BADEN-
WÜRTTEMBERG

Sicherheit für Benutzer der Internet-Technologie

Studie

Forschungsinstitut für anwendungsorientierte Wissens-
verarbeitung, Ulm

Juli 1997

Erstellt im Auftrag des Landes Baden-Württemberg

vertreten durch die

Stabsstelle für Verwaltungsreform im Innenministerium

FAW Ulm

INNEN-
MINISTERIUM

Titel	Sicherheit für Benutzer der Internet-Technolgie
Herausgeber	Forschungsinstitut für anwendungsorientierte Wissensverarbeitung (FAW)
Erstellt durch	Ahmet Arslan, Wolf-Fritz Riekert Forschungsinstitut für anwendungsorientierte Wissensverarbeitung (FAW) an der Universität Ulm Helmholtzstraße 16 89081 Ulm Internet-Mail: arslan@faw.uni-ulm.de
Auftraggeber	Land Baden-Württemberg vertreten durch die Stabsstelle für Verwaltungsreform im Innenministerium Dipl.-Math. G. Schäfer, Internet-Mail: Schaefer@sik.im.bwl.de
Hinweise	Die Bewertung und Beschreibung der genannten Techniken und Produkte erfolgt nach sorgfältiger Analyse und ohne Nennung von Handels- und Urheberrechten. Dennoch können sich bei der Komplexität der behandelten Materie Fehler eingeschlichen haben. Der Verfasser, das FAW (Auftragnehmer) und das Innenministerium Baden-Württemberg (Auftraggeber) können deshalb keine Gewähr für die Richtigkeit aller gemachten Aussagen übernehmen.
Copyright © 1997	
Nutzungsregelung	

Inhaltsverzeichnis

1 Einsatz der Internet-Technologie in Verwaltung, Unternehmen und im privaten Bereich

Das Internet ist ein weltweites Computernetz, in dem hunderttausende größere Rechnerverbünde und somit Millionen einzelner Computer zusammengeschlossen sind. Das Internet hat sich zum weltgrößten und mächtigsten globalen Informations- und Kommunikationsmedium entwickelt und stellt die Quelle der größten Innovationen nicht zuletzt auf dem Gebiet der Sicherheit dar.

Inzwischen haben sich viele Unternehmen etabliert, die die wirtschaftlichen Vorteile des Internet erkannt haben. Dabei steht in erster Linie nicht die Informationsbeschaffung, sondern die betriebliche Kommunikation, der Datenaustausch, die Produktwerbung und der Kundenservice im Vordergrund. Der Grundsatz „der Stärkere schluckt den Schwächeren“ wird im Zeitalter der Internets abgelöst durch den Grundsatz „der Schnellere schluckt den Langsameren“.

Auch die Verwaltungen gestalten ihre Informations- und Kommunikationstechnik (IuK), indem sie die Vorteile des Internets ausnutzen. Seit Anfang 1996 gilt in Baden-Württemberg das „Architekturmodell der Landesverwaltung Baden-Württemberg für offene Systeme“ (IM 1996), das den Einsatz der schon seit den 80er Jahren benutzten Internet-Protokolle sowohl im internen Landesverwaltungsnetz (sog. „Landesintranet“) sowie für die Kommunikation mit externen Rechnern im globalen Internet regelt. Damit ist die Internet-Technologie fester Bestandteil der IuK-Strategie der Landesverwaltung.

Diese Internet-Technologie bietet den Nutzern erhebliche Produktivitätsvorteile, jedoch ist die Nutzung dieser Dienste auch mit Risiken verbunden. Die vorliegende Studie versucht solche Risiken aufzuzeigen und ihnen Schutzmechanismen und Maßregeln gegenüberzustellen, mit denen unerwünschte Effekte weitestgehend verhindert werden können.

Die Nutzungsarten des Internets können in drei verschiedene Anwendungsszenarien unterteilt werden, die unterschiedliche Ausmaße an Sicherheitsrisiken mit sich bringen:

1. Direktanschluß an das Internet

Hier wird ein einzelner Rechner per Modem und Telefonleitung über einen Provider an das Internet angeschlossen (Abbildung 1). Diese Variante spielt besonders bei kleinen Behörden und im privaten Bereich ein große Rolle. Bei eventuellen Angriffen besteht ein Sicher-

heitsrisiko nur für den einzelnen Rechner und läßt sich durch entsprechende Maßnahmen auf ein Minimum reduzieren.

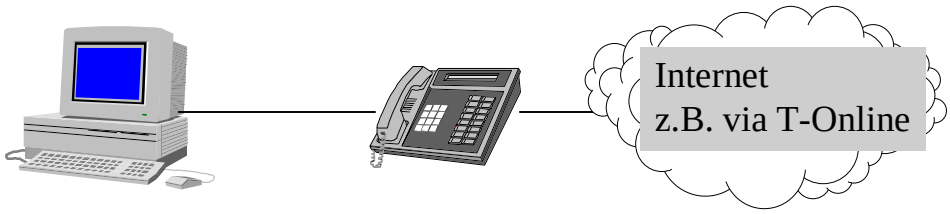

Abbildung 1: Direktanschluß an das Internet

2. Nutzung des Internets in einem Intranet

Neben dem Internet-Anschluß verfügt der Rechner gleichzeitig über eine Verbindung zu einem Intranet, im Land Baden-Württemberg beipielsweise zum Landesintranet (Abbildung 2). Bei eventuellen Angriffen besteht nicht nur ein Sicherheitsrisiko für den an das Internet angeschlossenen Rechner sondern auch für das Intranet. Die zu ergreifenden Sicherheitsmaßnahmen sind entsprechend komplizierter.

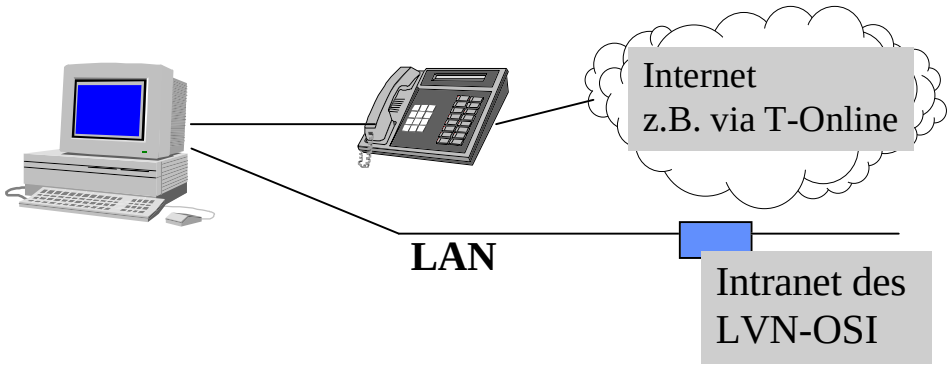

Abbildung 2: Nutzung des Internets in einem Intranet

3. Einsatz der Internet-Technologie in einem Intranet

Der Rechner ist nur in einem Intranet integriert, in dem alle Internet-Technologien zum Einsatz kommen (Abbildung 3). Intranets werden zunehmend in Verwaltungen sowie in vielen Unternehmen zum Informationsaustausch und zur Kommunikation verwendet. Diese Variante stellt ein geringes Sicherheitsrisiko dar, da hier nur ein Angriff von Personen innerhalb des in vielerlei Hinsicht geregelten Intranets stattfinden kann. Durch entsprechende Mechanismen können auch hier die Risiken minimiert werden.

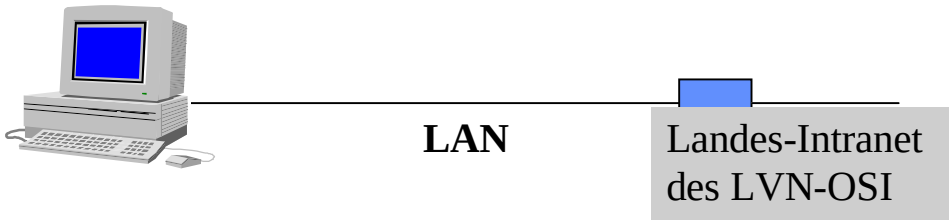

Abbildung 3: Einsatz der Internet-Technologie in einem Intranet

In der Landesverwaltung Baden-Württemberg bestehen zu allen eingesetzten Techniken Datenschutz- und Sicherheitskonzepte sowie eine Konzeption zum Einsatz kryptografischer Sicherheitsarchitekturen (IM 94, IM 96, IM 97/1, IM 97/2). Eine zusammenfassende und erläuternde Darstellung ist in (Schäfer, 97) veröffentlicht.

2 Internet-Technologie aus Sicht des Nutzers

Um die Dienste des Internet nutzen zu können, muß ein Zugang zum Internet existieren. Internetzugänge werden inzwischen von vielen Anbietern, den sogenannten Providern, angeboten, die sich durch unterschiedliche Dienstleistungen auszeichnen. Es existieren zwei verschiedene Zugangsarten:

- Direktanschluß an das Internet

  Bei dieser Zugangsart wird ein Rechner zu einem Bestandteil des Internet. Beliebig viele andere Rechner, die über ein lokales Netz auf diesen Rechner zugreifen, bilden eine sogenannte Domäne und können die Dienste des Internet nutzen. Beispielsweise heißt der Domänenname des FAW, *faw.uni-ulm.de*. Diese Zugangsart stellt eine flexible aber auch teure Möglichkeit dar und bietet sich nur für Institutionen an, die einer größeren Zahl von Rechnern, beispielsweise in ihrem Intranet, den Internetzugang ermöglichen wollen.

- Zugang über ein Modem

  Bei dieser Zugangsart wird über ein Modem (Analog, ISDN) eine Verbindung zu einem System des Providers, das Zugang zum Internet hat, hergestellt. Typischerweise wird hierbei die Domäne des Providers genutzt, z.B. „T-Online.de“ oder „aol.com“. Je nach erforderlicher Bandbreite kann hierzu eine Standleitung oder auch eine Wählleitung verwendet werden. Zum Anmelden auf dem System ist jedoch eine Zugangsberechtigung erforderlich, über die eine Zuordnung der genutzten Dienste für die Abrechnung erfolgt. Generell stehen bei dieser Zugangsart - je nach Provider - nicht alle Dienste des Internet zur Verfügung bzw. müssen extra bezahlt werden.

Alle Dienste, die dem Nutzer innerhalb des Internet zur Verfügung stehen, unterliegen prinzipiell demselben Schema und zwar dem sogenannten Client-Server Prinzip. Ein Server ist eine Instanz, die verschiedene Dienstleistungen wie Datenbankabfragen, Dateitransfer oder Informationsrecherche usw. ermöglicht. Ein Client nutzt die Dienste von Servern. Der Client ist ein Programm oder ein Gerät und stellt entsprechende Anforderungen an den Server, der die gewünschten Dienstleistungen erbringt und gegebenenfalls Ergebnisse zurückliefert.

Die wichtigsten Dienste im Internet werden im folgenden kurz dargestellt:

Email (Electronic Mail)

Email, ein Dienst zum Verschicken von elektronischer Post

Email (elektronische Post) ist einer der meistgenutzten Dienste im Internet. Er ermöglicht das Verschicken von elektronischer Post an beliebige Teilnehmer im Netz, die über eine entsprechende Email-Adresse verfügen müssen. Email bestand ursprünglich nur aus einer Nachricht in Textform und Zusatzinformationen wie Absender, Betreff und Weiterleitung. Inzwischen wird das Anhängen von beliebigen Dateien an die Email unterstützt, womit ein einfacher Dateiversand ermöglicht wird.

FTP (File Transfer Protocol)

FTP, ein Dienst zum Dateitransfer im Netz

FTP ermöglicht den komfortablen Zugriff auf Dateien und Dateistrukturen über Netzwerke hinweg. Mit FTP können Dateien auf dem lokalen und auf dem entfernten Rechner angelegt, kopiert, gelöscht usw. werden, sofern der Server dies dem jeweiligen Nutzer erlaubt und dieser sich mit Hilfe eines Paßwortes ordnungsgemäß identifiziert hat. Im Internet existieren inzwischen unzählige Server, die ein breites Spektrum von frei verfügbaren Programmen (Shareware, Public Domain) anbieten. Diese FTP-Archive sind über die Benutzerkennung *anonymous* und Eingabe der Mailadresse als Paßwort für jeden zugänglich.

Telnet

Telnet, ein Dienst zum Aufbau von Terminalverbindungen zu anderen Rechnern im Netz

Mit Hilfe von Telnet lassen sich Terminalsitzungen (Remote Login) an entfernte Rechner in einem Netzwerk aufbauen. Hierzu ist eine Zugangsberechtigung (Account) oder ein öffentlicher Zugang auf dem entfernten Rechner notwendig. Telnet wird unter anderem zur Fernwartung von Rechnern oder Verwendung von Informationssystemen (Datenbanken, Bibliotheksinformations-systeme) eingesetzt.

World-Wide-Web (WWW)

WWW, ein Informationsdienst im Internet

Das World-Wide-Web (WWW) ist der jüngste Informationsdienst im Internet und basiert auf der Hypertext-Technologie. Hypertext nennt man eine Präsentationsform von Text oder anderen Informationen, die durch sogenannte Links (Hyperlinks) untereinander verknüpft sind. Zur Definition von Hypertextseiten wird die sogenannte Hypertext-Markup-Language (HTML) verwendet. Die Übertragung der Hypertextseiten zwischen Client und Server erfolgt mittels des HTTP-(Hypertext Transfer Protocol) Protokolls.

Über entsprechende WWW-Clients (auch Browser genannt), die in der Lage sind, unterschiedlichste Arten von Informationen wie z.B. Text, Grafik, Audio und Video darzustellen, können Hypertext-Dokumente von WWW-Servern angefordert und angezeigt werden. Entlang der Hyperlinks kann man sich von einem Dokument zum nächsten bewegen, was auch als „surfen“ im WWW bezeichnet wird.

WWW, Integration vieler Internet-Dienste

Ein weiterer Vorteil des WWW ist die Tatsache, daß die wichtigsten anderen Dienste im Internet (u.a. Email und FTP) ebenfalls durch das WWW integriert werden und somit unter einer einheitlichen Benutzeroberfläche zur Verfügung stehen. Beispielsweise wird bei der Anwahl eines Hyperlinks, der auf eine Datei auf einem FTP-Server verweist, automatisch über Dateitransfer diese Datei heruntergeladen.

