinem Schaden relativ gering, jedoch zeigt er die Tendenz der Malware. Dazu zählt das Ausspionieren des Rechners durch Trojaner und die Kontrolle des PCs durch wöchentliches Verbinden zu einer Webseite. Letzteres wird oft auch genutzt, um den Virus selbst zu updaten oder den Virus von dort zu verbreiten.

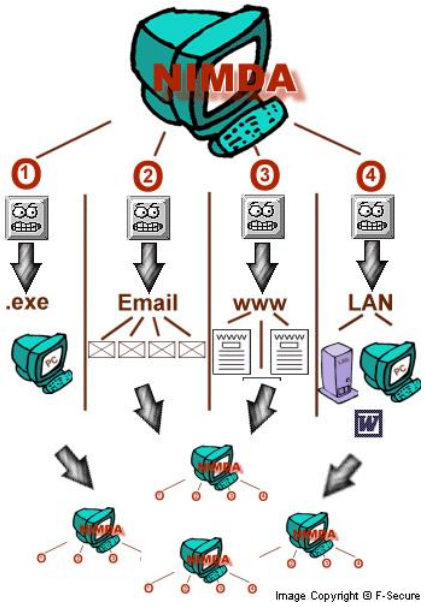


Abbildung 10.4: nimda

10.6.3 Lovgate

Schädlinge der Familie Lovgate zeigen das ganze Potential kombinierter Angriffe. Lovgate-Viren (es gibt bereits mehr als 30 Varianten!) sind Würmer, Trojaner und Viren in einem. Sie nutzen Schwachstellen und Fehler in Software gleichermaßen wie systemimmanente Mängel von Kommunikationsprotokollen (vgl. Kapitel 10.3.2). Eine Auswahl der Funktionen und Arbeitsweisen soll dies verdeutlichen.
Lovgate-Viren verbreiten sich als *Massmailing-Würmer* über E-Mail und lokale Netze und ermöglichen dem Angreifer unbefugten Zugriff und Fernsteuerung des Computers.

Der Wurm versendet sich per E-Mail mit Hilfe der MAPI-Schnittstelle von Windows (Schnittstelle von Microsoft, um mit jeder Windows-Software E-Mails verschicken zu können). Er antwortet dabei auf (ungelesene) E-Mails aus Outlook-Ordnern (MAPI-Postordner) oder extrahiert E-Mail-Adressen aus WAB-, TXT-, HTM-, HTML- SHT-, PHP-, ASP-, DBX-, TBB-, ADB -und PL-Dateien. Betreff und Text der Mail werden aus einem Pool von Möglichkeiten gebildet, die der Wurm selbst mitbringt und die den Nutzer dazu verleiten sollen, den Anhang der Mail zu öffnen (Ausnutzung menschlicher Schwächen - vgl. Kapitel 10.3.2). Die Benennung des Anhangs der E-Mail, der den Wurm selber enthält, ebenso wie die Benennung von auf Netzfreigaben und Ordner kopierten Dateien erfolgt nach demselben Prinzip (Ziel: Weiterverbreitung/Aktivierung).

Weiterhin verschleiert der Wurm seine Aktivität/Identität und versucht gegebene Schutzmaßnahmen zu umgehen. Dies realisiert er, in dem er die Dateien (und Prozesse), die die eigentlichen schädigenden Funktionen ausführen und in Systemordner kopiert wer-

den, nach bekannt scheinenden Diensten und Systemdateien benennt (z.B. “Microsoft Network Firewall Services“, win.exe, winGate.exe, winhelp.exe, kernel66.dll). Außerdem versucht Lovgate bestimmte, laufende Antivirenprozesse und andere Sicherheitsdienste zu stoppen, deren Namen z.B. folgende Zeichenketten enthalten: NAV, McAfee, Symantec, RavMon. Er kann auch den Absender der verschickten E-Mail fälschen (*Spoofing*). Zum "Knackenßchwach geschützter Netzwerkressourcen und zur Erlangung von Admin-Rechten, verwendet Lovgate eine interne Liste der häufigsten und offensichtlichsten Kennwörter (*Dictionary-Attacke*).

Für die Fernkontrolle läuft Lovgate als (HTTP-)Server an Port 20808. Jeder, der sich mit einem Webbrowser an diesem Port verbindet, kann Dateien von allen verknüpften Laufwerken herunterladen und Dateien auf alle beschreibbaren Laufwerke hochladen. Auf Port 1098 und 20168 wartet er auf TCP-Verbindungen, über die willkürliche Befehle auf dem infizierten Rechner ausgeführt werden können (*Backdoor*). Ebenfalls protokolliert er mögliche Benutzernamen/Kennwort-Kombination in C:/NetLog.txt (*Spyware*).

Lovgate infiziert, indem er die Erweiterung von EXE-Dateien in ZMX ändert und sich in den Speicherort der originalen EXE kopiert (*Virus*).

Die vielfältige Arbeitsweise der Lovgate-Viren zeigt, wie wichtig es ist, bei Gegenmaßnahmen nicht nur auf einzelne Punkte zu setzen (z.B. Antiviren-Software), sondern die Gesamtheit möglicher Gegenmassnahmen (siehe Kapitel 10.5) auszuschöpfen und ergänzend und koordiniert einzusetzen. Dass das Antiviren-Programm auf dem aktuellsten Stand ist (um neue Varianten von Lovgate zu erkennen), ist hier genauso wichtig, wie eine gut konfigurierte Firewalls (E-Mail-Filter, Port-Blocker, Packet-Filter, etc.). Proaktive Maßnahmen können helfen, nicht beachtete Schwachstellen auf übergeordneter Ebene “auf die Schliche zu kommen“.

10.7 Social Engineering

Social Engineering ist eine Methode, um nicht allgemein zugängliche Informationen durch Äushorchenßu erlangen. Oft gibt sich ein Angreifer bei Gesprächen durch die Kenntnisse der richtigen Schlagworte als Insider zu erkennen und erhält so zusätzliche Informationen, die an anderer Stelle ausgenutzt werden können. Social Engineers nutzen die Naivität der Mitarbeiter eines Betriebes und deren Bedürfnis involviert und hilfreich zu sein aus, um an die gewünschten Informationen zu gelangen.

10.7.1 Computer Based Social Engineering

Eine denkbare Möglichkeit hierfür ist ein Popup, welches einem Benutzer mitteilt, die Netzwerkverbindung sei unterbrochen worden und er möge seinen Benutzernamen und Passwort erneut eingeben. Die eingegebenen Daten werden mittels E-Mail an den Eindringling geschickt. Diese Methode benötigt verschiedene Technologien um die Mitar-

beiter auszutricksen und erfordert schon eine Vorkenntnis zum Opfer zu haben, um auf das gewünschte System zugreifen zu können.

10.7.2 Human Based Social Engineering

Es wird zuvor versucht Hintergrundinformationen über die betreffende Person zu erlangen. Sei es Namen von Mitarbeitern, Telefonnummern. Eine der wohl einfachsten Methoden einen Namen ausfindig zu machen ist, danach zu fragen: ein öffentlicher Dienstplan, eine Website oder sogar das Namensschild am Büro oder Haustür. Ebenso Müll zu stehlen und diesen nach Informationen zu durchsuchen - so genanntes "trashingöder "dumpster diving"(das ist gesetzlich nicht illegal da Müll weder Privat noch Eigentum ist). Ist das Grundwissen eines Opfers verfügbar, tritt der Social Engineer mit einem Mitarbeiter in Kontakt. Ob nun per Telefon, Fax oder E-Mail. Sogar persönliche Gespräche gehören dazu. Er gibt vor ein neuer Mitarbeiter, Manager, vom Reparaturdienst, IT Support oder ähnliches zu sein.