Zur Identifizierung der Dokumente auf den verschiedenen Servern verwendet man spezielle Netzwerkadressen, sogenannte URL (Uniform Resource Locator). Die URL setzt sich aus der Zugriffsmethode, die den Transport verschiedener Daten und Dokumente regelt, den Namen des Rechners, auf dem sich die Daten befinden und den genauen Verzeichnis-Pfad, in dem sich das Dokument befindet, zusammen. Somit kann direkt in der URL über die Zugriffsmethode angegeben werden, welcher Dienst (z.B. ftp, http) verwendet werden soll (z.B. http://www.faw.uni-ulm.de).

Hypertext-Dokumente können auch Interaktionskomponenten, sogenannte WWW-Formulare, enthalten, über die der Nutzer Informationen eingeben und an den WWW-Server übertragen kann. Die zum Server übertragenen Daten können mit Hilfe von Programmen ausgewertet werden, die in einer beliebigen Programmiersprache geschrieben sind. Zum Anschluß derartiger Programme an einen WWW-Server steht das sogenannte Common Gateway Interface (CGI) zur Verfügung.

Durch die WWW-Formulare wird zwar ein gewisser dynamischer Ablauf innerhalb der WWW-Seiten erreicht, jedoch muß für jede Interaktion des Benutzers eine Verbindung mit dem Server aufgebaut werden. Des weiteren findet keine Lastverteilung zwischen dem Server und dem Client statt. Während der Server bei vielen Anfragen sehr stark belastet wird, ist der Client im Wartezustand. Das Verlangen nach einer Lastverteilung vom Server auf den Client sowie mehr Interaktivität auf den WWW-Seiten, forcierte zum Teil die Entwicklung von Java, JavaScript und ActiveX. Darauf wird im folgenden näher eingegangen.

Java

Java, eine Programmiersprache für heterogene Systeme

Java ist eine objektorientierte Programmiersprache, die bei Sun Microsystems entwickelt wurde, um sichere, architekturunabhängige Programme für heterogene Netzwerke schreiben zu können. Java bietet die Möglichkeit, Stand-Alone-Anwendungen (Java-Applikationen) sowie Anwendungen für das WWW (Java-Applets) zu schreiben. Java Applets können in HTML-Seiten integriert, über das Internet angefordert und auf einer beliebigen Maschine ausgeführt werden, ohne daß der Entwickler die lokale Umgebung des Anwenders, wie Hardware und Betriebssystem, kennen muß. Somit können Programme mit vergleichbarer Funktionalität wie lokale Applikationen über das Internet auf den Rechner geladen werden.

JavaScript

JavaScript, eine Skriptspache, die sich in WWW-Seiten einbetten läßt

JavaScript ist eine von der Firma Netscape Communications entwikkelte Skriptsprache, die direkt in die HTML-Seiten eingebettet und über einen Interpreter interpretiert und ausgeführt wird. Die Motivation für die Entwicklung von JavaScript war die Unzulänglichkeit der vorhandenen Techniken (HTML, CGI) für Benutzerinteraktionen. Jede Interaktion (z.B.: Eingabe von Daten) mußte an den Server gesendet werden, um mit Hilfe eines CGI-Programmes Plausibilitätsprüfungen zu machen. Durch den Einsatz von JavaScript wurde die Anzahl der notwendigen Verbindungen zum Server drastisch verringert. Dynamisch zur Laufzeit können mit JavaScript beispielsweise Eingaben überprüft oder auch Berechnungen durchgeführt werden. Des weiteren lassen sich mit JavaScript wichtige Funktionen des Browsers, wie Öffnen und Schließen von Fenstern, Manipulieren von Formular-Elementen und das Anpassen von Browser Einstellungen verwirklichen.

ActiveX

ActiveX, Erweiterung der WWW-Seiten um multimediale Eigenschaften

ActiveX, eine Entwicklung der Fa. Microsoft, ist eine Kombination von verschiedenen Technologien, um die Interaktivität in Netzwerken zu erhöhen. WWW-Seiten können mit Hilfe der ActiveX-Technologie, um eine Vielzahl von multimedialen Effekten, unterschiedlichen Layouts und ausführbaren Applikationen, die über das Internet geladen werden, erweitert werden. Folgende ActiveX-Komponenten sind aus Nutzersicht relevant:

1. ActiveX-Controls, sind kleine ausführbare Programme (ähnlich wie die genannten Java Applets), die in WWW-Seiten eingebunden werden können,
2. ActiveX-Documents, ermöglichen die Anzeige von nicht HTML-Dokumenten wie Word oder Excel innerhalb des Browsers,
3. ActiveX-Scripting (VBScript und JScript), sind Sprachen, die in die WWW-Seite integriert werden und gewisse Interaktionsmöglichkeiten des Nutzers unterstützen (ähnlich wie das bereits angeführte JavaScript).

MIME (Multi-purpose Internet Mail Extension)

MIME, eine Spezifikation zur Übertragung von bel. Datenformaten über Email oder WWW

MIME ist ein Internet-Standard, der die Übertragung und Kennzeichnung von beliebigen Datenformaten (Text, Ton, Bild, Video, Programme usw.) mittels Email ermöglicht. Aus verschiedenen Datentypen zusammengesetzte Emails sind ebenfalls möglich. Im Kontext des WWW wird MIME im HTTP-Protokoll zur Spezifikation der übertragenen Daten verwendet.

Newsgroups

Newsgroups, Diskussionsgruppen für den Informations- und Meinungsaustausch

Usenet-Newsgroups sind elektronische Diskussionsgruppen, die den Informations- und Meinungsaustausch mit Menschen in aller Welt ermöglichen. Jede Gruppe (Newsgroup) enthält zahlreiche Artikel zu bestimmten Themen sowie viele Diskussionsbeiträge. Jeder kann sich an Diskussionen beteiligen oder auch neue Diskussionen initiieren. Durch die große Anzahl von existierenden Newsgroups, sind sie zur besseren Orientierung nach Titeln organisiert und gruppiert. Dazu werden zusammengesetzte Namen, wie z.B. "comp.lang.java", verwendet. Im Beispiel bezeichnet "comp" Computerthemen, "lang" die Untergruppe Sprachen (languages) usw. Newsgroups können auch für einen bestimmten Benutzerkreis reserviert werden.

3 Sicherheit bei der Nutzung von Email

Bei der Entwicklung des Internet-Email-Konzeptes stand in erster Linie die Robustheit und einfache Realisierbarkeit des Nachrichtentransports im Vordergrund. Die Standard-Email über das Internet ist vergleichbar mit einer Postkarte, deren Inhalt beispielsweise Mitarbeiter der Post lesen können. Erst durch die kommerzielle Nutzung der Email als Kommunikationsmedium bei Verwaltungen und Unternehmen gewann der Aspekt der Sicherheit immer mehr an Bedeutung.

3.1 Risiken

Die Verwendung von Email bringt verschiedene Risiken mit sich, die im folgenden näher erläutert werden:

- Erstellen von Kommunikationsprofilen des Absenders

  Für den Transport der Email sind Rechner, sogenannte „Mail Transfer Agents“ (MTA) zuständig, die eingehende Emails auswerten und entsprechend der Zieladresse an einen anderen MTA weiterleiten. In Internet kann somit eine Email über viele Stationen geleitet werden (Routing), bis sie den Empfänger erreicht. Standardmäßig protokollieren MTA’s für alle Email, die durchgeleitet werden, neben einer eindeutigen Identifikation die Absenderadresse, die Empfängeradresse, Datum und Uhrzeit. Diese Protokolle sind mindestens für den Systemadministrator des Systems zugänglich, bei manchen Systemen auch für normale Nutzer und werden einige Monate aufgehoben. Der Systemadministrator kann ohne weiteres diese Protokolle auch für längere Zeit archivieren und Kommunikationsprofile des Absenders erstellen und auswerten. Bei vielen Internet-Providern findet in der Regel aus Gründen der Entgeltberechnung eine Protokollierung aller versandten Email statt.

- Einsehen von privaten bzw. vertraulichen Nachrichten

  Die Systemadministratoren der MTA’s können neben der Protokollierung der Email-Daten auch die Speicherung der Email-Inhalte veranlassen. Je nach Konfiguration der MTA-Software können auch Archive für die Emails der letzten Monate erstellt werden. Somit können private und auch vertrauliche Emails durch Dritte eingesehen werden.

- Verändern und Verfälschen von Nachrichten möglich

  Der Systemadministrator der MTA’s ist jederzeit in der Lage, eingegangene bzw. weiterzuleitende Emails zu verändern und zu verfälschen. Weiterhin ist auch normalen Nutzern über das

Ändern der Absenderdaten möglich, unter falschem Absender Emails zu verschicken. Dies kann unter Umständen dem Absender erheblichen Schaden zufügen, falls beispielsweise wichtige Erkenntnisse oder auch Entscheidungen über Email mitgeteilt werden.

- Transfer von Viren und gefährlichen Programmen in das System

  Die Möglichkeit, beliebige Dokumente bzw. Dateien an eine Email zu hängen ist eine komfortable Möglichkeit des Dateitransfers. Jedoch bringt sie erhebliche Gefahren mit sich. An eine Email angehängte Winword- bzw. Excel-Dokumente können Makro-Viren enthalten. Beim Anklicken dieser Dokumente innerhalb der Email-Applikation (z.B. Netscape Mail) führt das automatisch zum Start der entsprechenden Applikation, wobei die enthaltenen Makros ausgeführt werden, die daraufhin das System infizieren. Dies kann dazu führen, daß Applikationen wie die Textverarbeitung funktionsunfähig werden, die Festplatte gelöscht wird oder sich der Virus über Email weiterverbreitet (siehe auch Kapitel 5).

- Systemüberlastung durch riesige Emails

  Um ein System zu sabotieren, werden riesige Emails, die bedeutungslose Texte enthalten, verschickt. Durch die begrenzten Ressourcen, die Mailbox-Programmen zur Verfügung stehen, führen enorm große Emails zu einem Überlauf und eventuellen Absturz, was den Ausfall der Email-Dienste mit sich bringt. Dies wiederum führt unweigerlich zur Störung der betrieblichen Datenverarbeitung.

- Belästigung der Nutzer mit Werbe-Emails

  Inzwischen wird im Internet auch unaufgefordert Werbung in Form von Email verschickt, deren Empfängeradressen entweder willkürlich über Email-Adreßsammlungen bestimmt oder gezielt durch Veröffentlichungen oder Teilnahme an Diskussionsforen usw. ausgesucht werden. Der Empfänger muß für die Trennung der für ihn essentiellen Emails von den Werbe-Emails Zeit aufwenden. Das verärgert und kann in größeren Unternehmen eine Minderung der Produktivität bedeuten.

- Verlust der Email bei der Übertragung

  Der Email-Versandmechanismus (vergleichbar mit der Zustellung einer Postkarte) garantiert keine hundertprozentige Zustellung der Email, da der Absender keinen Nachweis über die Zustellung bekommt. Es ist durchaus möglich, daß ein Systemadministrator eines MTA vorsätzlich den Weitertransport einer Email beispielsweise durch Löschen unterdrückt oder aufgrund von technischen Mängeln während der Übertragung eine Email verloren geht. Dieses Problem ist besonders bei der Abwicklung von wichtigen Interaktionen über Email zu berücksichtigen,

da beispielsweise termingebundene Abwicklungen in Verzug geraten können.

3.2 Schutzmöglichkeiten

Mit zusätzlichen technischen Hilfsmitteln kann die Sicherheit bei der Nutzung von Email erhöht werden. Besonders die Kryptografie spielt in diesem Zusammenhang eine große Rolle. Im folgenden werden Mechanismen, die die Sicherheit bei Email erhöhen, vorgestellt:

- Einsatz von PEM und PGP zur Verschlüsselung

  PEM (Privacy Enhanced Mail) und PGP (Pretty Good Privacy) sind Verfahren, die das Verschlüsseln bzw. Signieren von Nachrichten zulassen. Beide Verfahren setzen auf dem mächtigen Verschlüsselungsalgorithmus RSA[1] auf, der auf einem Zwei-Schlüssel-Prinzip (public key) basiert. Bei diesem Verfahren besitzt jeder Nutzer zwei verschiedene Schlüssel: einen geheimen Schlüssel, der nur ihm bekannt ist und einen öffentlichen Schlüssel, der anderen Teilnehmern im Netz zugänglich gemacht werden muß. Hierzu sind entsprechende Schlüsselverwaltungs-Instanzen[2], sogenannte Key-Server, notwendig, die die Verteilung der öffentlichen Schlüssel an andere Internet-Teilnehmer übernehmen. Die notwendigen Schlüssel kann der Nutzer selbständig mit Hilfe der Programme generieren.

  Will ein Nutzer A an einen Nutzer B eine verschlüsselte Nachricht schicken, so verschlüsselt A diese Nachricht mit dem öffentlichen Schlüssel von B. Nur B kann die empfangene Nachricht mit seinem geheimen Schlüssel, den nur er kennt, entschlüsseln. Hiermit ist gewährleistet, daß auch nur der Nutzer B die Nachricht lesen kann. Um auch die Authentizität, damit ist die sichere Identifikation des Nutzers A gemeint, sicherzustellen, ist eine Signierung der Nachricht durch Nutzer A erforderlich. Hierzu verschlüsselt der Nutzer A eine durch sogenanntes Hashing gebildete Quersumme der Nachricht mit seinem geheimen Schlüssel und schickt diese mit. Der Nutzer B kann diese Quersumme mit dem öffentlichen Schlüssel des Nutzers A entschlüsseln. Gleichzeitig kann Nutzer B durch Hashing eine Quersumme der von ihm bereits entschlüsselten Nachricht bilden und kann die beiden Quersummen vergleichen. Bei Übereinstimmung der beiden Quersummen ist die Nachricht unverändert und der Absender ist wirklich der Besitzer des öffentlichen Schlüssels.