10.7.3 Reverse Based Social Engineering

Der Social Engineer erzeugt eine fiktive Autoritätsperson, sabotiert das Netzwerk und behauptet anschließend derjenige zu sein, der dieses Problem beheben soll. Somit bewirkt er, dass sich die Mitarbeiter an ihn wenden und ihm alle Informationen geben, die er möchte. Hat er alle Daten, die er braucht, behebt er den Fehler und niemand schöpft Verdacht, da alles wieder wie gewohnt funktioniert. Auch diese Methode benötigt gründliche Nachforschung und ein gewisses Maß an Zugriff am System.

10.8 Phishing

Der Begriff Phishing setzt sich aus den Wörtern password und fishing zusammen. Es wird hier die Metapher genutzt, dass aus einem Meer von Internetnutzern Passwörter und andere Zugangsdaten herausgefischt werden. Der erste aufgetretene Fall von Phishing war bereits im Jahr 1996, wo Hacker Zugangsdaten zu America Online Accounts gestohlen haben. Im Laufe der Zeit hat sich das Phishing vom Stehlen von Accountdaten zum Stehlen von jeglichen persönlichen Daten, vor allem von finanziellen Daten, weiterentwickelt. Das Grundprinzip von Phishingattacken ist heute eine vertrauenswürdige Quelle (z.B. E-Mail oder Webseite einer Bank) vorzutäuschen, um an geheime Daten des Nutzers zu gelangen. Phishing eignet sich perfekt als Beispiel eines kombinierten Angriffs, da hier Elemente des Social Engineerings sowie mehrere der genannten Malwares genutzt werden.

10.8.1 Übertragung der Phishingangriffe

E-Mails

Die am häufigsten genutzte Übertragungstechnik von Phishingangriffen ist die E-Mail. Wie gewöhnliche SPAMs werden Phishingmails an eine große Zahl vermeintlicher E-Mail-Adressen gesendet. Durch bekannte Mängel am Kommunikationsprotokoll SMTP, kann der Phisher die E-Mail mit einer falschen E-Mail-Adresse senden. Phishingmails nutzen mehrere Techniken, um den Internetnutzer zu täuschen:

- offiziell aussehende und geschriebene E-Mails
- Kopien von rechtmäßigen E-Mails mit leicht veränderter URL
- HTML-basierte E-Mails, um den Web-Link innerhalb der Mail zu fälschen
- Viren und Würmer als Anhänge der Mails
- eine Fülle von Techniken, um durch SPAM-Filter durchzukommen
- gefälschte Referenzen zu bekannten Message Boards und Mailing Listen
- Fälschung der Herkunft der E-Mail

Abbildung 10.5 zeigt ein Beispiel einer Phishingmail, die unzählige Postbankkunden erreicht hat. Der Nutzer wird hier gebeten zu seiner eigenen Sicherheit den Link anzuklicken und in das darauf folgende Formular Kontonummer, PIN und zwei gültige TANs einzutippen. Der Phisher hat sich in diesem Beispiel jedoch relativ wenig Mühe gegeben, seine Tat zu verschleiern. Zwar erscheint die Mail in einem glaubwürdigen Layout und die Quelladresse wurde gefälscht, doch weist die Mail sprachliche Unstimmigkeiten auf, was anhand des Ausdrucks und der Schreibweise der Umlaute erkennbar ist. Des Weiteren wurde beim darauf folgenden Formular keine echt wirkende Postbank-URL genutzt, sondern eine IP-Adresse, ohne sichere HTTPS-Verbindung.
Da bekannt ist, dass E-Mails mit HTML-Code schädliche Codeteile besitzen können, formatieren einige Phisher ihre HTML-E-Mails wie das Textformat. Eine gängige Technik ist zu dem, den Link der Mail über einen vorher befallenen Rechner zu leiten, was die Verfolgung der Phishingmail extrem erschwert.

Web-Seiten

Ein Verfahren, das immer mehr an Anwendung gewinnt, ist schädlichen Inhalt in Webseiten einzubauen. Die Inhalte können hier auf Webseiten des Phishers liegen oder auf Seiten Dritter. Die Phisher bedienen sich hier verschiedener Techniken:

- getarnte Links in bekannten Webseiten und Message Boards
- gefälschte Werbebanner und Grafiken, die zu Phisherseiten führen

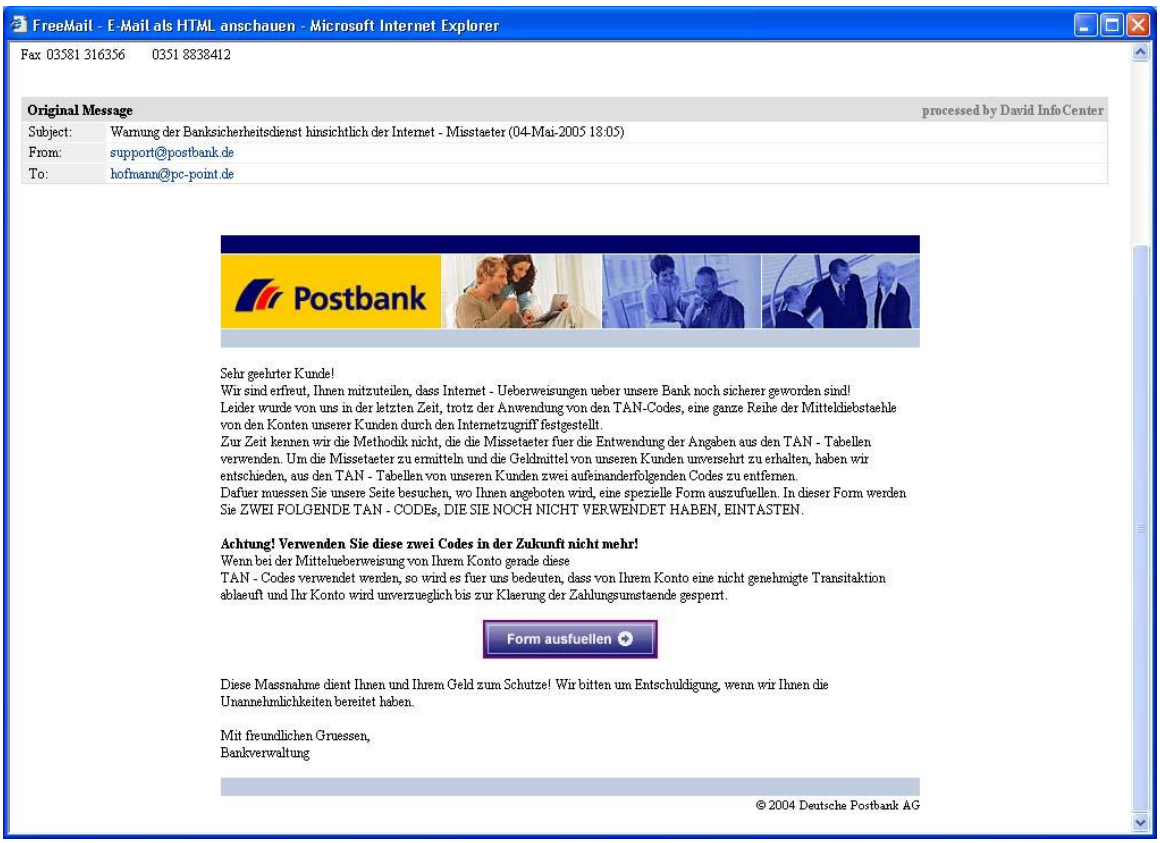


Abbildung 10.5: Beispiel Phishingmail

- Pop-ups zur Verschleierung der Phishernachricht
- eingebettete Inhalte in Webseiten, die Trojaner installieren

Bei der heutigen Fülle an Werbebanner ist es leicht für Phisher eigene Banner zu entwerfen und zu verlinken. Der einzige Aufwand ist die Ziel URL zu fälschen, so dass diese echt aussieht.