[1] siehe http://www.rsa.com

[2] für Infos Email (*Subject: HELP)* an pgp-public-keys@informatik.uni-hamburg.de

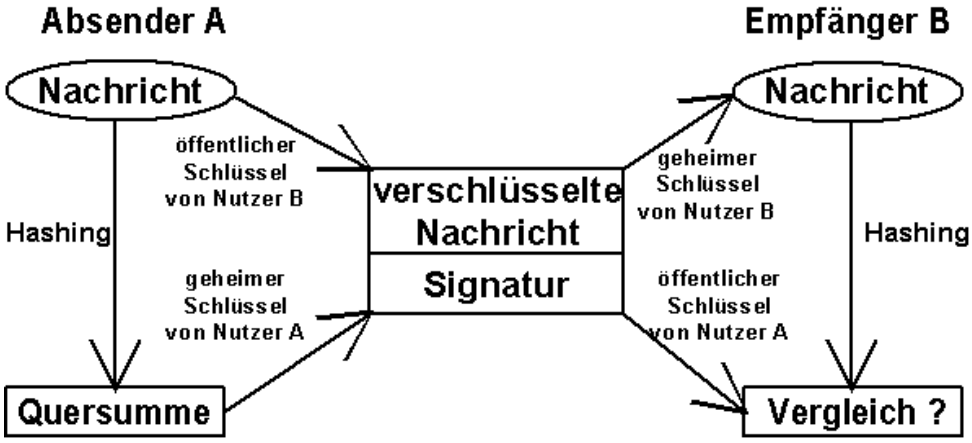

Abbildung 4: Public-Key-Verfahren

PGP und PEM sind sehr wirkungsvolle Methoden gegen Einsehen, Verändern oder Verfälschen von Email-Inhalten. Inzwischen sind internationale Varianten der PGP-Programme verfügbar, die auf europäische[3] Krypto-Algorithmen aufsetzen und somit nicht unter die amerikanischen Export-beschränkungen fallen. Dadurch können frei wählbare Schlüssel mit beliebiger Länge zur Verschlüsselung gewählt werden, womit eine extrem hohe Sicherheit erreicht werden kann. Für private Nutzung können diese Programme von diversen Servern[4] kostenlos heruntergladen werden. Jedoch sind PEM und PGP für einen generellen Einsatz im Internet zu kompliziert, da derzeit nur eine unzureichende und unter Umständen fehlerbehaftete Einbindung in gängige Email-Applikationen[5] existiert.

- Einsatz von S/MIME zur Verschlüsselung

  S/MIME (Secure Mutipurpose Internet Mail Extension) ist eine Erweiterung des MIME-Standards (siehe Kapitel 5), um einen sicheren Email-Versand zu ermöglichen. Die S/MIME-Verschlüsselung basiert ebenfalls auf dem RSA-Verschlüsselungsalgorithmus. S/MIME bietet zusätzlich zur Wahrung der Vertraulichkeit und Integrität der Email (durch Verwendung von Verrschlüsselungsalgorithmen) einen Authentifizierungsmechanismus, der auf Zertifikate nach dem X.509-Standard basiert. Da S/MIME auf dem MIME-Standard aufsetzt, ist die Integration in gängige Email-Applikationen[6] im Gegensatz zu PGP bzw. PEM einfacher. Bereits der Messenger

[3] Die internationale Version des PGP basiert auf den Krypto-Algorithmen der Schweizer Firma Ascom Systec AG (http://www.ascom.ch/systec/).

[4] z.B. http://www.ifi.uio.no/pgp/download.shtml

[5] Die Seite http://www.ifi.uio.no/pgp/winutils.shtml enthält Informationen über Frontends und Windows-Applikationen, die PGP unterstützen.

[6] z.B. http://www.connectsoft.com; http://www.deming.com; http://www.opensoft.com, http://www.netscape.com u.s.w.

(Email-Applikation) des Netscape Communicators unterstützt S/MIME.

Um eine verschlüsselte Email mit S/MIME zu verschicken, muß der Nutzer über ein Zertifikat eines Trustcenters[7] verfügen. Dieses Zertifikat garantiert die Echtheit des öffentlichen Schlüssels des Nutzers. Die Trustcenter bieten verschiedene Arten von Zertifikaten an, die meist in Klassen unterteilt sind. Diese unterscheiden sich meist in der Art der Überprüfung der Identität des Antragstellers und somit in der Vielfältigkeit des Einsatzes. Beispielsweise sind Zertifikate (Klasse 1 bei Verisign), bei denen die Identifizierung des Nutzers über Email stattgefunden hat, nur zur Nutzung von S/MIME gedacht. Während Zertifikate, bei denen die Identität des Nutzers über Ausweispapiere oder ähnliches geschieht, auch für Transaktionen, die eine Identifizierung des Nutzers erfordern, verwendet werden können.

Verisign[8], ein Trustcenter in Amerika, bietet kostenlos für einen Zeitraum von sechs Monaten ein Zertifikat für Testzwecke an. Dazu schickt Verisign dem Nutzer nach Eingabe seiner Daten eine Email, die eine Kennung enthält, mit der das Zertifikat von einem Verisign-Server heruntergeladen werden kann. Das heruntergeladene Zertifikat wird automatisch in die Email-Umgebung (Messenger) eingefügt und kann verwendet werden. Um nun anderen Nutzern verschlüsselte Email zu senden, ist der gegenseitige Austausch der öffentlichen Schlüssel notwendig. Hierzu ist das einmalige Verschicken einer signierten Email notwendig. Über diese signierte Email kann der Empfänger den öffentlichen Schlüssel des Absenders in die Schlüsselverwaltung der Email-Applikation übernehmen und damit verschlüsselte Email an den Besitzer dieses öffentlichen Schlüssels schicken.

Durch die einfache Integration in gängige Email-Applikationen stellt S/MIME eine Alternative gegenüber PEM und PGP dar. Jedoch ist die Ausfuhr von Algorithmen, die frei bestimmbare Schlüssel mit einer Länge über 40 Bit enthalten, durch die amerikanischen Exportbeschränkungen nicht zugelassen. Durch die immer größere Performanz von Computersystemen stellen 40 Bit lange Schlüssel keine ausreichende Sicherheit dar. Inzwischen gibt es Bestrebungen der amerikanischen Regierung alle verschlüsselten Dokumente und Kommunikationen um Informationen zur Schlüsselwieder-herstellung (key recovery block) zu erweitern. Hierzu soll der zur Entschlüsselung der Dokumente notwendige Schlüssel mit einem öffentlichen Schlüssel einer durch die Regierung kontrollierten Instanz verschlüsselt

[7] Die Seite https://certs.netscape.com/client.html bietet eine Zusammenstellung verschiedener Trustcenter an.

[8] Siehe http://digitalid.verisign.com/enroll.html

und an die Dokumente angehängt werden. Somit wäre die Regierung immer in der Lage, mit ihrem geheimen Schlüssel den sog. key-recovery-block und somit das eigentliche Dokument zu entschlüsseln.

Durch die Exportbeschränkungen und Bestrebungen der amerikanischen Regierung, die Verschlüsselung zu kontrollieren, ist kein hundertprozentiger Schutz mit S/MIME möglich. Jedoch können die für S/MIME verwendeten Krypto-Algorithmen nutzerseitig durch deutsche Algorithmen, die längere Schlüssel unterstützen, ausgetauscht werden, um eine maximale Sicherheit zu erreichen. Bisher sind jedoch keine deutschen Algorithmen vorhanden, die für S/MIME eingesetzt werden können.

- Verwendung von Anonymous Remailern

  Um die Erstellung von Kommunikationsprofilen teilweise zu verhindern bzw. um anonyme Emails verschicken zu können, können Rechner im Internet, sogenannte Anonymous Remailer, verwendet werden. Die Anonymous Remailer anonymisieren die Absenderadresse der eingehenden Email, durch Zuordnen einer eindeutigen neuen Absenderadresse (z.B. an12345@anon.penet.fi) und leiten diese an den Empfänger weiter. Dabei wird die Zuordnung zwischen der Absenderadresse und der generierten anonymen Adresse gespeichert, so daß der Empfänger an die anonymisierte Absenderadresse antworten kann. Mit dieser Technik ist zumindest gewährleistet, daß alle Stationen (MTA's), die zwischen dem Remailer und dem Empfänger an der Weiterleitung der Email beteiligt sind, sowie der Empfänger selbst, nicht erkennen, wer der Absender ist. Jedoch ist die Email auf dem Weg zum Remailer selbst nicht anonymisiert, womit alle an der Weiterleitung zum Remailer beteiligten MTA's potentielle Angreifer sein können. Dieser Nachteil wird bei Verwendung von Servern[9] im WWW, die das Eingeben und Verschicken von Emails über Formularfelder anbieten, umgangen. Die Voraussetzung ist natürlich ein vertrauenswürdiger Server, der bei Nutzung seiner Dienste keine Informationen über den Nutzer sowie dessen Email protokolliert. Nachteilig ist jedoch, daß die Empfänger der Email keine Möglichkeit haben, auf diese Email zu antworten.

  Die Verwendung von Anonymous Remailern ist sinnvoll, wenn die Anonymität des Absenders, beispielsweise bei der Teilnahme an umstrittenen Diskussionsforen oder Umfragen über Email, eine große Rolle spielt. Leider wurden diese Dienste für Straftaten (z.B. Drohbriefe, Belästigungen usw.) mißbraucht, wodurch viele der frei nutzbaren Remailer deaktiviert wurden.

[9] z.B. http://www.shinshin.com/ PREMAIL/premail.html

Jedoch stehen immer mehr private Remailer[10], die eine Benutzerkennung erfordern, zur Verfügung.

- Einsatz von Anti-Viren-Programmen

  Um die Infizierung von Computersystemen mit Viren zu verhindern, werden in vielen Institutionen gängige Anti-Viren-Programme (Anti-Viren-Kit der Firma Dr. Solomons[11] im LVN) eingesetzt. Diese Programme laufen meist als residente Programme im Hintergrund und überprüfen bereits vor dem Start von ausführbaren Programmen bzw. beim Zugriff auf Disketten auf möglichen Befall mit Viren.

  Microsoft hat inzwischen in die Office-Arbeitsumgebungen (Office 97) einen Dialog integriert, womit der Nutzer beim Öffnen von Dokumenten, die Ausführung von enthaltenen Makros explizit bestätigen muß. Somit hat der Nutzer die Möglichkeit, verdächtige Dokumente zuvor nach Viren zu durchsuchen oder das Dokument ohne Makros zu öffnen.

  Eine komfortable Möglichkeit, Viren über Email abzufangen, bietet das Produkt MailGuard[12] der Firma Dr. Solomon, das auf dem MIMEsweeper-Produkt der Firma Integralis[13] aufsetzt. MailGuard kann in beliebigen Email-Servern und Plattformen (wie NT, Unix und OS2) die eingehenden und abgehenden Emails nach Viren durchsuchen. Infizierte Emails werden in einem speziellen Ordner in Quarantäne gestellt und der Systemadministrator wird benachrichtigt, der die Datei desinfizieren, reparieren und anschließend an den endgültigen Empfänger weiterleiten kann. MailGuard unterstützt zudem alle gängigen Email-Formate und Dekomprimierungsverfahren, wodurch auch komprimierte Dateien, die an Emails angehängt sind, nach Viren durchsucht werden. Mit Hilfe von MailGuard wird verhindert, daß Mitarbeiter an externe Personen bzw. Unternehmen Viren weitergeben oder auch Viren in das eigene Computersystem einschleusen.

Folgende Tabelle stellt die Risiken und entsprechende Schutzmöglichkeiten bei der Verwendung von Email gegenüber:

[10] z.B. http://interlink-bbs.com/anonremailer.html

[11] siehe http://www.drsolomon.com

[12] siehe http://www.drsolomon.com/products/mailguard/index.cfm

[13] siehe http://www.mimesweeper.integralis.com/

Risiken durch Email	Schutzmöglichkeit
Erstellen von Kommunikationsprofilen des Absenders	Verwendung von Anonymous Remailer
Einsehen von privaten bzw. vertraulichen Nachrichten	Verwendung von Kryptografie
Verändern und Verfälschen von Nachrichten	Verwendung von Kryptografie
Transfer von Viren und gefährlichen Programmen in das System	Verwendung von Anti-Viren-Programmen und Produkten wie MailGuard
Systemüberlastung durch riesige Emails	Mail-Server Konfiguration
Belästigung der Nutzer mit Werbe-Emails	keine Schutzmöglichkeit
Verlust der Email bei der Übertragung	keine Schutzmöglichkeit

3.3 Empfehlungen

Folgende Richtlinien sollten im Hinblick auf den Einsatz von Email berücksichtigt werden, um eine maximale Sicherheit zu erreichen:

- Innerhalb einer Organisation sollten klare Regeln (Email-Policy) in Bezug auf Verwendung von Email definiert werden.
- Bei der Übertragung von sensiblen bzw. vertraulichen Informationen im Internet über Email sollten auf jeden Fall Krypto-Verfahren wie PEM bzw. PGP eingesetzt werden. In Intranets ist dies nicht notwendig, wenn die Vertraulichkeit durch andere betriebliche Maßnahmen sichergestellt ist.
- Bei Teilnahme an Diskussionsforen oder Umfragen per Email sollten Anonymous Remailer eingesetzt werden, wenn durch die volle Namensnennung die Privatsphäre gefährdet würde.
- Anti-Viren-Programme müssen nach Identifizierung neuartiger Viren bzw. nach Bedarf aktualisiert werden.
- Produkte (MailGuard) zum Durchsuchen von ein- und abgehenden Emails nach Viren sollten eingesetzt werden.
- Bei Verwendung der älteren Version des Microsoft Office-Paketes (bis Version 7) sollte der Mime-Type application/msword bzw. x-msword entfernt werden, um ein automatisches Starten der Applikation und somit den Start von vorhandenen Makros zu verhindern (siehe Kapitel 5).
- Der Austausch von Dokumenten in Formaten, die Makros unterstützen, sollte vermieden werden. Statt dessen können Formate wie RTF oder HTML verwendet werden.

- Falls empfangene Word-Dokumente nicht bearbeitet, sondern nur betrachtet werden sollen, kann das Programm „Wordview“ verwendet werden, das die Ausführung von Makros nicht unterstützt.
- Um einem Verlust von Daten durch Virenbefall vorzubeugen, muß ein schlüssiges Backup-Konzept entwickelt und umgesetzt werden.
- Nutzer müssen im Hinblick auf Sicherheitsmängel bei Verwendung von Email geschult werden.
- siehe auch Kapitel 5.3, Empfehlungen (MIME-Types)

4 Sicherheit beim File-Transfer

Über File-Transfer (FTP) können beliebige Programme bzw. Dokumente, die auf einem Server bereitgestellt werden, heruntergeladen werden. Diese heruntergeladenen Programme bzw. Dokumente können mit Viren infiziert sein oder gefährliche Aktionen auf dem Rechner ausführen und somit die Sicherheit des Computersystems gefährden.

4.1 Risiken

Der File-Transfer bringt verschiedene Risiken mit sich, die im folgenden näher erläutert werden:

- Transfer von Viren und gefährlichen Programmen in das System

  Beim File-Transfer von beliebigen Servern können Programme bzw. Dokumente heruntergeladen werden, die Viren enthalten bzw. installieren. Beispielsweise werden im Internet ausführbare Dateien unter dem Namen eines gängigen Programmes verbreitet, die beim Starten entweder Systemressourcen beschädigen bzw Viren installieren oder das System bzw. den Nutzer ausforschen und Informationen an Dritte weitergeben.

4.2 Schutzmöglichkeiten

Um die Sicherheit beim File-Transfer zu erhöhen, können verschiedene Mechanismen, die im folgenden erläutert werden, eingesetzt werden:

- Verhindern von File-Transfer

  Der restriktivste Schutz wird durch das Verhindern des File-Transfer-Dienstes erreicht. In einem Intranet kann der File-Transfer durchaus zugelassen werden, wenn sichere Dokumente bzw. Dateien übertragen werden. File-Transfer vom Internet kann beispielsweise über spezielle Rechner gestattet werden, die vom Intranet abgeschottet sind und als Testplattform für heruntergeladene Programme bzw. Dokumente dienen.

- Einsatz von Anti-Viren-Programmen

  Mit dem Einsatz von Anti-Viren-Programmen kann die Gefahr der Infizierung des Rechners mit Viren durch heruntergeladene Programme bzw. Dokumente, minimiert werden. Hierzu existieren verschiedene Programme, die meist im Hintergrund laufen und vor dem Starten von ausführbaren Dateien bzw. Öffnen von Dokumenten einen Viren-Check durchführen (siehe Schutzmöglichkeiten bei Email).

Durch die Integration des File-Transfer-Dienstes in die WWW-Umgebung, existieren bereits Anti-Viren-Plugins[14], die die Funktionalität des Browsers zur Erkennung und Bekämpfung von Viren erweitern. Hierbei durchsucht der Browser vor dem Speichern bzw. Verarbeiten, heruntergeladene Programme bzw. Dokumente nach Viren und bricht gegebenenfalls mit einer Warnung ab.

Die Viren-Programme können jedoch keinen hundertprozentigen Schutz gewährleisten, da nur nach bereits identifizierten Viren durchsucht werden kann. Somit werden neuartige Viren von Anti-Viren-Programmen nicht erkannt und können auf den Rechnern erheblichen Schaden anrichten.

4.3 Empfehlungen

Folgende Richtlinien sollten im Hinblick auf den Einsatz von File-Transfer berücksichtigt werden, um eine maximale Sicherheit zu erreichen:

- File-Transfer im Internet sollte in Institutionen nur für bestimmte Nutzergruppen zugelassen werden.
- File-Transfer sollte nur von vertrauenswürdigen Servern erfolgen.
- Generell sollten Anti-Viren-Programme auf den Rechnern installiert werden.
- Anti-Viren-Programme müssen regelmäßig und vor allem nach Identifikation neuartiger Viren aktualisiert werden.
- Ein schlüssiges Backup-Konzept muß entwickelt und umgesetzt werden.
- Nutzer müssen im Hinblick auf Sicherheitsrisiken durch File-Transfer geschult werden.

[14] siehe http://www.eliashim.com

5 Sicherheit bei der Nutzung von MIME-Types

Browser können standardmäßig nur das HTML-Format sowie GIF-, JPEG- und XBM-Grafikformate anzeigen. Um andere Datenformate zu verarbeiten werden externe Applikationen, sogenannte *helper applications*, verwendet. Der Netscape Navigator verfügt über eine Zuordnungsliste, in der die Datenformate den einzelnen externen Applikationen zugeordnet werden. Diese Zuordnung wird über den MIME-Type-Mechanismus realisiert. Diese Zuordnungsliste wird ebenfalls in der Netscape Mail-Applikation verwendet, um an Email angehängte Dateien bzw. Dokumente entsprechenden Applikationen zuordnen zu können.

WWW-Server versorgen alle Dateien, die sie zum Browser schicken mit einem entsprechenden MIME-Type (z.B. text/html für HTML-Seiten). Über diesen MIME-Type kann der Browser entscheiden, ob das übertragene Datenformat im Browser selbst angezeigt werden kann oder ob eine externe Applikation zur Anzeige notwendig bzw. eingerichtet ist. Bei WWW-Servern, die keine MIME-Type's mitschikken, interpretiert der Browser zur Identifizierung des Datenformats die Dateierweiterung (z.B. *.doc*). Beim Empfang eines Datenformats, für den eine externe Applikation vorgesehen ist, wird diese automatisch durch den Browser mit den entsprechenden Daten gestartet.

Mime-Types stellen eine komfortable Möglichkeit dar, um eine automatisierte Anzeige bzw. Verarbeitung von beliebigen Datenformaten über den Browser zu ermöglichen. Jedoch sind damit enorme Sicherheitsrisiken verbunden, da über unsachgemäß eingestellte MIME-Types beliebiger Programm-Code auf dem Rechner gestartet werden kann.

5.1 Risiken

Die unsachgemäße Verwendung von MIME-Types bringt verschiedene Risiken mit sich, die im folgenden näher erläutert werden sollen:

- Automatische Ausführung von ausführbaren Dateien, Skripten und Makros:

  MIME-Types, die für ausführbare Programme, Skripten usw. definiert sind, ermöglichen die automatische Ausführung dieser Programme auf dem Client-Rechner. Beispielsweise können auf einem WWW-Server ausführbare Programme (.exe), Batch-Dateien (.bat) oder Skripte (.pl) abgelegt werden, die zwar den Anschein eines ungefährlichen Programmes erwekken (z.B. Softwareupdate), in Wirklichkeit jedoch einen Virus in-

stallieren, Festplatten zerstören oder auch Nutzer ausforschen können.

- Belästigen des Nutzers durch Abspielen von Musikstücken:

  In der Standardinstallation verfügen die Browser über MIME-Types für das Erkennen von Audio-Daten. Somit wird das automatische Abspielen von Musikstücken ermöglicht. Diese Möglichkeit kann mißbräuchlich ausgenutzt werden, etwa um beim Betreten einer WWW-Seite nervende bzw. obszöne Musikstücke abzuspielen.

Folgende Tabelle stellt die Standard-MIME-Types mit deren möglichen Sicherheitsrisiken dar:

MIME-Type	**Dateiendung**	**Sicherheitsrisiko**
application/octet-stream application/octet-string application/x-msdownload	exe, bin, sys exe, bin, sys exe, bin, sys	Ausführung von bel. Code auf dem Rechner (Viren, Ausforschung usw.)
application/zip application/x-gzip application/x-compress application/x-gtar application/x-tar	zip gz Z gtar tar	Archiv kann Viren oder gefährliche ausführbare Programme enthalten, wobei die Gefahr nicht beim Öffnen des Archivs besteht, sondern beim Start eines darin enthaltenen Programms oder Dokuments.
application/x-perl application/x-tcl application/x-sh application/x-csh	pl tcl sh csh	Ausführen von bel. Code auf dem Rechner
application/msword application/msexcel	doc, dot xls	Dokument kann Makroviren enthalten
application/postscript	ps	Dokument kann Code enthalten, das in älteren Postscript-Viewern ausgeführt wird, oder durch entsprechende Steuerkommandos können Paßworte im Drucker aktiviert werden, was die weitere Nutzung behindert
application/x-wav	wav	Ungewollte Musikstücke können auf dem Client-Rechner abgespielt werden

5.2 Schutzmöglichkeiten

Um die Sicherheit bei Verwendung von MIME-Types zu erhöhen, können folgende Mechanismen, die nachstehend erläutert werden, eingesetzt werden:

- Einschränken der MIME-Types

  Der restriktivste Methode, die aber gleichzeitig eine maximale Sicherheit bietet, wird durch das Entfernen aller MIME-Types, die eine Ausführung von Code bzw. Skripts bewirken, erreicht. In diesem Fall fragt der Browser beim Empfang eines Datenformates, für das kein MIME-Type definiert ist, den Nutzer, der dann entscheiden kann ob die Datei gespeichert bzw. verworfen wird oder ob eine entsprechende Applikation gestartet werden soll.

- Einsatz von Anti-Viren-Plugins für Browser

  Über Anti-Viren-Plugins[15] wird die Funktionalität des Browsers zur Erkennung und Bekämpfung von Viren erweitert. Hierbei durchsucht der Browser vor dem Speichern bzw. Verarbeiten heruntergeladene Programme bzw. Dokumente nach Viren und bricht gegebenenfalls mit einer Warnung ab.

5.3 Empfehlungen

Folgende Richtlinien sollten im Hinblick auf den Einsatz von MIME-Types berücksichtigt werden, um eine maximale Sicherheit zu erreichen:

- Nur unbedingt erforderliche MIME-Types sollte man im Browser einrichten.
- Bei Institutionen sollte nur ein vorgegebener Satz von MIME-Types zugelassen werden.
- Anti-Viren-Plugins sollten installiert werden.
- Verschiedene Bürokommunikationsprogramme, u.a. auch Microsoft Office, lassen sich in einem Modus aufrufen, in dem keine Makros beim Öffnen eines Dokumentes ausgeführt werden oder die Makrounterstützung ganz deaktiviert wird. Dieser Modus sollte bei fremden Dokumenten gewählt werden (siehe Beschreibung der jeweiligen Programmpakete).
- Nutzer müssen im Hinblick auf Sicherheitsrisiken bei Verwendung von MIME-Types geschult werden.

[15] siehe http://www.eliashim.com

6 Sicherheit bei Standard-WWW-Techniken

Bereits das „Surfen“ im WWW, in dem beliebige Informationen für alle (ohne Jugendschutz) zugänglich sind, sowie die Abwicklung von Geschäften im Internet, wobei vertrauliche Informationen (Paßwörter, Kreditkartennummern usw.) übertragen werden müssen, bringt Sicherheitsrisiken mit sich.

6.1 Risiken

Die Verwendung der Standard-WWW-Technologie bringt Sicherheitsrisiken mit sich, die im folgenden erläutert werden:

- Abfangen der gesendeten Informationen zum Server

  Viele Server, die nur einer gewissen Nutzergruppe den Zugang zu den angebotenen Seiten erlauben wollen, versehen diese Seiten mit einem Paßwortschutz. Wird eine geschützte Seite durch einen Browser abgerufen, so wird automatisch ein Browser-Dialog-Fenster geöffnet, der die Authentifizierung des Nutzers verlangt. Jedoch geschieht die Übertragung dieser Paßwörter sowie Daten aus jeglichen WWW-Formularen vom Browser zum WWW-Server im Klartext, womit ein Angreifer mit der entsprechenden Hard- und Software die Übertragung ohne größere Probleme abfangen kann. Das für das WWW genutzte Kommunikationsprotokoll (HTTP) bringt es mit sich, daß der WWW-Browser die Paßwörter jedesmal senden muß, wenn eine geschützte Seite angefordert wird. Hierdurch wird ein Abfangen der Informationen noch weiter erleichtert. Somit können etwaige Angreifer Informationen lesen, die nicht für sie bestimmt sind. Ein weiteres Problem ist, daß WWW-Dienste existieren, die es dem Nutzer erlauben, ihr Paßwort frei zu wählen. Häufig wählen die Nutzer hierfür dasselbe Paßwort wie auf dem heimischen Rechner. Böswillige Serverbetreiber könnten diese Informationen für etwaige Einbruchsversuche in Computersysteme nutzen.

- Erstellung von Profilen über Surf-Gewohnheiten des Nutzers

  Jeder Verbindungsaufbau mit einem WWW-Server hinterläßt durch die Protokollierungsmechanismen der einzelnen Server gewisse Informationen (z.B. IP-Adresse, Name und Betriebssystem des Computers, Art und Version des verwendeten Browsers, URL der aktuellen Seite), mit denen Profile über einzelne Nutzer erstellt werden können. Diese Profile sind aber meist nicht aussagekräftig, da sie sich nur auf einen Server beziehen. Jedoch könnten verschiedene Serverprotokolle zusammengefügt und über automatisierte Verfahren ausgewertet werden,

um ein Internet-übergreifendes Profil über Nutzer erstellen zu können. Bei der Anzahl der existierenden Server im Internet ist dies jedoch unrealistisch und nicht praktikabel.

- Jugendschutz

  Die Ämter sowie Organisationen sind durch die wachsende Flut von WWW-Servern und Seiten nicht in der Lage, die Rechtmäßigkeit der angebotenen Informationen zu kontrollieren. Dadurch wird besonders Jugendlichen der Zugang zu Informationen über Sex, Drogen, Rechtextremismus, Verherrlichung von Gewalt usw. ermöglicht. Des weiteren erleichtert das Internet verbotenen Organisationen, sich ungestört zu verständigen oder neue Mitglieder zu werben.

6.2 Schutzmöglichkeiten

Um die genannten Sicherheitsrisiken zu minimieren, können folgende Mechanismen eingesetzt werden:

- Aktivieren der Warnmeldungen des Browser

  Standardmäßig sind im Browser Warnmeldungen aktiviert, die den Benutzer auf eventuelle Sicherheitsrisiken bei der Übertragung von Formularinhalten (z.B. vertrauliche Informationen wie Kreditkartennummern) über das Internet hinweisen. Der Benutzer kann somit entscheiden, ob die Übertragung der Information unbedenklich ist oder ob er den Vorgang abbrechen möchte. Folgendermaßen können die Einstellungen in den Browsern angepaßt werden, um die Ausgabe von Warnmeldungen zu aktivieren:

	Netscape Navigator 3	**Netscape Communicator 4**	**Microsoft Internet Explorer 3**
Aktivieren der Selektionsbox	*Options / Security Preferences / General / Show an alert before/ Submitting a form insecurely*	*Communicator / Security Info / Navigator / Show a warning before / Sending unencrypted Info to a site*	*Ansicht / Optionen / Erweitert / Vor dem Senden über eine offene Verbindung warnen*

- Einsatz von Verschlüsselungsmethoden (SSL)

  SSL (Secure Socket Layer) ist ein Protokoll, das den Austausch von verschlüsselten Informationen über das Internet erlaubt. SSL ist zwischen der Transport- und Anwendungsebene integriert, womit sie für Applikationen transparent erscheint. Somit können bestehende Applikationen ohne große Modifikation auf eine sichere Übertragung zurückgreifen.