IRC und Instant Messaging

Neu in der Welt des Phishers sind IRC und IM Foren. Mit steigender Beliebtheit dieser Kommunikationskanäle steigt auch das Interesse der Phisher. Neuste Clientsoftware bieten die Einbettung dynamischer Inhalte an, was es dem Phisher leicht macht genannte Techniken auch hier anzuwenden. Mit Bots können zu dem leicht getarnte Links verschickt werden.

befallene Internetnutzer als Übertragungsquelle

Als Quelle der Phishingangriffe werden vermehrt Computer von nichts ahnenden Internetnutzern verwendet. Diese werden vorher mit Trojanern befallen und dienen von da

an, als Nachrichtenverteiler. Zu dem werden ganze Netzwerke infiziert, die damit eine schnelle Verteilung einer großen Zahl von Phishingmails ermöglichen. Um nicht eine unverarbeitbare Flut von Informationen zu erhalten, nutzen Phisher Keylogger, die nur bei ausgewählten Schlagwörtern die Tastatureingaben speichern.

10.8.2 Täuschungsmanöver der Angreifer

Um den Erfolg der Angriffe zu sichern nutzen die Angreifer viele verschiedene Methoden, um die Nutzer zu täuschen. Von den folgenden Techniken wird nur auf einige genauer eingegangen:

- Man-in-the-middle Attacken
- URL-Fälschung
- Cross-Site Scripting Attacken
- Session Attacken
- Überwachung der Nutzerdaten / -eingaben
- Nutzen der Schwächen der Client-Software (Webbrowser)

Man-in-the-middle Attacken

Eine sehr erfolgversprechende Technik ist die Man-in-the-middle Attacke. Der Angreifer stellt sich hier zwischen den Nutzer und der Webapplikation und arbeitet als Proxy auf dem gesamten Kommunikationskanal (siehe Abbildung 10.6). Dieser Angriff arbeitet sowohl auf HTTP und HTTPS Verbindungen. Der getäuschte Nutzer verbindet sich hier z.B. über eine gefälschte URL mit dem Phishing-Server, der jede Aktion an das gewollte Ziel weiterleitet und dokumentieren kann. Das funktioniert selbstverständlich in Echtzeit und in beide Richtungen. Somit bemerkt der Nutzer nichts von dem Angriff, auch seine Transaktionen werden korrekt ausgeführt, soweit dies im Sinne des Angreifers ist.

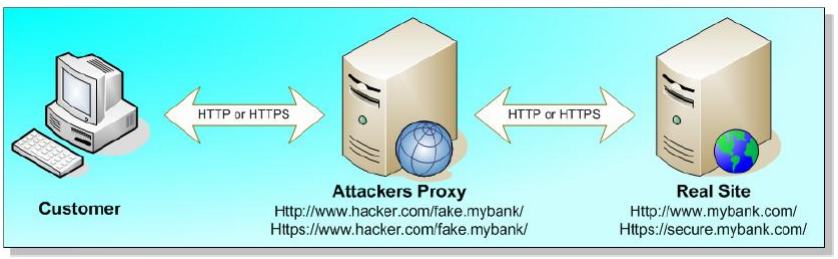


Abbildung 10.6: Man-in-the-middle-Attacke

URL-Fälschung

Ein Grundbaustein der meisten Phishingattacken ist die Nutzung gefälschter Links, um den Nutzer auf ihre Webseiten zu locken. Dafür stehen den Angreifern verschiedene Verfahren zur Verfügung von denen hier einige vorgestellt werden:

- verwirrende Domain-Namen
  Genutzt wird eine gezielte Registrierung von verwirrenden Domainnamen, um ein echt wirkenden Link zu Erzeugen. Beispielsweise ist eine Domain my-ebanking.de mit der Subdomain deutsche-bank denkbar. Der Link wäre dann http://deutsche-bank.my-ebanking.de

- Ausnutzen des URL Verkürzungsdienst
  Da viele URLs mit allen Parametern sehr lang sein können, bieten Organisationen Dienste an, die die URL in eine kürzere umformen und weiterleiten. Dieser Dienst lässt sich leicht von Phishern ausnutzen, um das Ziel des Links zu verschleiern.

- Verschleierung des Hostnamens
  Viele Webbrowser gestatten Authentifizierungen innerhalb der URL für den Login in der Form: URI://username:password@hostname/path. Bei geschickter Wahl des Benutzernamens z.B. postbank.de und des Passwortes z.B. ebanking kann von der eigentlichen Adresse abgelenkt werden. Es ergibt sich dann bspw. die URL http://postbank.de:ebanking@phisher-site.com/fake.htm. Durch das Ersetzen des Domainnamens mit dessen IP-Adresse erhält man eine schwerer erkennbare URL http://postbank.de:ebanking@210.122.144.22/login.htm.

10.8.3 Abwehrmechanismen

Phisher besitzen eine große Zahl an Möglichkeiten, um Internetnutzer anzugreifen und zu täuschen. Somit genügt es nicht eine Lösung zu finden, die alle Angriffe abdeckt. Den besten Schutz hat man, wenn an den drei Ebenen Vorkehrungen getroffen werden:

1. Client Seite
2. Server Seite
3. Unternehmens Seite

Client Seite

Die Client Seite beinhaltet die PCs der Internetnutzer. So unterschiedlich die Erfahrung der Nutzer im Web ist, so unterschiedlich ist auch das Sicherheitsbewusstsein der Nutzer. Hier können an vielen verschiedenen Stellen die Sicherheiten erhöht werden. Durch die Verstärkung des Desktopschutzes durch Antiviren Software, Firewalls, Anti-Spam und Programme, die Spyware erkennen und blocken, können Phishingangriffe verhindert werden. Da ein Großteil der Phishingangriffe durch HTML-basierte E-Mails entstehen, ist es ratsam E-Mails mit HTML-Code zu verbieten. Dazu kommt das Blocken von

möglichen gefährlichen E-Mail-Anhängen. Da nicht alle Nutzer das gesamte Spektrum gängiger Browser nutzen, sollten Browsereinstellungen nur die Technologien freischalten, die benötigt werden. Somit könnte die Deaktivierung verschiedener Technologien, wie Pop-Up Fenster, Java Runtime und ActiveX Unterstützung, Phishingangriffe verhindern. Zu dem existieren Anti Phishing Tools, die in Browser integriert werden können, z.B. Pop-Up-Blocker oder auch Software, die gegebene URLs mit bekannten URLs von Phishern vergleicht.

Server Seite

Durch Einführung von Anti-Phishing Technologien in die Webanwendungen kann schon hier ein Angriff verhindert werden. Einerseits können die Internetnutzer durch die Webseiten zu dem Phishing Thema sensibilisiert werden und andererseits über aktuelle Angriffe gewarnt werden. Ein Hauptproblem bei Phishingangriffen ist die Ungewissheit über die Echtheit der Kommunikation. Bei E-Mails kann dem dahingehend Folge geleistet werden, dass Nutzer persönlich angesprochen werden und Namen z.B. des persönlichen Betreuers auf Seiten der Bank erwähnt werden. Durch Anbieten von Portalen zur Echtheitsprüfung von E-Mails, können sich Nutzer über die Echtheit vergewissern. Viele Probleme entstehen durch schlecht implementierte Sicherheiten bei Eingabe geheimer Daten. So sollten Eingabefelder beim zurückgehen geleert sein und Daten vor der Verarbeitung gereinigt werden. Dazu kommt die Berücksichtigung vieler bekannter Techniken der Phisher, wie das Prüfen, von welchem Link die Seite betreten wurde und das Verbot der Nutzung von IP-Adressen in URL Informationen.

Unternehmer

Sicherheitsmaßnahmen auf Seite der Unternehmer erfordern ein Zusammenspiel der Maßnahmen der Server und Client Seite. Sie beinhalten automatische Überprüfungen der Server, über die E-Mails versendet werden, eine Signatur der E-Mails oder auch eine Überprüfung von Domains mit ähnlichen Namen zu Firmen. Somit können schon vorher vermeintlich bösartige Internetadressen erkannt werden. Gateway Dienste können zu dem eine Überwachung und Kontrolle von ausgehender und ankommender Kommunikation leisten. Diese Dienste können Virenscanner beinhalten, Spam-Filter und Content-Filter, so dass Trojaner nicht durchgelassen werden oder auch Nutzer vom Betreten gefährlicher Webseiten abgehalten werden.

10.9 Zusammenfassung und Ausblick

„Anbieter herkömmlicher Sicherheitssoftware behaupten, es sei unmöglich, jede Art von bösartigem Code eindeutig zu identifizieren. Dies gelte insbesondere für Trojanische Pferde, die aufgrund ihrer geschickten Tarnung eingeschleust werden können. Zudem tauchen ständig neue Varianten auf."[9]

[9] Zitat aus [4]

Diese Aussage ist übertragbar auf jede Art von neuartigen Angriffen. Ob nun rein technischer Natur, durch das Ausnutzen von bekannten und unbekannten Schwachstellen in Softwaresystemen, systemimmanenten Mängeln von Kommunikationsprotokollen wie dem Internet Protokoll, dessen Mängel historisch gewachsen sind (z.B. fehlende Möglichkeiten zur Verschlüsselung und Authentifikation, u.ä.) oder der besonderen Einbindung menschlicher Eigenschaften (Phishing, Aktivierungsprinzipien von Malware) - Sicherheitsvorkehrungen werden im ewigen Rüstungswettstreit mit den Angreifern stehen. Der Kreativität von Angreifern - z.B. neuen koordinierten, synchronisierten dDoS-Attacken per Backdoor-Trojaner ferngesteurter Rechner (Zombies) - können nur Grenzen gesetzt werden, sie können aber nie komplett verhindert werden. Das Schwachstellenpotential dynamisch "lebender"Netzwerke ist jedoch eine nie versiegende Quelle für neuartige Angriffsszenarien. Es gibt ausserdem nicht **die** identifizierbaren kombinierten Angriffskonzepte, sondern nur das Prinzip, dass hoch entwickelte Angriffe Sicherheitsarchitekturen auf mehreren Ebenen und an mehreren Punkten angreifen und deshalb übergeordnet erkannt werden müssen. Zumeist kombinieren sie mehrere Möglichkeiten der Verbreitung (eMail-Anhang, Netzwerk-Hintertüren, Datei-/Betriebssystem-Manipulationen), können Sicherheitssysteme gezielt umgehen (z.B. Stealth-Viren), ihre Identität verschleiern, arbeiten zunehmend verteilt (z.B. dDoS/Botnets), sind schwer lokalisierbar und haben fast immer zerstörerische oder wirtschaftliche Absichten.

Neben traditionellen reaktiven Maßnahmen[10], wie Antiviren-Programmen, Firewalls, Intrusion Detection und Intrusion Prevention Systemen u.ä., bei denen es besonders auf Tages-Aktualität und die richtige Konfiguration ankommt, ist es notwendig die limitierten Ressourcen eines Unternehmens auf die Identifikation und Eliminierung derjenigen Sicherheitslücken auszurichten, die durch interne und externe Angriffe ausgenutzt werden können (relevante IT-Risiken!). Exposure Risk Management eröffnet einen neuen Weg zu einer effizienten und umfassenden Absicherung komplexer IT-Infrastrukturen. In jedem Fall müssen kompetente und konsistente Sicherheitssysteme personelle und funktionelle Aspekte integrieren und übergeordnete organisatorische Rahmenbedingungen einschließen [11].

[10] Eine interessante Möglichkeit, die vielen existierenden reaktiven Technologien zur Bekämpfung bekannter wie auch neuer Gefahren aus dem Netz zu konsolidieren, zu kombinieren, zentral zu administrieren und von ihren Synergieeffekten zu profitieren, ist das Konzept des *integrierten Content Security Management (iCSM)*, das beispielhaft in [13] beschrieben wird.

[11] dazu „[...]Ausgaben der Unternehmen [sind] nicht immer zielgerichtet. Ernst & Young rät, mehr Geld für Personal und Organisation und weniger für Technik auszugeben. Vielfach liege das Sicherheitsproblem in einer falschen Organisation und einer fehlenden Kenntnis der Mitarbeiter.“ , Zitat aus [6]

Literaturverzeichnis

[1] F-Secure, 2005. http://www.f-secure.com/nimda/nimda.shtml.

[2] Sophos, 2005. http://www.sophos.de.

[3] *Exploit*. Wikipedia, 2005. http://de.wikipedia.org/wiki/Exploit.

[4] *Technologie zum proaktiven Blockieren von Code, 10.06.05*. IT SecCity, 2005. http://www.itseccity.de.

[5] *Vorsicht vor falschen Sicherheits-eMails*. Postbank, 2005. http://www.postbank.de/pbde_pk_home/pbde_pk_produkteundpreise/pbde_pk_serviceundkredite/pbde_pk_online_banking/pbde_pk_trojaner_infoseite.html.

[6] FAZ (ht). *Internet-Kriminalität erreicht Europa, 27.09.04*. FAZ.NET, 2004. http://www.faz.net/s/Rub7A5627BF4B684A7C90706514DD856EC4/Doc~EDC30CA28A0694ED49742481F7374E567~ATpl~Ecommon~Scontent.html.

[7] FAZ (ht). *Mydoom richtet Milliardenschäden an, 03.02.04*. FAZ.NET, 2004. http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc~E4EB4DAB0E2F0426C9100A688DC3043DD~ATpl~Ecommon~Scontent.html.

[8] Gunter Ollmann. *The Phishing Guide*. September 2004.

[9] Kryptocrew. *Methodik: Social Engineering, 20.11.2002*. computec.ch, 2005. http://www.computec.ch/dokumente/unsortiert/Social%20Engineering.html.

[10] Prof. Dr. Hans Jürgen Ott. *Daten- und Rechnerssicherheit*. KECoS, 2005. http://www.kecos.de/script/script_create.php?a_tree=tree&line_nr_sel=211&level_sel=1.

[11] Trend Micro Deutschland GmbH (ma). *Phishing-Angriffe nehmen zu und Zombie-Netzwerke breiten sich aus, 14.01.05*. IT SecCity, 2005. http://www.itseccity.de/?url=/content/virenwarnung/statistiken/050114_vir_sta_trendmicro.html.

[12] Verschiedene Autoren. *Dossier: IT-Security*. Computerworld, 2005. http://www.hissoft.ch/presse.html.

[13] webwasher AG. *Kosten senken und Sicherheit erhöhen - durch integriertes Content Security Management*. webwasher AG, 2003. http://www.cyberguard.com/download/white_paper/icsm.pdf.