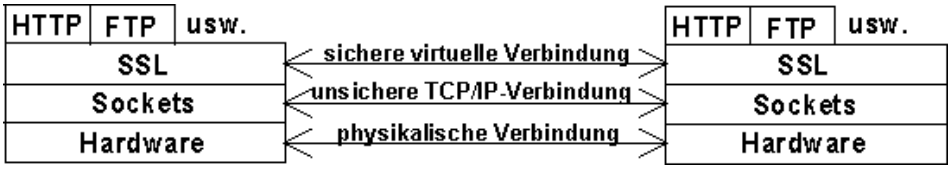

Abbildung 5: SSL-Aufbau

Bei Verwendung von SSL laufen vor der eigentlichen Datenübertragung folgende Interaktionen zwischen dem Client und dem Server ab:

In der sogenannten Hallo-Phase baut der Client eine Verbindung zum Server auf und teilt ihm mit, welche Kryptographie-Algorithmen er unterstützt. Der Server wählt daraus ein Public-Key/Private-Key- und ein Hash-Verfahren aus, die für folgende Verschlüsselungen verwendet werden. Gleichzeitig sendet der Server ein Zertifikat, das die Kennung des Servers und seinen öffentlichen Schlüssel enthält. Dies ist jedoch für die Identifikation des Servers nicht ausreichend, da das Zertifikat möglicherweise aus einer anderen Verbindung kopiert worden sein könnte. Der Client generiert daraufhin einen Sitzungsschlüssel (Session Key) für einen Datenaustausch mit dem Private-Key-Verfahren. Dieser wird nun mit dem öffentlichen Schlüssel des Servers verschlüsselt. Diesen chiffrierten Schlüssel schickt der Client an den Server, der mit seinem geheimen Schlüssel den Sitzungsschlüssel entschlüsseln kann. In der abschließenden Authentifizierungs-Phase authentifiziert der Client den Server, indem er ihm eine Reihe von mit dem Sitzungsschlüssel chiffrierten zufälligen Testnachrichten schickt. Der Server kann diese Testnachrichten nur dann korrekt dechiffrieren und bestätigen, wenn er im Besitz des geheimen Serverschlüssels ist und somit der >>echte<< Server ist. Optional kann der Server auf vergleichbare Weise den Client authentifizieren. Anschließend findet die Übertragung der eigentlichen Daten statt. Die Client-Authentifikation funktioniert jedoch nur dann, wenn der Client über ein offiziell registriertes Zertifikat von einem entsprechenden Trustcenter[16] verfügt. Derzeit existieren keine Trustcenter in Deutschland, die Zertifikate zur Client-Authentifikation vergeben. Somit müssen Nutzer Zertifikate von Trustcenter, die in anderen Ländern betrieben werden, beziehen. Für Intranet-Lösungen können eigene Trustcenter aufgebaut werden, um Zertifikate für den internen Gebrauch zur Verfügung zu stellen. Damit kann eine zuverlässige Authentifizierung der Nutzer innerhalb des Intranet realisiert werden.

SSL wird bereits in gängigen Browsern sowie Servern unterstützt und bietet damit eine sichere Übertragung von Informa-

[16] Die Seite https://certs.netscape.com/client.html bietet eine Zusammenstellung verschiedener Trustcenter an.

tionen über das Internet (bei Verwendung von beliebig langen Schlüsseln). Jedoch unterstützen die Exportversionen der Browser bzw. Server, durch die amerikanischen Exportbestimmungen, nur Schlüssellängen von 40 Bit (siehe Kapitel 3.2, S/MIME), während die Standard-Versionen (Browser, Server) 128 Bit Schlüssellängen unterstützen. Inzwischen bieten 40 Bit Schlüssel keinen ausreichenden Schutz mehr. Bereits Anfang 1997 gelang es unter Verwendung eines Netzwerks von Workstations einen 40 Bit Schlüssel in nur 3.5 Stunden zu knacken. Um diese Nachteile zu umgehen wurde außerhalb der USA eine unabhängige Implementation der SSL 3.0 Version, unter dem Namen SSLeay[17], entwickelt. SSLeay ist frei verfügbar und kann von vielen FTP-Servern heruntergeladen werden. Inzwischen ist SSLeay bereits in frei verfügbare WWW-Server (Apache, NCSA) sowie Clients (Mosaic) integriert, die somit eine absolut sichere Übertragung von Informationen über das Internet ermöglichen. Jedoch befinden sich die meisten angepaßten Applikationen in einer Testphase oder laufen nicht stabil. Damit ist ein professioneller Einsatz bisher nicht empfehlenswert.

- Verwendung von Anonymisierungsdiensten

  Die Erstellung von Profilen über die „Surfgewohnheiten“ von Nutzern kann durch Verwendung von Anonymisierungsdiensten[18] verhindert werden. Diese Dienste arbeiten als Vermittler zwischen dem Nutzer und der angeforderten Seite. Um eine beliebige Seite anonym zu empfangen, muß der Nutzer vor die URL die Adresse des Anonymisierungsdienstes stellen (z.B. http:// www.anonymizer.com:8040/*http://xxx.com/*). Der entsprechende Dienst fordert diese Seite an, ohne Daten über den Benutzer weiterzugeben, paßt existierende Verweise (Hyperlinks) innerhalb des Dokumentes an, entfernt alle Elemente, die keine Anonymität zulassen (Java, Javascript usw.) und gibt die endgültige Seite an den Nutzer weiter. Somit bieten die Anonymisierungsdienste eine gute Möglichkeit während des „Surfens“ im Internet anonym zu bleiben. Natürlich setzt dies voraus, daß die Daten des Nutzers weder protokolliert noch verarbeitet werden. Nachteilig ist die etwas längere Wartezeit, da die angeforderte Seite zuerst vom Anonymisierungsdienst empfangen, verarbeitet und weiter geschickt wird.

- Mechanismen für den Jugendschutz

  Um Jugendliche vor WWW-Seiten mit pornographischen, rechtsextremen, Gewalt verherrlichenden und anderen schädli-

[17] siehe http://remus.prakinf.tu-ilmenau.de/Reif/Publications/IX9606/urls.html für weitere Informationen

[18] siehe http://www.anonymizer.com/

chen Inhalten zu schützen, existieren Softwaremodule[19], die Seiten nach bestimmten Schlüsselwörtern durchsuchen, beurteilen und gegebenenfalls herausfiltern oder direkt über Listen, die verbotene Server enthalten, den Zugang zu Servern verhindern. Hierzu wurde auch der PICS- (Platform for Internet Content Selection) Standard entwickelt, der das Format festlegt, wie WWW-Seiten beurteilt werden können. Jedoch werden keine Bewertungsmerkmale für Inhalte (Sex, Drogen, Gewalt usw.) definiert. Somit können Seiten beliebig durch Anbieter oder durch andere Stellen oder Personen beurteilt und bewertet werden. Der Nutzer muß für sich entscheiden, welche Bewertungsmerkmale seinen Anforderungen gerecht werden. Beispielsweise können Eltern für ihre Kinder die Bewertungsmerkmale nach dem RSAC-System[20] (Gewalt, Nacktheit, Sex und Sprache) verwenden, oder eine andere Bewertung hernehmen, die möglicherweise noch restriktiver ist und mehr Bereiche umfaßt.

Der Internet Explorer ab der Version 3 verfügt über Mechanismen, mit denen nach dem RSAC-System beurteilte Inhalte nur für bestimmte Nutzer (Paßwort) zugelassen werden können. Jedoch stellt das keinen sicheren Schutz dar, wenn durch Installieren eines neuen bzw. anderen Browsers der Zugriff auf beliebige Seiten trotzdem möglich wird. Besser sind Systeme[21], die direkt auf den Netzwerk-Protokollen bzw. auf Proxy-Servern aufsetzen. Besonders für Unternehmen bieten sich diese Systeme an, da durch die Einschränkung auf bestimmte WWW-Seiten die private Nutzung bzw. Ablenkung der Mitarbeiter verhindert wird.

6.3 Empfehlungen

Folgende Richtlinien sollten im Hinblick auf den Einsatz von WWW-Technologie berücksichtigt werden, um eine maximale Sicherheit zu erreichen:

- Vertrauliche Informationen sollten nur zu einem mit SSL gesicherten Server übertragen werden.
- Die Verwendbarkeit von SSLeay muß für einzelne Fälle evaluiert werden.
- Mit Einsatz von Filterprogrammen sollten Zugriffsbeschränkungen auf WWW-Seiten realisiert werden.

[19] die Seite: *http://www.childwelfare.com/kids/webfilt.htm* enthält Informationen über diverse Jugendschutz-Softwarepakete.

[20] siehe http://www.rsac.org/; RSAC wird auch für die Bewertung von Video-Spielen verwendet.

[21] siehe http://www.webster.com/; http://www.mimesweeper.integralis.com/

- Mailing-Listen[22], die Sicherheitsaspekte im WWW behandeln, sollten abonniert werden.
- Es sollten jeweils die aktuellsten Browser verwendet werden, da erkannte Fehler sofort verbessert werden.
- Anonymisierungsdienste können verwendet werden, um die Erstellung von Nutzerprofilen über „Surfgewohnheiten“ zu vermeiden.
- Zugriffskennungen die für WWW-Server notwendig sind, sollten sich von Zugriffskennungen für den lokalen Rechner unterscheiden.
- Eltern müssen auf die Notwendigkeit, den Jugendschutz bei der Nutzung des Internet zu realisieren, hingewiesen werden.
- Vor dem „surfen“ im Internet sollten alle geöffneten Applikationen und Dokumente geschlossen und Arbeits-ergebnisse gesichert werden, um einem eventuellen Verlust zu vermeiden.
- Nutzer müssen im Hinblick auf Sicherheitsrisiken bei der Nutzung der WWW-Technologie geschult werden.

[22] z.B. http://www-ns.rutgers.edu/www-security/www-security-list.html beschreibt eine Mailing-Liste, die alle Aspekte der Sicherheit im WWW abdeckt.

7 Sicherheit bei der Nutzung von Java

Java ist eine objektorientierte Programmiersprache, die bei Sun Microsystems entwickelt wurde. Java wurde für verteilte Systeme entwickelt und verfügt über ein integriertes Sicherheitskonzept. Das Sicherheitskonzept wird anhand der Metapher Sandkastenprinzip (engl. „sandbox“) beschrieben. Die Idee hierbei ist, den Java-Code in einer Umgebung mit klar definierten Grenzen (entsprechend im Sandkasten: der Sand wird durch einen Kasten zusammengehalten), ablaufen zu lassen. Der Sandkastenmechanismus beinhaltet eine Vielzahl von kooperierenden Systemkomponenten, wie den Security-Manager, der als Teil der Applikation läuft, sowie in der Java-Virtual-Machine eingebundene Sicherheitsmechanismen (Klassenlader, Byte-Code-Verifizierer) und schließlich die Sprache selbst. Der Sandkasten stellt sicher, daß möglicherweise bösartige Anwendungen, die über das Netz geladen werden, keinen Zugriff auf Systemressourcen erlangen. Lokal geladene Anwendungen hingegen unterliegen keinen Zugriffsbeschränkungen.

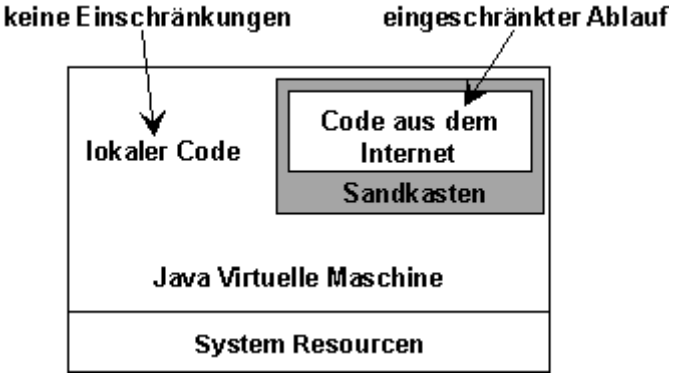

Abbildung 6: Java Sandkastenmodell

Die Sprache Java bietet schon mit ihrem Speicherverwaltungsmodell eine Sicherheitsbarriere. Die Speicherbelegung geschieht erst beim Ablauf des Programms, während eine separat laufende Komponente (garbage collection) die Speicherbereinigung übernimmt. Des weiteren wird in Java keine Zeigerarithmetik zugelassen, womit der Zugriff auf unerlaubte Speicherbereiche verhindert wird. Die Einhaltung der Sicherheitsregeln werden vom Java-Compiler überprüft.

Wird eine HTML-Seite mit einem eingebetteten Applet aufgerufen, so ruft der Browser den Applet-Klassenlader auf, der Bestandteil der Java Ablaufumgebung ist. Der Klassenlader holt den Code des Applets vom entsprechenden Server und stellt für dieses Applet einen eigenen Adressraum zur Verfügung, in dem es kontrolliert ablaufen kann. Um sicherzustellen, daß der Byte-Code nicht durch einen manipulierten Compiler erzeugt worden ist, wird der Byte-Code durch einen Byte-Code-Verifizierer einer Reihe von Tests unterzogen. So-

mit findet vor der Ausführung von jeglichem Byte-Code eine strenge Prüfung auf Einhaltung der Spezifikationen der Java Sprache statt. Während der Ausführung des Applet-Codes ist der Security-Manager aktiv, der den Aufruf von gefährlichen Funktionen, wie File I/O, Netzwerkzugriffe und beispielsweise die Instantiierung eines eigenen Klassenladers, überprüft und gegebenenfalls unterbindet. Der Security-Manager sorgt für die Einhaltung des Sandkastenkonzeptes.

Des weiteren bietet Java ein Werkzeug an, das die Kennzeichnung von Dateien ermöglicht, die sogenannte Java Archives (Abkürzung: JAR) enthalten. JAR-Dateien können neben Java-Code unter anderem auch Audio- und Video-Daten enthalten. Der Anbieter kann diese Archive durch eine digitale Signatur kennzeichnen. Der Browser kann diese Signatur verifizieren und entsprechend den Code in einer mehr oder weniger abgesicherten Umgebung ablaufen lassen. Außerdem kann auch ein Applet den Nutzer über dessen Signatur identifizieren und entscheiden, ob die Ausführung verweigert wird oder ob eine Freigabe aller Systemressourcen des Servers stattfindet. Um den Einsatz von Signaturen zu vereinfachen, sollen auch Signaturen von Fremdanbietern unterstützt und Online-Registrierungen bzw. Genehmigungen ermöglicht werden.

Zusätzlich stellt Java Klassenbibliotheken zur Verfügung, mit denen die gesicherte Übermittlung von Nachrichten (message digest), Schlüsselverwaltung, Zertifikatsverwaltung und Zugriffskontrollmechanismen erleichtert wird.