11 Staatliche und öffentliche Einrichtungen: BSI, CERT, ENISA

Michal_Olejniczak, Jan_Schaumkessel

11.1 Management Summary

Ziel dieser Seminararbeit ist es anderen Studenten und Interessierten den Aufbau, die Arbeitsweise und die Kritikpunkte an öffentlichen Einrichtungen wie dem BSI, der ENISA oder der CERT näher zu bringen. Folgende Vorgehensweise wurde hierbei gewählt: zuerst erfolgt eine Management Summary, in der wir einen Überblick über diese Organisationen geben, sie voneinander abgrenzen, unsere eigene Meinung erläutern und zum Schluss eine Ausblick in die Zukunft wagen. Danach begutachten wir jede Organisation genauer und führen ihre Struktur, Aufgaben und Ziele auf. Als Hilfe dienten hier diverse Medien wie Statistiken und Fotos. Problematisch war jedoch, dass wir zur Internet Security Agency kein Material gefunden haben und deshalb die anderen Organisationen eingehender untersucht haben.

Die wesentliche Erkenntnis war, dass BSI und ENISA vergleichbare Organisationen auf unterschiedlichen Ebenen sind. Das BSI auf Bundes - bzw. auf nationaler Ebene und die ENISA auf europäischer. Die offiziellen Aufgaben scheinen auf den ersten Blick identisch, die Formulierungen scheinen wechselseitig kopiert worden sein.

Auf den zweiten Blick sieht man, dass das BSI im Gegensatz zur ENISA eine aktive Einrichtung mit umfangreichen "Marktaktivitätenïst. Insbesondere das umfangreiche und weit verbreitete IT-Grundschutzhandbuch und die Produktzertifizierung seien hier exemplarisch genannt. Von der ENISA sind derartige konkrete Marktaktivitäten nicht ersichtlich - es scheint sich hier mehr um eine "Lobby-Organisation"der nationalen IT-Sicherheitsorgane auf europäischer Ebene zu handeln.

CERTS hingegen sind Organisationen, welche auf aktuelle technische IT-Sicherheitsprobleme reagieren und Warnungen und zum Teil auch Lösungsansätze an angeschlossene Techniker abgeben. Die CERTS können externe kommerzielle Unternehmen sein (siehe MCert)

oder altruistisch motivierte lose Teams. Große Unternehmen leisten sich eigene CERTs. Aus eigener professioneller Erfahrung in der Abwicklung von BSI-Projekten, hat der Autor ein zwiespältiges Bild vom BSI. Zum einen eine unflexible starre Behörde mit schwacher Führung. Zum andern ein exzellenter Ruf aufgrund von qualifizierten Mitarbeitern. Als problematisch sieht der Autor den Status des BSI als nachgelagerter Behörde des BMI. Daher erklären sich auch kritiklose "Gefälligkeitsgutachtenßu den Einsatzszenarien von Biometrie und RFID in den geplanten neuen Ausweispapieren des BMI.

BSI und ENISA sind keine CERTs, das BSI ist aber am MCert involviert.

Auf dem letzten BSI-Tag hat der BMdI Otto Schili eine stärkere Involvierung des BSI in aktuelle IT-Projekte sowie als Berater in die Gesetzgebung des Bundes angekündigt. Aufgrund des zu erwartenden Regierungswechsels ist die Position der neuen Regierung hierzu noch unklar. Allerdings ist aufgrund der Wichtigkeit der IT-Sicherheitsthematik auch von einer Stärkung des BSI unter einer bürgerlichen Regierung auszugehen.

Die Zukunft der ENISA ist hier schon ungewisser, da ein nennenswerter Beitrag zur IT-Sicherheit (geschweige denn eine merkbare Marktpräsenz) nicht erkennbar ist. Die sich abzeichnende Entwicklung zu einem schlankeren Europa hat keinen Bedarf an derartigen sinnlosen Organisationen. Die Bedeutung der rein technisch und daher nicht ganzheitlich orientierten CERTs wird eher zurückgehen, da sich die Erkenntnis der Notwendigkeit einer ganzheitlichen Betrachtungsweise der IT-Sicherheit weiter durchsetzen wird. Die CERT werden aber ihre technische Nische finden und nicht verschwinden.

11.2 Das BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministerium des Innern. Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft. Als Behörde ist sie damit im Vergleich zu sonstigen europäischen Einrichtungen einzigartig. Derzeit sind dort rund 380 Informatiker, Physiker, Mathematiker und andere Mitarbeiter beschäftigt. Seinen Hauptsitz hat das BSI in Bonn. Die Gründungsgeschichte des BSI reicht in das Jahr 1986 zurück. Zu diesem Zeitpunkt wurde in der Vorgängerorganisation ZfCh (Zentralstelle für das Chiffrierwesen) eine Arbeitsgruppe aufgebaut, die sich vor dem Hintergrund der schnellen Entwicklung der IuK-Technik mit den Sicherheitsfragen beschäftigte. Bis dahin hatte sich die ZfCh auf die zentrale Aufgabe Kommunikationssicherheit konzentriert. Die Arbeitsgruppe vergrößerte sich bald auf 70 Mitarbeiter. Sie befassten sich mit der Evaluierung und Zertifizierung von IT-Produkten und -systemen. Vor allem die Zertifizierung war schließlich der Auslöser für die Gründung einer eigenständigen Behörde, des BSI. 1990 wurde vom Bundestag die Errichtung im Geschäftsbereich des Bundesministeriums des Innern beschlossen.

Die Aufgaben des BSI sind im "Gesetz über die Errichtung des Bundesamtes für Si-

Abbildung 11.1: Abbildung - Der Sitz der BSI

cherheit in der Informationstechnik (BSI-Errichtungsgesetz - BSIG) vom 17. Dezember 1990 geregelt.

Mit der rasanten Fortentwicklung der Informationstechnik entstehen in fast allen Bereichen des Alltags neue IT-Anwendungen - und damit auch immer neue Sicherheitslücken. Je abhängiger der Mensch von der Informationstechnik wird, desto mehr stellt sich die Frage nach deren Sicherheit. Unsere Gesellschaft ist stärker als zuvor durch Computerversagen, -missbrauch oder -sabotage bedroht. Bisher kann nicht ausreichend sichergestellt werden, dass die Informationstechnik das tut, was sie soll, und nichts tut, was sie nicht soll.

Weil die Probleme in der Informationstechnik so vielschichtig sind, ist auch das Aufgabenspektrum des BSI sehr komplex: Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt Sicherheitsvorkehrungen. Es informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und versucht Lösungen dafür zu finden. Dies beinhaltet die Prüfung und Bewertung der IT-Sicherheit von IT-Systemen, einschließlich deren Entwicklung in Kooperation mit der Industrie.

Auch bei technisch sicheren Informations- und Telekommunikationssystemen können Risiken und Schäden durch unzureichende Administration und Anwendung entstehen. Um diese Risiken zu minimieren beziehungsweise zu vermeiden, wendet sich das BSI an eine Vielzahl von Zielgruppen: Es berät Hersteller, Vertreiber und Anwender von Informationstechnik. Darüber hinaus analysiert es Entwicklungen und Trends in der Informationstechnik.

11.2.1 Aufgabenspektrum des BSI

Prüfung und Bewertung der Sicherheit von IT-Systemen

Die Evaluierung und Zertifizierung nach internationalen Kriterien macht die Sicherheitseigenschaften von Produkten transparent. Dies ist für die Konkurrenzfähigkeit im hart umkämpften Markt ein wichtiges Zugpferd; für die Zulassung in Sicherheitsbereichen

von Staat und Industrie ist es Voraussetzung.

Entwicklung von IT-Schutzvorkehrungen

Das BSI entwickelt und vertreibt selbst IT-Sicherheitssysteme, angefangen von Produkten für den Umgang mit klassifizierten Informationen bis hin zu Administrationstools für Unix oder die Umsetzung des IT-Grundschutzes. Die Produkte werden teilweise in enger Kooperation mit Partnern aus der Industrie entwickelt.