Die strengen Sicherheitsaspekte engen natürlich die Funktionalität und Möglichkeiten von Applets ein. Deshalb sollen in Zukunft Mechanismen integriert werden, mit denen der Anwender fein justierbare Zugriffsmechanismen sowie konfigurierbare Sicherheitspolicen definieren kann. Somit kann beispielsweise der Benutzer Konfigurationen aufstellen, womit Applets vom Server A Lesezugriffe auf den Client und Applets vom Server B Schreib- und Lesezugriffe erlaubt werden. Diese Möglichkeit läßt sich auf alle Systemressourcen, wie Dateisystem, Geräte, Ports usw., anwenden. Die Verwaltung der Zugriffskontrollisten findet in einer Art Datenbank statt.

Sicherheitsaspekte bei Applets

Durch die Tatsache, daß Java Applets über das Netz auf den lokalen Rechner geladen und dort ausgeführt werden, wurden strenge Regeln für die Ausführung festgesetzt.

Generell unterliegen Applets, die über das Netz geladen werden, folgenden Einschränkungen:

- kein Lesen und Schreiben von Dateien auf dem Client möglich,
- keine Netzwerkverbindung zu anderen Rechnern möglich, außer zu dem Rechner, von dem das Applet stammt,
- kein Starten von fremden Programmen auf dem Client möglich,
- kein Laden von zusätzlichen Bibliotheken möglich,

- kein Aufruf von Systemfunktionen möglich,
- besondere Kennzeichnung der Fenster, die durch Applets gestartet werden.

Applets können neun definierte Systemeigenschaften lesen:

- Java Versionsnummer (z.B.: 1.02),
- Java herstellerspezifische Bezeichnung (z.B.: Netscape Communications Corporation),
- URL-Adresse des Java Herstellers (z.B.: http://home.netscape.com),
- Versionsnummer der Java-Klassen-Bibliothek (z.B.: 45.3),
- Betriebssystemname (z.B.: NT),
- Systemarchitektur (z.B.: Pentium),
- Code für das Dateitrennzeichen (z.B.: „/“),
- Code für das Pfadtrennzeichen (z,B.: „;“),
- Code für das Zeilentrennzeichen (z.B.: „\n“).

Diese Einschränkungen stellen den Standardfall dar. Falls der Anwender über Einstellungen, die in den neuen Browserversionen unterstützt werden sollen, die Sicherheitsbeschränkungen für bestimmte Java-Applets aufhebt bzw. lockert, kann ein Applet im Extremfall dieselben Zugriffsrechte genießen wie eine lokal gestartete Applikation.

7.1 Risiken

Aufgrund der Tatsache, daß Java für verteilte Systeme entwickelt worden ist, bietet es mit seinen durchdachten Mechanismen eine ausreichende Sicherheit. Jedoch sind durch Implementierungsfehler Angriffe durch Java-Applets ermöglicht worden, die sich in folgende Kategorien unterteilen lassen:

- Angriffe, die das System oder seine Ressourcen modifizieren:

  Die Konsequenzen dieser Art von Angriffen sind sehr ernst, da meist der Rechner den Dienst verweigert oder Daten gelöscht bzw. verändert werden können. Java verfügt über ausreichende Schutzmechanismen gegen diese Art von Angriffen. Jedoch wurden in der Vergangenheit verschiedene Angriffe dieser Art durch Programmier- bzw. Implementationsfehler in den Ablaufumgebungen (Browser) ermöglicht.

- Angriffe, die eine weitere Benutzung des Systems verhindern (hostile applets):

  Bei dieser Art von Angriffen verbrauchen die Applets gewollt (der Effekt wurde vorsätzlich erzeugt) oder ungewollt (Programmierfehler) massiv Systemressourcen, wie Speicher und

Rechnerzeit, oder erzeugen Tausende von Fenstern, um das System zu überlasten. In den meisten Fällen läßt sich der Fehler durch Beenden des Browsers oder notfalls durch Herunterfahren des Rechners beheben. Trotzdem kann diese Art von Angriffen die Produktivität sowie die betrieblichen Datenverarbeitung erheblich beeinflussen. Java bietet keine Schutzmechanismen gegen diese Art von Angriffen, da automatisiert nicht unterschieden werden kann, ob das Applet für seinen normalen Betrieb viele Ressourcen in Anspruch nimmt oder ob es böswillig ist.

- Angriffe zur Ausforschung des Nutzers:

  Angriffe dieser Art umfassen das Lesen von fremden Nachrichten (Emails), Ändern von Nachrichten und das Verschicken von unverschämten bzw. bösartigen Texten. Die Java Umgebung bietet genügend Schutz, um Angriffe dieser Art abzuwehren. Java unterstützt Verschlüsselungsverfahren (Message Digest) zum Schicken und Empfangen von Nachrichten.

- Angriffe, um die Nutzer zu belästigen:

  Auch diese Angriffe können zu erheblichem Ärger für den Nutzer führen. Denkbare Angriffe sind das Spielen von unerwünschten Musikstücken oder Darstellen von obszönen Bildern auf dem Bildschirm, um den Anwender zu belästigen. Die Java Umgebung bietet hiergegen keinen Schutz, jedoch läßt sich das Applet einfach durch Springen auf eine andere Seite beenden.

Folgende Tabelle stellt die Angriffsarten und Javas Schutzmechanismen gegenüber:

Art des Angriffs	**Java Schutzmechanismus**
Angriffe, die das System oder seine Ressourcen modifizieren	*Schutz durch den Sandkastenmechanismus (Security- Manager, Klassenlader, Byte-Code-Verifizierer)* *Schutz durch Zertifizierung von Applets*
Angriffe zur Ausforschung des Nutzers	*siehe oben*
Angriffe, die eine weitere Benutzung des Systems verhindern	*kein Schutz durch Javas Schutzmechanismen* *manuelles Beenden der Java-Applets*
Angriffe, um die Nutzer zu belästigen	*kein Schutz durch Javas Schutzmechanismen (vgl. Kap. 7.2)*

7.2 Schutzmöglichkeiten

Trotz aller Sicherheitsmechanismen, die Java bietet, können u. U. Angriffe stattfinden, da die Implementierung dieser komplexen Si-

cherheitsmechanismen seitens der Anbieter von Java-Ablauf-Umgebungen fehlerhaft sein können. Aus diesem Grund werden weitere Mechanismen erläutert, mit denen der Nutzer sich absichern kann.

- Abschalten der Java-Funktionalität von Browsern:

  Die restriktivste Methode ist die Abschaltung der Java-Funktionalität im verwendeten Browser. Damit können keine Java-Applets innerhalb des Browsers gestartet werden. Das bedeutet einen enormen Einschnitt in den Funktionsumfang von WWW-Seiten. Folgendermaßen kann die Java-Funktionalität des entsprechenden Browsers abgeschaltet werden:

	Netscape Navigator 3	**Netscape Communicator 4**	**Microsoft Internet Explorer 3**
Deaktivieren der Selektionsbox	*Options / Network Preferences / Languages / Enable Java*	*Edit / Preferences / Advanced / Enable Java*	*Ansicht / Optionen / Sicherheit / Aktive Inhalte / Java Programme aktivieren*

- Verwendung von Filterprogrammen für Java

  Eine weitere Möglichkeit ist die Verwendung von Filterprogrammen für Java. Java Filterprogramme bieten einen effektiven Schutz gegen ungewollte Java Applets, ohne die Java-Unterstützung im Browser abschalten zu müssen.

  Der Browser wird durch eine entsprechende Software erweitert, die vor dem Laden eines Applets den Benutzer durch eine Dialogbox warnt und gleichzeitig die Möglichkeit gibt, das Applet abzuweisen oder zu starten. Weiterhin kann die Adresse (URL) dieses Servers in eine Datenbank aufgenommen werden, um für künftige Sitzungen festlegen zu können, daß das Applet ohne Rückfrage akzeptiert bzw. abgewiesen wird. Über entsprechende Konfigurationsmenüs läßt sich die Datenbank mit den Serverlisten jederzeit ändern und erweitern. Es besteht sogar die Möglichkeit, nur Applets innerhalb eines Intranets zuzulassen.

  Filterprogramme für Java sind eine gute Möglichkeit, die Sicherheitsbedenken bei Verwendung von Java Applets in den Griff zu bekommen, bis sich die Signierung von Java-Code im Internet durchgesetzt hat. Die Signierung von Java-Code wird ab den Versionen 4 der Browser-Software von Netscape und Microsoft unterstützt.

Das kommerzielle Produkt SurfinShield der Firma Finjan sowie ein für Forschungszwecke frei verfügbares Programm der Universität Princeton wurden in diesem Kontext evaluiert.

Die Merkmale sind in der folgenden Tabelle zusammengefaßt:

Name	**SurfinShield**	**Java Filter**
Hersteller	*Finjan Software*	*Universität Princeton*
Vetrieb	*Citco Building, Giborai Israel Street, South Netanya 42504 Israel*	*kein Vertrieb*
Internet Adresse	*http://www.finjan.com*	*http://www.cs.princeton.edu/sip/JavaFilter*
Version	*2.0*	*1.0*
Unterstützung für NT/Win95	*ja*	*ja*
Unterstützung für Unix	*ja*	*nein*
Unterstützung für Netscape Navigator	*ja, bis Version 3*	*ja, für Version 3*
Unterstützung für Microsoft Internet Explorer	*ja, für Version 3*	*nein*
Protokollierungsmechanismen	*ja*	*nein*
Alarmierung des Nutzers bei Sicherheitsverletzungen durch das Applet	*ja*	*nein*
Verhindert das Laden von verdächtigen Applets	*ja*	*ja*
Beenden von Applets bei Verletzung von Sicherheits-regeln	*ja*	*nein*
Verwendete Ressourcen werden dargestellt (z.B. Speicher, Anzahl von Applets)	*ja*	*nein*
Gewichtungsmöglichkeit der Sicherheitsaspekte	*ja*	*nein*
Adress-Datenbank für verdächtige Applets	*ja*	*ja*
Update Möglichkeit der Adress-Datenbank durch Nutzer und durch Anbieter	*ja*	*ja, durch Nutzer*

7.3 Empfehlungen

Obwohl immer wieder von gravierenden Sicherheitslücken in Java berichtet wird, gehört Java zu den wenigen Sprachen, die über ein integriertes durchdachtes Sicherheitskonzept verfügen, was Java für einen sicheren WWW-Einsatz prädestiniert. Die Sicherheitslücken entstanden in der Vergangenheit durch Fehler in der Implementierung und waren nie systemimmanent. Unabhängige Institutionen (z.B.: CERT[23]) evaluieren Sicherheitsaspekte von Java, um eventuelle Fehler zu erkennen und in einer neuen Version beheben zu können.

Folgende Richtlinien sollten im Hinblick auf den Einsatz von Java berücksichtigt werden, um eine maximale Sicherheit zu erreichen:

- Es sollten immer die neuesten Versionen der Browser-Software verwendet werden, oder entsprechende Updates der älteren Versionen installiert werden, um erkannte Fehler auszuschließen. Jedoch sollten keine Test- bzw. Betaversionen von Browsern verwendet werden. Der Einsatz von Browser-Versionen, die zertifizierte Java Applets unterstützen, sollte angestrebt werden.
- Filterprogramme für Java-Applets sollten eingesetzt und deren Adreßlisten mit verdächtigen WWW-Servern in festgelegten Zeitabständen aktualisiert werden.
- Administratoren sollten in bestimmten Zeitabständen die Hinweise der entsprechenden Institutionen (z.B.: CERT) auswerten, die beim Erkennen von potentiellen bzw. aktuellen Sicherheitsangriffen Hilfestellung und Ratschläge geben.
- Nutzer müssen über die Gefahren beim Herunterladen von Code vom einem unbekannten Server informiert und geschult werden.
- Kritische Systeme, die beispielsweise sehr vertrauliche Informationen verarbeiten, sollten durch Sicherheitsexperten getestet und abgenommen werden.

[23] siehe http://www.cert.org

8 Sicherheit bei der Nutzung von JavaScript

Im Gegensatz zu den Angriffsmöglichkeiten mit Java-Applets ist mit JavaScript keine Schädigung des Clients möglich, da keine JavaScript-Methoden existieren, die einen Zugriff auf das Dateisystem des Rechners sowie Verbindungsaufbau zu anderen Rechnern im Netz zulassen. Jedoch konnten Sicherheitsprobleme mit JavaScript in zwei Bereichen identifiziert werden:

1. Nutzer und Computersysteme werden ausgeforscht,
2. Rechner werden überlastet und verweigern die Arbeit.

8.1 Risiken

Folgende Sicherheitslücken wurden bisher bei der Verwendung von JavaScript identifiziert:

- Verschicken von Emails ohne Kenntnis des Nutzers

  Mit JavaScript kann das Mail-Tool des Browsers (Netscape-Mail) zum Senden einer Email ohne Wissen des Nutzers angesprochen werden. Mit dieser Methode lassen sich Email-Adressen von Nutzern erfassen und für Werbezwecke oder gar für böswillige Zwecke einsetzen.

- Auslesen der Legende des Browsers

  JavaScript ermöglicht das Auslesen der sogenannten Legende des Browsers, d.h. die zuletzt besuchten WWW-Adressen (URL) können ermittelt und an einen beliebigen Rechner im Netz verschickt werden. Die gesammelten Daten können zur Erstellung von Nutzerprofilen verwendet werden. Eine weitere Methode ist das Öffnen eines für den Nutzer nicht erkennbaren (1*1 pixel) Browser-Fensters, das während einer Sitzung im Hintergrund alle angesprungenen Adressen (URL) protokolliert.

- Auslesen von Verzeichnisstrukturen auf dem Client

  Mit JavaScript lassen sich die Verzeichnisstrukturen der lokalen Festplatte sowie aller im Zugriff befindlichen Netzwerkplatten des Clients auslesen und an einen beliebigen Server übertragen. Hierzu ist jedoch die Interaktion des Nutzers notwendig: Der Nutzer muß durch Bestätigen eines Schaltfeldes den Vorgang initiieren. Die Seiten können jedoch so gestaltet werden, daß ein anderer Sachverhalt vorgetäuscht wird und der Benutzer bedenkenlos dieses Schaltfeld betätigt. Dies bedeutet die Ausforschung der Nutzer, ihrer Daten und Computersysteme sowie ein enormes Sicherheitsrisiko, da Informationen über die

Infrastruktur einer Organisation einen anschließenden Einbruch in das System erleichtern.