Beratung von Herstellern, Vertreibern und Anwendern von IT-Systemen

Die Aufklärungs- und Beratungsleistungen richten sich an private Anwender, IT-Verantwortliche in Behörden und Unternehmen sowie an Hersteller von IT-Produkten. Damit wird gewährleistet, dass alle Beteiligten von Anfang an IT-Sicherheitsaspekte bei Entwicklung und Einsatz der Systeme beachten können.

Mitarbeit in internationalen Gremien

Das BSI vertritt und unterstützt mit seiner Gremienarbeit, z. B. in der Nato und in der EU, die Interessen Deutschlands im Hinblick auf IT-Sicherheitsaspekte. Mit dem Einfluss des BSI sollen Fehlentwicklungen verhindert, der Informationsaustausch gefördert und internationale Kontakte gepflegt werden.

Trendforschung und Projektarbeit zu neuen technologischen Ansätzen

Die frühzeitige und möglichst präzise Vorhersage von zukünftigen Entwicklungen ermöglicht rechtzeitiges, umsichtiges Handeln. Aus diesem Grund beschäftigt sich das BSI in Arbeitsgruppen und Projekten mit allen wichtigen Themen in Bezug auf die kommende IT-Sicherheit. Zu nennen sind hier z.B. Öpen Source Software", die IT-Implementierung in biometrischen Systemen oder die Aktivitäten der Trusted Computing Group (TCG). Ziel dieser Industrievereinigung ist es, einen Sicherheitschip "TPM"(Trusted Platform Module) zur Absicherung verschiedener IT-Geräte - z.B. PCs, Smartphones oder PDAs - zu entwickeln.

11.2.2 Die Köpfe / das Management des BSI

Präsident: Dr. Uwe Helmbrecht Jahrgang 1955, studierter Physiker und Mathematiker, bis 1983 wissenschaftlicher Angestellter am Institut für theoretische Physik der Ruhr-Universität Bochum. Wechsel zu Messerschmitt-Bölkow-Blohm (heute EADS). Bis 1995 dort in verschiedenen Führungspositionen tätig. Vor Amtsantritt beim BSI 2003 Direktor und Bereichsleiter bei der Bayerischen Versorgungskammer, München.

Vize Präsident: Michael Hange Jahrgang 1950, Studium der Mathematik in Bonn. Seit 1977 in der Bundesverwaltung als Referent und ab 1985 als Referatsleiter im Bereich

Abbildung 11.2: Abbildung - Dr. Uwe Helmbrecht/Michael Hange

IT-Sicherheit tätig. Mit Gründung des BSI Abteilungsleiter und maßgeblich am Auf - und Ausbau beteiligt. Seit 1994 Vizepräsident und in dieser Funktion als nationaler Direktor für Kommunikationssicherheit deutscher Repräsentant in IT-Sicherheitsgremien der NATO und EU.

11.2.3 Die wichtigsten Anwendungsbereiche des BSI

2.3.1 Der IT-Grundschutz

Leitung: Herr Dr. Isselhorst / Frau Münch Aufgaben: Entwicklung und Weiterpflege des IT-Grundschutzhandbuches.

2.3.2 Die Produktzertifizierung nach Common Criteria

Leitung Herr Kowalsky / Frau Dr. Rührmann Aufgaben: Entwicklung und Weiterpflege der CC und entsprechender PPs (Schutzprofile) Zertifizierung nach CC (Common Criteria) Zertifizierung nach IT-Grundschutz

Abbildung 11.3: Abbildung - Durch das BSI vergebene CC-Zertifikate

An dieser Statistik sieht man gut, dass sich die BSI- Zertifikate in den letzten Jahren enorm gesteigert und etabliert haben, was auf eine gesteigerte Aufmerksamkeit und Bedeutung in der IT - Industrie und Öffentlichkeit zurückzuführen ist.

11.3 ENISA

Sitz: Heraklion,
Griechenland Gründungsjahr: 14.03.2004

Die rasante Entwicklung der Kommunikationsnetze und Informationssysteme wirft unweigerlich die Frage nach ihrer Sicherheit auf, die für die Gesellschaft mehr und mehr an Bedeutung gewinnt. Die zunehmende Zahl von Sicherheitsverletzungen hat bereits erheblichen finanziellen Schaden verursacht, das Vertrauen der Nutzer untergraben und war der Entwicklung des elektronischen Handels abträglich. Darüber hinaus besteht immer die Gefahr, dass ein Angriff auf die zentralen Informationssysteme schwer wiegende Auswirkungen auf die Verfügbarkeit wesentlicher Dienste für die Bürger Europas hat. Mit der steigenden Anzahl an Internetverbindungen und der stärkeren Vernetzung werden die Sicherheitsanforderungen künftig noch schärfer gefasst werden müssen.

Einzelpersonen, Behörden und Unternehmen haben darauf reagiert, indem sie Sicherheitstechnologien und -verfahren einsetzen. Die Reaktionen der Mitgliedstaaten haben sich jedoch als untauglich und ungenügend koordiniert erwiesen, um den Sicherheitsproblemen wirksam entgegentreten zu können. Abgesehen von einigen Verwaltungsnetzen gibt es zwischen den Mitgliedstaaten auf diesem Gebiet keine systematische grenzübergreifende Zusammenarbeit, obwohl die Sicherheitsfragen gewiss nicht als isolierte Probleme anzusehen sind, die jeweils nur ein einzelnes Land betreffen. Aufgrund dieser Erkenntnisse und der Notwendigkeit angemessener Antworten auf diese Bedrohungen haben die europäischen Stellen eine Agentur für Netz- und Informationssicherheit (ENISA) geschaffen.

11.3.1 Ziele

Durch die Schaffung der ENISA sollen in erster Linie die Kapazitäten der Europäischen Gemeinschaft, der Mitgliedstaaten und der Unternehmen hinsichtlich der Reaktion auf die Bewältigung von Problemen der Netz- und Informationssicherheit verstärkt werden. Darüber hinaus soll die Agentur die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor erleichtern und fördern, damit auf diese Weise ein hinreichend hohes Sicherheitsniveau in allen Mitgliedstaaten erreicht wird. Schließlich kann die Agentur der Kommission bei der Durchführung technischer Vorarbeiten für die Aktualisierung und Weiterentwicklung des Gemeinschaftsrechts im Bereich Netz- und Informationssicherheit behilflich sein.

11.3.2 Aufgaben

Um die oben dargelegten Ziele zu erreichen, soll die Agentur folgende Aufgaben erfüllen:

- Erhebung geeigneter Informationen zur Analyse der derzeitigen und absehbaren Risiken für die Netz- und Informationssicherheit sowie Bereitstellung der Analyseergebnisse für die Mitgliedstaaten und die Kommission;

- Beratung des Europäischen Parlaments, der Kommission und anderer zuständiger Stellen sowie ggf. Unterstützung im Rahmen ihrer Ziele;
- Förderung der Zusammenarbeit zwischen den verschiedenen in diesem Bereich tätigen Akteuren (z. B. durch Anhörungen der Industrie und der Hochschulen) und Erleichterung der Zusammenarbeit zwischen der Kommission und den Mitgliedstaaten bei der Entwicklung gemeinsamer Methoden zur Verhinderung von Sicherheitsproblemen;
- Beitrag zur Sensibilisierung und zur frühzeitigen, objektiven und umfassenden Informationsvermittlung in Fragen der Netz- und Informationssicherheit für alle Nutzer. Dies kann durch Förderung des Austauschs der jeweils besten Verfahren, einschließlich der Verfahren zur Warnung der Nutzer erreicht werden;
- Unterstützung der Kommission und der Mitgliedstaaten in ihrem Dialog mit der Industrie, um sicherheitsrelevante Probleme bei Hardware- und Softwareprodukten anzugehen;
- Verfolgen der Entwicklung von Standards für Produkte und Dienstleistungen im Bereich der Sicherheit sowie Förderung von Risikobewertungsmaßnahmen;
- Beitrag zu den Bemühungen der Gemeinschaft um eine Zusammenarbeit mit Drittländern und internationalen Organisationen zur Förderung eines gemeinsamen Gesamtkonzepts in Sicherheitsfragen.