- Auslesen und Übertragen von Dateien des Clients

  Über eine Interaktion des Benutzers (Drücken eines Schaltfeldes) können bestimmte Dateien, von denen der Pfad und Name bekannt ist, auf dem Client ausgelesen und auf einen beliebigen Server übertragen werden. Die Kenntnis des verwendeten Betriebssystems reicht im allgemeinen aus, um Pfad und Dateinamen von wichtigen Systemdateien zu erraten. Beispielsweise ist meist das Windows-Betriebssystemen im Verzeichnis *C:\Windows* installiert, in der sich auch alle Initialisierungsdateien befinden, die für beabsichtigte Einbruchversuche Aufschluß über das Computersystem geben können.

- Überlasten des Systems

  Diese Art der Angriffe bringen kein unmittelbares Sicherheitsrisiko mit sich, jedoch kann besonders bei Verwaltungen und Unternehmen die Produktivität stark beinträchtigt werden. Beispielsweise werden durch Öffnen von unendlich vielen Browser-Fenstern, Warn-Meldungen oder einem massivem Gebrauch von Systemressourcen die Verwendung des Rechners behindert und das System zum Absturz gebracht. Abhilfe schafft hier meist das Beenden des Browsers über den Task-Manager (*Strg-Alt-Entf/Task-Manager/Task Beenden*) oder das Rebooten des Rechners, was für den Nutzer wiederum Warte- bzw. Ausfallzeit bedeutet und ggf. den Verlust von Arbeitsergebnissen.

Die genannten Sicherheitslöcher sind implementationsabhängig: Sie hängen von der Version des verwendeten Browsers ab. Die folgende Tabelle gibt einen Überblick:

	Netscape Navigator 2.0	**Netscape Navigator 2.01**	**Netscape Navigator 3.0**	**Netscape Navigator 3.01**	**Netscape Communicator 4.0**	**Microsoft Internet Explorer 3.0**
Verschicken von Emails ohne Kenntnis des Nutzers	*möglich*	*nicht möglich*	*möglich*	*nicht möglich*	*nicht möglich*	*nicht möglich*
Auslesen der Legende des Browsers	*möglich*	*möglich*	*nicht möglich*	*nicht möglich*	*nicht möglich*	*nicht möglich*
Auslesen von Verzeichnisstrukturen auf dem Client	*möglich*	*nicht möglich*	*nicht möglich*	*nicht möglich*	*nicht möglich*	*nicht möglich*
Auslesen und Übertragen von Dateien des Clients	*möglich*	*nicht möglich*	*nicht möglich*	*nicht möglich*	*nicht möglich*	*nicht möglich*
Überlasten des Systems	*möglich*	*möglich*	*möglich*	*möglich*	*möglich*	*möglich*

8.2 Schutzmöglichkeiten

Der restriktivste, aber sicherste Schutz ist durch das Abschalten der Verwendung von JavaScript gegeben. Folgende Einstellungen müssen hierzu geändert werden:

	Netscape Navigator 2.02	**Netscape Navigator 3**	**Netscape Communicator 4**	**Microsoft Internet Explorer 3**
Aktivieren bzw. Deaktivieren der Selektionsbox im Menü	*Options / Security Preferences / Disable Javascript* ***aktivieren***	*Options / Network Preferences / Languages / Enable Javascript* ***deaktivieren***	*Edit / Preferences / Advanced / Enable Javascript* ***deaktivieren***	*Ansicht / Optionen / Sicherheit / Aktive Inhalte / ActiveX Skripts ausführen* ***deaktivieren***

Um dem Verschicken von Email ohne Kenntnis des Nutzers entgegenzuwirken, hat Netscape ab der Navigator Version 3.01 eine Einstellungsmöglichkeit integriert, die eine Warnung ausgibt, bevor eine Email durch ein Script verschickt werden kann. Diese Warnung kann folgendermaßen eingeschaltet werden:

> Im Menü *Options/Network Preferences/Protocols* die Selektionsbox *Submitting a Form by Email* aktivieren

8.3 Empfehlungen

Viele der vorhandenen Sicherheitslöcher von JavaScript wurden inzwischen seitens der Browser-Anbieter beseitigt. Jedoch sind Angriffe, die die Unwissenheit des Anwenders ausnutzen, nicht auszuschließen. Denkbar sind hier Angriffe, die durch Vortäuschen eines anderen Sachverhaltes den Nutzer zur Eingabe von sensitiven Daten (Passwörter, Kreditkartennummer usw.) oder Bestätigen von Interaktionen auffordern.

Folgende Regeln sollten eingehalten werden, um eine maximale Sicherheit bei dem Einsatz von JavaScript zu gewährleisten:

- Die JavaSript Funktionalität sollte während dem willkürlichen Surfen im Internet deaktiviert werden. Nur bei vertrauenswürdigen Servern sollte eine Aktivierung in Erwägung gezogen werden.
- Es sollten immer die aktuellsten Versionen der Browser verwendet werden. Die Version 4 des Navigators unterstützt zertifizierten JavaScript-Code. Somit kann der Nutzer selbst festlegen, von welchem Server Scripts zugelassen werden und von welchem nicht.

- Bei nicht vertrauenswürdigen Servern sollten Schaltfelder nicht bedenkenlos gedrückt werden, da nicht klar ist, welche Aktionen tatsächlich angestoßen werden.
- Vor dem Surfen im WWW sollte man alle wichtigen geöffneten Dokumente sichern und die zugehörigen Applikationen schließen, um dem Verlust von Arbeitsergebnissen bei Systemüberlastung bzw. Systemabsturz vorzubeugen. Dies sollte bei jeglicher WWW-Benutzung berücksichtigt werden, da Browser oft viele Ressourcen verbrauchen.
- Nutzer müssen auf Gefahren durch JavaScript hingewiesen werden.

9 Sicherheit bei der Nutzung von ActiveX

Heruntergeladene ActiveX-Komponenten unterliegen keinerlei Einschränkungen und können somit alle Aktionen ausführen, die auch lokal gestartete Applikationen können. Somit stellen ActiveX-Komponenten, wenn sie über das Internet benutzt werden, grundsätzlich ein immenses Sicherheitsrisiko dar.

9.1 Risiken

Die Verwendung von Activex-Komponenten in einem Intranet bringt keine Risiken mit sich, wenn sichergestellt werden kann, daß nur getestete und sichere ActiveX-Komponenten verfügbar sind. Im folgenden werden Risiken, die bei der Verwendung von ActiveX über das Internet existieren, erläutert.

- Ausforschung von Nutzern bzw. Computersystemen:

  Über entsprechende ActiveX-Komponenten kann auf beliebige Nutzer- bzw. Systeminformationen zugegriffen werden, die automatisch über unterschiedliche Methoden (EMail, FTP, Newsgroups usw.) an Dritte weitergegeben werden können. Durch die fehlenden Protokollierungsmechanismen der Browser kann nach einem Angriff nicht mehr festgestellt werden, welche ActiveX-Komponente für den Angriff verantwortlich ist. Meist merkt der Nutzer nicht einmal, daß ein Angriff stattgefunden hat, da bösartige ActiveX-Komponenten einen normalen Ablauf vortäuschen und entweder nachts oder wenn der Nutzer nicht aktiv ist (z.B. Bildschirmschoner aktiv), Angriffe durchführen. Beispielsweise hat der Chaos-Computer-Club in Frankfurt öffentlich demonstriert, wie über eine ActiveX-Komponente die Transaktionsdateien des Quicken Online-Banking-Programms verändert wurden, um bei der nächsten Transaktion des Nutzers gleichzeitig Überweisungen auf ein eigenes Konto durchzuführen.

- Herunterladen von Viren möglich

  Heruntergeladene ActiveX-Komponenten können beliebige Viren im System installieren (siehe Kapitel 3.2: Risiken bei Email).

- Beschädigung von Systemressourcen

  Da ActiveX-Komponenten keinen Einschränkungen unterliegen, können sie beliebige Systemressourcen verändern und beschädigen. Denkbar wären das Löschen der Festplatte und somit Verlust von wichtigen Daten (z.B. Kundendaten, Auswertungen usw.) oder nur das Verändern von bestimmten Daten (z.B. Forschungsergebnisse, Buchhaltung usw.). Dies kann im Extremfall schlimme Auswirkungen haben, da der Nutzer mögli-

cherweise nicht sofort die Veränderung der Daten erkennt und mit falschen Daten weiter arbeitet (siehe Kapitel 3.2: Risiken bei Email).

- Überlasten des Systems

  ActiveX-Komponenten können, entweder durch Programmierfehler oder vorsätzlich, durch massiven Verbrauch von Systemressourcen, den Rechner überlasten und zum Absturz bringen. Dies kann den Verlust von nicht gespeicherten Dokumenten und Arbeitsergebnissen bedeuten und somit die betriebliche Datenverarbeitung und die Produktivität beinträchtigen.

9.2 Schutzmöglichkeiten

Um die Sicherheit bei der Nutzung von ActiveX zu erhöhen, können folgende Mechanismen eingesetzt werden:

- Abschalten der ActiveX Unterstützung:

  Der restriktivste aber maximale Schutz kann durch Abschalten der ActiveX-Unterstützung erreicht werden. Jedoch können damit keine ActiveX-Komponenten mehr verarbeitet werden. Beim Internet Explorer muß hierzu im Menü *Ansicht / Optionen / Sicherheit* die Selektionsbox *ActiveX Steuerelemente und Plugins aktivieren* deaktiviert werden.

- Verwendung von Microsofts Authenticode-Mechanismus

  Authenticode ist ein Mechanismus, der die Signierung von ausführbarem Code erlaubt. Durch die Signatur soll gewährleistet werden, das der Autor des Codes identifiziert werden kann und daß der Code während des Transports nicht verändert wurde. Hierzu werden zwei Komponenten an den Code angefügt:

  1. Eine digitale Signatur die den Code mit einem geheimen Schlüssel signiert.
  2. Ein digitales Zertifikat, das den zugehörigen öffentlichen Schlüssel, den Namen der Person oder Organisation dem der Schlüssel gehört und eine digitale Signatur eines anerkannten Trustcenters enthält.

  Für die Realisierung dieses Ansatzes ist die Existenz einer Infrastruktur, sogenannte Certifikation Authorities (CA) oder Trustcenter, zur Authentifizierung des Code-Betreibers und Zuordnung von Zertifikaten, notwendig. Jeder Nutzer ist in der Lage Code, zu signieren. Alle Werkzeuge, die zur Signierung von Code notwendig sind, sind im frei verfügbaren Microsoft Acti-

veX-Softwareentwicklungspaket[24] enthalten. Zur Signierung von Code sind folgende Schritte notwendig:

1. Das Programm *makecert* muß gestartet werden, das für den Nutzer ein public/private Schlüsselpaar sowie ein Zertifikat erstellt. Das erstellte Zertifikat muß von einem CA signiert werden, der dabei die Identität des Antragstellers überprüft. Jedoch sind hierfür die notwendigen Werkzeuge derzeit im ActiveX-Entwicklungspaket nicht enthalten. Deshalb ist ein Standard-Schlüssel im Entwicklungspaket enthalten, der die selbständige Signierung für Testzwecke erlaubt. Somit übernimmt der Nutzer gleichzeitig die Rolle eines CA.
2. Anschließend wird mit Hilfe des Programms *cert3spc* das signierte Zertifikat in ein PKCS7-Objekt gewandelt. Die PKCS7-Objekte dienen als Träger für Zertifikate nach dem X.509-Standard und können beliebig viele Zertifikate enthalten.
3. Das erstellte PKCS7-Zertifikat kann schließlich zur Signierung des Codes benutzt werden. Hierzu wird das Programm *SignCode* verwendet, das nach erfolgreicher Ausführung das Zertifikat in den Code integriert. Über entsprechende Programme (PeSigMgr, ChkTrust) kann der signierte Code getestet werden.

Der generelle Ablauf beim Empfang von signiertem Code im WWW ist folgendermaßen:

Der Internet Explorer verfügt nach Installation über eine vordefinierte Liste an verschiedenen CA, deren öffentliche Schlüssel bekannt sind. Der Internet Explorer versucht mit einem der öffentlichen Schlüssel das Zertifikat des empfangenen Codes zu entschlüsseln, und bekommt bei Erfolg den öffentlichen Schlüssel des Nutzers. Damit kann er schließlich die Signatur des Nutzers entschlüsseln. Somit ist die Identität und die Unverfälschtheit des Codes sichergestellt. Da signierter Code durch CA's nicht einzeln getestet wird, kann durchaus eine Komponente signiert werden, die die Sicherheit des Clients gefährdet. Inzwischen existiert bereits eine signierte ActiveX-Komponente die das Windows-Betriebssystem herunterfahren kann. Das zeigt, daß durch CA's signierte Komponenten ebenfalls keinen hundertprozentigen Schutz bieten können. Sobald jedoch CA's erfahren, daß ein bestimmter Code unzuverlässig ist, können sie dessen Signatur für ungültig erklären. Dies setzt voraus, das der Browser zur Laufzeit eine Verbindung zum CA aufbaut und die Gültigkeit der Signatur überprüft. Verisign ermöglicht bereits die On-Line-Überprüfung von signierten Code.

[24] siehe http://www.microsoft.com/activex/

- Aktivieren einer hohen Sicherheitsstufe im Internet Explorer

  Standardmäßig ist der Sicherheitslevel im Internet Explorer auf hoch eingestellt. Somit werden nur ActiveX-Komponenten akzeptiert, die seitens einer vertrauenswürdigen Institution (CA) mit einer digitalen Signatur versehen wurden. Bei dieser Einstellung wird nur Code akzeptiert, der durch eines der standardmäßig im Internet Explorer definierten CA's signiert wurde. Durch die Einstellung eines mittleren Sicherheitslevels kann der Nutzer selbst entscheiden, welcher Code akzeptiert werden soll.

- Einsatz von ActiveX-Filtern

  Entsprechend den Java-Filterprogrammen bieten die ActiveX-Filterprogramme[25] die Möglichkeit, Listen mit Servern zu definieren, von denen ActiveX-Komponenten akzeptiert werden (siehe Kapitel 7.2).