11.3.3 Organisation

Die Agentur besteht aus

- einem Verwaltungsrat aus Vertretern der Mitgliedstaaten und der Kommission;
- einem Direktor, der auf der Grundlage einer Bewerberliste der Kommission vom Verwaltungsrat ernannt wird;
- einer ständigen Gruppe der Interessenvertreter, die vom Direktor eingesetzt wird und sich aus Vertretern der Industrie und der Verbraucher sowie wissenschaftlichen Sachverständigen zusammensetzt. Über diese Gruppe erhält die Agentur Zugang zu den neuesten Informationen, die eine Antwort auf die Bedrohungen der Netzsicherheit bieten können.

Die Agentur gewährleistet einen problemlosen Zugang der Öffentlichkeit und interessierter Kreise zu objektiven und zuverlässigen Informationen, insbesondere zu ihren eigenen Arbeitsergebnissen.

11.3.4 Überprüfungsklausel

Innerhalb von drei Jahren nach der tatsächlichen Einrichtung der Agentur wird die Kommission eine Bewertung vornehmen, wobei sie

- angibt, ob die Agentur über den festgelegten Zeitraum hinaus fortbestehen soll;
- Arbeitsweise und Einfluss der Agentur bewertet;
- die festgelegten Ziele und Verfahren grundlegend überprüft;
- ggf. prüfen soll, welche Veränderungen in Anbetracht der Entwicklung der institutionellen und rechtlichen Situation in der EU und auch im Hinblick auf weiterreichende Sicherheitsprobleme angebracht sein könnten.

11.3.5 Zusammenfassung

Der Aufgabenbereich der ENISA ist sehr breit ausgelegt. Die wichtigste Herausforderung besteht darin, in allen EU Staaten eine hohe Sicherheit in der elektronischen Kommunikation zu gewährleisten. Das ist mehr als verständlich, weil die einzelnen Mitgliedsstaaten einen anderen Ansatz zu diesem Problem verfolgen. Darüber hinaus sind die einzelnen Staaten unterschiedlich fortgeschritten in ihren Arbeiten. Im Prinzip ist das der Grund, wieso ENISA überhaupt entstanden ist. Man wollte einfach eine Einheit ins Leben berufen, die auf der europäischen Ebene tätig ist, die als wichtigster Ratgeber fungiert und dem EU-Parlament zur Seite steht. Wichtig ist noch ein anderer Tätigkeitsbereich der ENISA: die Entwicklung einer SSicherheitskulturïn der EU. Wieso ist das so wichtig? Nun, der erste Punkt ist, dass durch solche eine SSicherheitskulturës möglich wäre, neue Technologien schnell aufzunehmen und zu verwenden, wobei das Sicherheitsniveau konstant hoch wäre. Die Folge daraus wäre, dass die europäischen Märkte in der Lage wären, die Anforderungen der Konsumenten und Unternehmen besser zu erfüllen. Für ENISA ist noch eine wichtige Rolle vorgesehen: sie sollte auch kleinen und mittleren Unternehmen zur Seite stehen. Diese Unternehmen könnten dann die ENISA als einen Ratgeber sehen, wenn es um Informations- und Netzwerksicherheit geht. Die Unabhängigkeit von ENISA kann dazu beitragen, dass die Industrie bei der Bearbeitung von Sicherheitsproblemen aktiv partizipiert. Es ist klar, solche Situation wäre sehr wünschenswert, man könnte dann die neusten Sicherheitsrichtlinien gleich praktisch realisieren. Umgekehrt, die neuen Sicherheitsrichtlinien wären dann auch mehr praxisbezogen.

Das Thema IT-Sicherheit sollte eher global und international gesehen werden, und nicht national bzw. lokal. Jetzt ist ein passender Moment, diese Forderung nachzukommen. Schließlich wurde die EU vor kurzem erweitert und die neuen EU-Staaten sind nun angehalten, Vorgaben und Richtlinien der EU anzuwenden und umzusetzen. Selbst nach der Gründung von ENISA ist eine konkrete, an die tägliche Praxis ausgerichtete, Hilfestellung notwendig. Vor allem die Erfahrung der BSI bei dem Aufbau der

IT-Sicherheitsinfrastrukturen und im Gebiet der IT-Sicherheit in der öffentlichen Verwaltung wäre hier sehr gefragt. Soweit bekannt, ist die BSI bereit mitzumachen[1].

Die Zukunft, die ENISA bevorsteht, ist äußerst ungewiss. Die Organisation hat bis jetzt noch kein Vertrauen und keine Marktpräsenz aufbauen können. Da in der Zukunft mit einem Abbau der Bürokratie und demzufolge von einem schlankeren Europa auszugehen ist, sind die Perspektiven für ENISA eher düster.

11.4 CERT

CERT steht für Computer Emergency Response Team. Hierbei handelt es sich um Organisationen, die sich mit Computersicherheit befassen, Warnungen vor Sicherheitslücken herausgeben und Lösungsansätze bieten. Der Informationsfluss erfolgt dabei zumeist über Mailinglisten. Dort werden sicherheitskritische Themen erörtert und aktuelle Warnungen ausgegeben. Dabei ist zu beachten, dass CERT eine rein technische Organisation darstellt.

Die wichtigste Einheit ist das CERT Coordination Center (CERT/CC). Diese befindet sich an der Carnagie Mellon University in Pittsburgh am Software Engineering Institute (SEI) und ist ein Forschungs - und Entwicklungszentrum, das von der US Amerikanischen Regierung finanziell unterstützt wird. In November 1988 hat der Morris Wurm 10% der Internetsysteme zum Stillstand gebracht. Daraufhin hat die DARPA (Defense Advanced Research Project Agency) die SEI beauftragt, ein Zentrum zu gründen, dessen Aufgabe wäre, die Kommunikation zwischen den Experten während eines Sicherheitsnotfalls zu koordinieren und zukünftige Vorfälle zu vermeiden.

11.4.1 Analyse der Sicherheitslücken und Reaktion auf Vorfälle

Das wichtigste Ziel ist es, den Zustand der Internetsicherheit zu analysieren und die dadurch gewonnenen Erkenntnisse an die Systemadministratoren, Netzbetreuer und andere Personen in der Internetgemeinschaft zu übermitteln. Dabei wird bei der Erkennung von Sicherheitslücken und gefährlichen Aktivitäten Priorität zugewiesen. Die Angriffe, die die Internet Infrastruktur direkt betreffen (z.B. NSP, ISP, DNS, Router), erhalten eine höhere Priorität.

CERT/CC überwacht öffentliche Quellen, die über Sicherheitslücken berichten, und erhält selber Meldungen über Sicherheitslücken. Seit der Gründung in 1988 sind bereits Meldungen über 16,725 Sicherheitslücken eingetroffen. Wenn so eine Meldung eintrifft, dann untersuchen die Sicherheitsexperten die potentielle Sicherheitslücke. Dabei wird eng mit den Technologieherstellern zusammengearbeitet, diese werden über die Sicherheitsdefizite in ihren Produkten informiert. Die CERT/CC Mitarbeiter wollen auch erreichen, dass Produktanbieter die Standardsicherheit ihrer Produkte aufbessern und

[1] Quelle: http://5jahre.a-sit.at/praesentationen/bsi_2004-10-28.pdf

verschiedene Sicherheitsaspekte auch in die Basisversionen aufnehmen. CERT/CC interagiert mit mehr als 600 Hardware- und Softwareentwicklern, die unterschiedliche Methoden verwenden, um ihre Produkte zu verteilen und natürlich die Wahl haben, den Quellcode zur Verfügung zu stellen oder nicht.

Als Antwort auf die steigende Anzahl von Vorfällen, wurde das System AirCERT entwickelt. Es ist ein automatisiertes ïncident-reportingSSystem, mit dessen Hilfe es möglich ist, einen Echtzeitüberblick über die Vorfälle zu gewinnen. Dadurch ist es auch möglich Änderungen auf der Bedrohungsebene zu verfolgen. AirCERT ist zurzeit als ein OpenSource Projekt verfügbar.

11.4.2 Survivable Enterprise Management

Das Ziel ist es, verschiedenen Organisationen zu helfen sich selbst zu schützen und zu verteidigen. Es wurden zahlreiche Risikenabschätzungen entwickelt, die den Unternehmen dabei helfen, Informationsvermögen zu identifizieren und charakterisieren, als auch die Risiken, die mit diesem Informationsvermögen verbunden sind, zu identifizieren. Die Unternehmen können die Ergebnisse der Abschätzungen in ihre Sicherheitsstrategie einfließen, oder aber anhand dieser Ergebnisse eine komplett neue Sicherheitsstrategie entwickeln.

Eine Technik, zur Identifikation von Risiken in einem Netzwerksystem ist die OCTAVE (Operational Critical Threat Asset and Vulnerability Evaluation)Technik. Diese Methode kann auf ein einzelnes Unternehmen zugeschnitten werden. Sie berücksichtigt das Vermögen, die Bedrohungen und Sicherheitslücken (sowohl organisatorischer als auch technischer Natur). Dadurch gewinnt ein Unternehmen einen kompletten Überblick über den Stand der Systemsicherheit.

11.4.3 Ausbildung und Training

Dadurch, dass die Netzwerke global miteinander verbunden sind, entsteht eine große Herausforderung: die Einzelpersonen in den Unternehmen entsprechend auszubilden, damit die Sicherheit und Überlebensfähigkeit der Systeme verbessert wird. Deswegen werden für technische Mitarbeiter und Manager, Systemadministratoren und für das technische Personal entsprechende Ausbildungslehrgänge angeboten (z.B. OCTAVE, Informationssicherheit für technische Mitarbeiter usw.).

11.4.4 Überlebensfähige Netzwerktechnologien

In diesem Bereich konzentriert man sich auf die technische Basis zur Identifikation und dem Verhindern von Sicherheitsschwachstellen, als auch auf das Aufbewahren von essentiellen Diensten im Falle, dass in ein System eingedrungen oder das System gefährdet wird.

Ein anderer Aspekt der Forschung ist das „survivable systems engineering". Es umfasst die Analyse, inwiefern Systeme gegen raffinierte Angriffe anfällig sind und Methoden, wie man den Systementwurf verbessern kann. Es werden auch Techniken entworfen, mit dessen Hilfe es möglich sein wird, aktuelle und potenzielle Bedrohungen im Internet abzuschätzen. Diese Techniken beinhalten das Überprüfen einer großen Menge von Netzwerkdaten um schädliche Aktivitäten zu identifizieren.

11.4.5 Zusammenfassung

CERT ist schon seit einigen Jahren in dem Bereich IT-Security tätig. Interessant ist es zu beobachten, wie sich die Statistiken[2] im Laufe der Jahre verändert haben. Im ersten Jahr der Tätigkeit hat CERT nur auf 6 Geschehnisse reagiert. Im Jahr 1997 waren es schon 2134 und in den ersten drei Quartalen von 1998 steig die Zahl auf 2497 Geschehnisse. Daraus könnte man zwei Folgerungen ziehen: CERT hat sich im Bereich IT-Sicherheit etabliert und die Zahl der schädlichen Aktivitäten und Sicherheitslücken rapide gestiegen ist. Um den zweiten Punkt noch mehr zu verdeutlichen, hier ein Paar Zahlen, die die Entwicklung der gemeldeten Sicherheitslücken darstellen[3]:

Jahr	Sicherheitslücken
1995	171
1996	345
1997	311
1998	262
1999	417

Tabelle 1 Sicherheitslücken, 1995-1999

Jahr	Sicherheitslücken
2000	1,090
2001	2,437
2002	4,129
2003	3,784
2004	3,780
1Q2005	1,220

Tabelle 2 Sicherheitslücken, 2000-2005

Darüber hinaus sind auf der CERT-Website viele interessante Artikel zu finden, die sich mit der Sicherheitsproblematik befassen. Dabei wird ein breites Spektrum von Themen behandelt: von den besten Sicherheitspraktiken und der Risikenanalyse, bis zum

[2] Quelle: http://www.cert.org/about/10thBD12-98.htm
[3] Quelle: http://www.cert.org/stats/cert_stats.html

Cyberterrorismus und Internetbetrug. CERT publiziert auch die sogenannten Ännual Reports", wo die schwerwiegendsten Probleme und Sicherheitslücken aufgelistet und beschrieben werden. Für das Jahr 2003[4] waren die zwei gefährlichsten Aktivitäten, die gemeldet worden der W32/Sobig.F Wurm (ein E-Mail Wurm der sich im Anhang befindet und sich selbst weiterverschickt) und der MS-SQL Server Wurm (Dieser Wurm nutzt verschiedene Schwachstellen im MS-SQL Server, es ist dann möglich geheime Informationen auszulesen und Datenbanken zu manipulieren). Die gefährlichsten Sicherheitslücken waren die im RPC Interface und die im Internet Explorer (in beiden Fällen konnte der Eindringling Code ausführen oder DoS Angriffe durchführen).

Wie bereits erwähnt, konnte sich CERT in dem Gebiet Sicherheit etablieren. Das liegt vor allem daran, dass CERT eine sehr gute Reputation erlangt hat, hinsichtlich der Objektivität und der Diskretion. Die Organisationen versorgen CERT mit Informationen (auch geheimen oder vertraulichen) über Sicherheitslücken und Sicherheitskompromisslösungen, weil CERT imstande ist, ihre Identität geheim zu halten. CERT ist mit dem SEI verbunden, was zur Folge hat, dass CERT neutral bleiben kann. Dass hingegen ermögliche eine unbefangene Zusammenarbeit mit der Industrie und mit den Regierungsagenturen. Daraus folgt ein großes Vertrauen der Gemeinschaft, dadurch ist es auch möglich zuverlässige Trends und Charakteristiken der schädlichen Aktivitäten zu erstellen. Daher ist es eine sehr wichtige Organisation, die dazu beiträgt, dass die IT-Welt sicherer gestaltet werden kann, aber die Bedeutung der CERT wird in Zukunft eher zurückgehen, da sich die ganzheitliche Betrachtungsweise der IT-Sicherheit etablieren wird. CERT wird aber nicht ganz verschwinden, denn sie wird eine technische Nische finden, in der sie weiter existieren wird.

[4] Quelle: http://www.cert.org/annual_rpts/cert_rpt_03.html

Literaturverzeichnis

[1] http://www.bsi.de.

[2] http://www.Persicon.com.

[3] http://www.enisa.eu.int.

[4] http://www.cert.org.

[5] *BSI Einrichtungsgesetz*.

[6] BSI. Geschäftsbericht des BSI aus dem Jahre 2003. 2003.