- Einsatz des Internet Explorer Administration Kit (IEAK) in Netzwerken

  Der IEAK ermöglicht die Erstellung von spezifisch angepaßten Internet Explorern, die den einzelnen Nutzern zur Verfügung gestellt werden können. Somit können Administratoren bereits vor Installation des Browsers die Nutzer- sowie alle sicherheitsrelevanten Einstellungen konfigurieren. Der Nutzer erhält einen Browser, der zwar in der Funktionalität eingeschränkt sein kann, aber den Sicherheitsanforderungen entspricht. Zusätzlich kann verhindert werden, daß der Nutzer im nachhinein die Einstellungen des Browsers verändert. Der Administrator kann auch zentral alle einzelnen Browser administrieren bzw. konfigurieren. Somit könnte er beispielsweise für Nutzer, deren Browser auf Clients mit sehr vertraulichen Daten laufen, jegliches Herunterladen von Code verbieten. Damit ist eine dynamische Anpassung der Einstellungen des Browsers, beispielsweise an aktuelle Sicherheitslücken möglich.

9.3 Empfehlungen

Folgende Richtlinien sollten im Hinblick auf die Verwendung von ActiveX-Komponenten berücksichtigt werden, um eine maximale Sicherheit zu erreichen:

- Falls auf ActiveX-Komponenten verzichtet werden kann, sollte die ActiveX-Funktionalität des Browsers abgeschaltet werden.
- Es sollte ein hoher Sicherheitslevel im Internet Explorer eingestellt werden.

[25] z.B. http://www.finjan.com

- Nur von vertrauenswürdigen Servern sollten ActiveX-Komponenten heruntergeladen werden.
- Es muß ein schlüssiges Backup-Konzept entwickelt und umgesetzt werden, um den Schaden durch Verlust von Daten einzuschränken.
- Der IEAK sollte in Netzwerken auf jeden Fall eingesetzt werde, um von zentraler Stelle die Konfiguration des Internet Explorer der einzelnen Nutzer zu bewerkstelligen.
- Nutzer müssen im Hinblick auf Gefahren durch heruntergeladene ActiveX-Komponenten hingewiesen werden.

10 Sicherheit bei Cookies

Als Cookies wird die Information bezeichnet, die ein WWW-Server bei einem Verbindungsaufbau an den Browser schickt, um ihn bei nachfolgenden Interaktionen wiedererkennen zu können. Die Motivation für die Entwicklung des Cookies-Mechanismus war, daß im WWW jeder Verbindungsaufbau eines Browsers mit einem Server, als eine eigenständige Interaktion behandelt wird. Dadurch kann auf Daten, die ein Nutzer in einer vorhergehenden Interaktion eingegeben hat, in späteren Interaktionen nicht zurückgegriffen werden, da der Server keinerlei Hinweise dafür hat, daß beide Interaktionen zusammengehören. Cookies erlauben die Kennzeichnung zusammengehöriger Interaktionen, wodurch der Nachteil des WWW ausgeglichen werden kann.

Cookies sind Informationen, meistens nicht mehr als eine eindeutige Identifikationsnummer, die der WWW-Server beim ersten Verbindungsaufbau an den Browser schickt. Der Browser legt diese Information in einer Datei oder einem Verzeichnis ab. Bei allen darauffolgenden Verbindungen zu diesem Server liefert der Browser diese Information (Cookies) zurück an den Server, der damit den Nutzer identifizieren und den Kontext und die Einstellungen der letzten Sitzung wiederherstellen kann. Der Browser liefert die Cookies nur an den Server zurück, der ihm dieses Cookie geschickt hat. Hierzu verfügen die Cookies über einen Domänennamen, der kennzeichnet, von welchem Server sie stammen. Der Browser vergleicht vor jeder Anforderung einer neuen Seite die URL der Seite mit dem Domänennamen der Cookies. Nur wenn der Domänenname der Cookies in der URL der Seite enthalten ist, schickt er die Cookies an den Server. Problematisch ist, daß der Domänenname der Cookies beliebig gesetzt werden kann. Somit kann beispielsweise der Domänenname eines gesendeten Cookies auf *acme.com* gesetzt werden, womit dieser Cookies bei weiteren Anforderungen des Browsers an alle Server, die in ihrer URL *acme.com* enthalten gesendet wir. Um jedoch Domännamen in der Form *.edu, .com usw.* zu vermeiden, müssen die Domänennamen mindestens zwei Unterteilungen haben (z.B. www.rsa.com).

Musterbeispiel für die Verwendung von Cookies ist das Online-Shopping, um die Einkaufsliste in eine weitere Sitzung zu übernehmen. Außerdem: WWW-Server, die eine Identifizierung des Nutzers erfordern, speichern eine erfolgreiche Anmeldung über Cookies, damit sich der Nutzer in einer neuen Sitzung nicht mehr anzumelden braucht.

10.1 Risiken

Der Cookies-Mechanismus bringt folgendes Risiko mit sich:

- Erstellung von Profilen über Surf-Gewohnheiten des Nutzers:

  Jeder Verbindungsaufbau mit einem WWW-Server hinterläßt durch die Protokollierungsmechanismen der einzelnen Server gewisse Informationen, die meist nicht sehr aussagekräftig sind, da sie sich nur auf einen Server beziehen. Mit Hilfe von Cookies wird die Erstellung von Internet-übergreifenden Profilen ermöglicht.

  Inzwischen haben sich Werbeagenturen[26] im Internet etabliert, die mit interessenangepaßter Werbung für WWW-Nutzer werben. Die HTML-Seiten der Kunden werden durch die Werbeagentur um eine Grafik erweitert, die auf einem Server der Werbeagentur liegt. Greift nun ein Nutzer auf eine Seite mit dieser Grafik zu, so wird eine Verbindung zum Server der Agentur aufgebaut, um diese Grafik zu holen. Dieser Server aber weist dem Browser neben der Grafik einen Cookie mit einer eindeutigen Kennung zu. Bei einer erneuten Anwahl einer Seite eines Servers, der auch zum Kundenstamm dieser Werbeagentur gehört, kann der Server somit den Nutzer identifizieren. Nach einer gewissen Zeit kann die Werbeagentur Listen mit Vorlieben und Interessen des Nutzers erstellen und diesen Nutzer gezielt mit Werbung versorgen. Weiterhin können die Nutzerprofile den Kunden zur Verfügung gestellt oder zur Beurteilung der Effektivität von Werbung herangezogen werden.

10.2 Schutzmöglichkeiten

Mit folgenden Mechanismen können sich Nutzer gegen Cookies schützen:

- Deaktivieren des Cookies-Mechanismus im Browser

  Die restriktivste Methode kann über das Abschalten der Unterstützung von Cookies im Browser erreicht werden, die bisher jedoch nur im Netscape Communicator möglich ist. Hierzu muß die Selektionsbox „*Disable Cookies“* im Menü „*Edit / Preferences / Advanced / Cookies“* aktiviert werden.

- Aktivieren der Ausgabe von Warnmeldungen im Browser

  Über Einstellungen kann im Browser die Ausgabe von Warnmeldungen beim Empfang von Cookies aktiviert werden. Damit hat der Benutzer die Möglichkeit zu entscheiden, von welchen Servern Cookies akzeptiert werden sollen und von welchen nicht. Jedoch versuchen viele Server durch aufeinanderfolgende Versuche einen Cookie zu setzen, den Nutzer mit Dialogboxen zu überhäufen, so daß er schließlich doch diesen Cookie akzeptiert.

[26] z.B: DoubleClick Network (http://www.doubleclick.net)

Folgende Einstellungen müssen im Browser zur Ausgabe einer Warnung aktiviert werden:

	Netscape Navigator 3	**Netscape Communicator 4**	**Microsoft Internet Explorer 3**
Aktivieren der Selektions-box im Menü	*Options / Network Preferences / Protocols / Accepting a cookie*	*Edit / Preferences / Advanced / Cookies/ Warn me before accepting a cookie*	*Ansicht / Optionen / Erweitert / Warnungen / Vor der annahme von cookies warnen*

- Verhindern der dauerhaften (persistenten) Haltung von Cookies

  Cookies werden zur Laufzeit des Browsers dynamisch im Speicher gehalten, wobei zusätzlich eine persistente Speicherung im Filesystem stattfindet. Durch entsprechende Mechanismen kann die persistente Speicherung in das Filesystem verhindert werden. Somit gehen beim Beenden des Browsers alle Cookies verloren und ein zusammenhängendes Nutzerprofil kann nicht erstellt werden.

  Die Vorgehensweise zeigt folgende Tabelle:

	Netscape Navigator 3	**Netscape Communicator 4**	**Microsoft Internet Explorer 3**
Pfad der persistent abgelegten Cookies:	*<Installationspfad des Netscape Navigators> / Netscape / Program/**cookies.txt***	*<Installationspfad des Netscape Communicators> / Netscape / Users / <Benutzer des Systems> / **cookies.txt***	<Windows Installationspfad> / **Cookies**
Verhindern der persistenten Haltung durch:	*Aktivieren eines Schreibschutzes auf die Datei cookies.txt*	*Aktivieren eines Schreibschutzes auf die Datei cookies.txt*	Löschen des Verzeichnisses „Cookies“ und erstellen einer Datei mit dem Namen „Cookies“

10.3 Empfehlungen

Um die Möglichkeit der Erstellung von Nutzerprofilen mit Hilfe von Cookies zu verhindern, sollten folgende Richtlinien eingehalten werden:

- Nur bei vertrauenswürdigen WWW-Servern sollte der Cookies-Mechanismus aktiviert werden.
- Im Browser sollte die Ausgabe von Warnmeldungen aktiviert werden.
- Nutzer sollten auf Probleme im Hinblick auf die Nutzung von Cookies geschult werden.

11 Sicherheitsaspekte bei Browsern

Die derzeit gängigsten Browser (Netscape Navigator und Internet Exlorer) verfügen über verschiedene Mechanismen, um die Sicherheit bei der Nutzung des Internet zu erhöhen. Folgende Tabelle stellt die verschiedenen Sicherheitsfeatures den Browserversionenen gegenüber:

Sicherheitsfeatures	**Netscape Navigator 3**	**Netscape Communicator 4**	**Microsoft Internet Explorer 3**	**Microsoft Internet Explorer 4 (Preview)**
Verschlüsselung (SSL)	*möglich*	*möglich*	*möglich*	*möglich*
Zertifikate	*möglich*	*möglich*	*möglich*	*möglich*
Zertifikate für Java Applets	-	*möglich*	*möglich*	*möglich*
Unterstützung für Server-Zertifikate	*möglich*	*möglich*	*möglich*	*möglich*
Unterstützung für Client-Zertifikate	*möglich*	*möglich*	*möglich*	*möglich*
Java- Sandkasten-prinzip	*möglich*	*möglich, Funktionalität von signierten Applets kann durch Nutzer angepaßt werden*	*möglich*	*möglich, Funktionalität von signierten Applets kann durch Nutzer angepaßt werden*
Verschlüsselte Mail (S/MIME)	-	*möglich*	-	-
Schutz vor unanständigen Inhalten	-	-	*möglich*	*möglich*
Schutz vor Cookies	*möglich*	*möglich*	*möglich*	*möglich*

Literatur

(IM, 94) Innenministerium Baden-Württemberg, Schäfer, Georg; Datenschutz- und Sicherheits-konzept für das LVN-OSI, A.z.: S-0278-LVN/30

(IM, 96) Innenministerium Baden-Württemberg, Schäfer, Georg; Einsatz der Verschlüsselung in der Landesverwaltung Baden-Württemberg, Konzeption, A.z.: S-0275.0/11

(IM, 97/1) Innenministerium Baden-Württemberg, Schäfer, Georg; Einsatz der Intranet-Technik in der Landesverwaltung Baden-Württemberg, Konzeption, A.z.: S-0278-LVN/58

(IM, 97/2) Innenministerium Baden-Württemberg, Schäfer, Georg; Datenschutz und Datensicherheit bei Client - Server - Systemen, Entwurf, A.z.: S-0275.0/12

(Schäfer, 97) Schäfer, Georg; Mit Sicherheit erfolgreich - Ein Leitfaden zur Sicherung moderner Informations- und Kommunikationssysteme, R.v. Decker Verlag, 1997, ISBN 3-7685-4796-5

(S. Garfinkel u. G. Spafford, 97) Web Security & Commerce, O'Reilly & Associates, 1997, ISBN 1-56592-269-7

Weiterführende Informationen im WWW

Informationen zu	**URL-Adresse**
ActiveX	http://ttrip1.worms.fh-rpl.de/sem/ws96_97/ ActiveX/einfuehr.htm
Anonymes „surfen“	http://www.anonymizer.com/
Ascom	http://www.ascom.ch/systec/
Certification Authorities	http://www.pca.dfn.de/eng/team/ske/pem-dok.html
Einführung in Java	http://remus.prakinf.tu-ilmenau.de/wetter/ java/vortrag.html
Internet Einführung	http://escher.north.de/~soenke/internet/internet-kurz.html#ftpg
Internet- und WWW-Kurs	http://www.erlangen.netsurf.de/kurs/
Internet Sicherheitssysteme	http://www.iss.net/vd/faq.html
Javascript- und ActiveX-Viren	http://www.cantrip.org/javirus.html
Java-, Javascript- und Acti-	http://www.digicrime.com/

veX-Angriffe	

Kryptografie-Regelungen und Gesetze in verschiedenen Ländern	http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm
Kryptografie-Protokolle im Vergleich	http://www.c2.org/~raph/comparison.html
Microsoft Sicherheitsfeatures	http://www.microsoft.com/security/
MIMESweeper	http://www.mimesweeper.integralis.com/
MIME-Types	http://www.fh-karlsruhe.de/~hema0011/ mime/mime.html
Netscape Sicherheitsfeatures	http://home.netscape.com/info/security-doc.html
PGP	http://www.ifi.uio.no/pgp/
Privatsphäre	http://cip.physik.uniwuerzburg.de/~hofmann/netschraeg.html
RSAC	http://www.rsac.org/
RSA	http://www.rsa.com
Sicherheit im WWW	http://www.cs.unc.edu/Courses/wwwc/public/hanes/security.html
Sicherheitslexikon	http://shoppingservice.com/lexikon.htm
Trustcenter in Deutschland	http://www.cert.dfn.de/dfnpca/certify/ http://www.in-ca.individual.net/ http://www.trustcenter.de/contents/index.html
Verisign	http://www.verisign.com/
Sicherheit und Verschlüsselung	http://www.yahoo.de/Computer_und_Internet/Sicherheit_und_Verschluesselung/
Zusammenstellung der häufig gestellten Fragen zur WWW-Technologie	http://www.netscapeworld.com/netscapeworld/common/nw.jumps.html