Sicherheit im Internet

Dr. Jan-Armin Reepmeyer
Betriebliche Datenverarbeitung

Risikoanalyse
Wer sind die Bösen?

- Mitarbeiter
  - verärgerte ehemalige und unehrliche Mitarbeiter
  - ca. 60 - 80 % der sicherheitskritischen Vorfälle aus eigenen Reihen
- Mitbewerber (Spionage)
  - spezielles Gebiet, auch Einsatz der „sozialen Komponente“
- Hacker
  - „bad guy“, 14 bis 24 Jahre alt, männlich, ohne Beruf bzw. Student, keine Freundin, Hacken ist Hobby
- Mitarbeiter mit schlechter Schulung
  - ohne Absicht, unbewusst

Sicherheitskonzept

- Grundlegende Erkenntnisse
  - Sicherheit kostet Geld
  - absolute Sicherheit unmöglich
- Folgerungen
  - Risikoanalyse und Festlegung eines Sicherheits-niveaus, auch partiell differenziert
  - Ableitung eines Maßnahmenbündels
- Vergl.: „ewiger Kampf“ Bank vs. Safeknacker

Risikoanalyse
Was kann passieren?

- Geheime Daten werden bekannt
- Daten werden gelöscht
  - Arbeit behindert
- Daten werden verfälscht
  - falsche Entscheidungen werden getroffen
- Rechner und Netze nicht mehr benutzbar
  - Denial of Service (DoS), Ansatzpunkt für Erpressung
- Rechner und Netze unerlaubt benutzt
  - Rechenleistung, Plattenplatz, Nutzung für andere Attacken

Risikoanalyse
Wo sind die Angriffspunkte?

- Risiken der ans Netz angeschlossenen Computer
- Risiken in der Kommunikation über das öffentliche Netz (Internet)
- Risiken, die auch ohne Anschluss an das Internet bestehen
  - Viren, Backups, Passwörter

Firewalls

- Koppeln gesicherte an ungesicherte Netzwerke
- schützen das gesicherte Netzwerk und ermöglichen gleichzeitig den möglichst ungestörten Zugriff auf das ungesicherte Netzwerk
- stellen den einzigen Zugang vom gesicherten zum ungesicherten Netzwerk dar

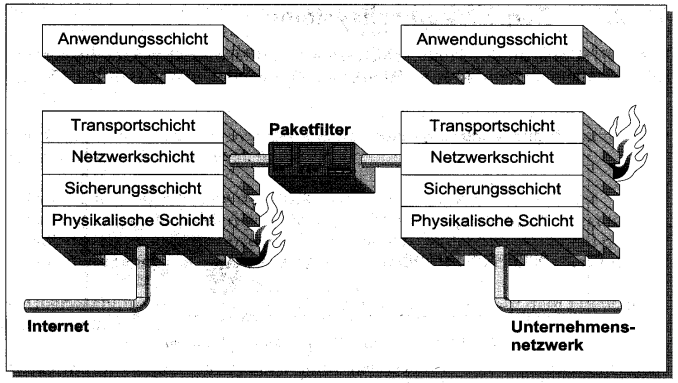
Gegenmaßnahmen

- Risiken der ans Netz angeschlossenen Computer
  Firewalls
- Risiken in der Kommunikation über das öffentliche Netz (Internet)
  Verschlüsselung, Digitale Signatur
- Risiken, die auch ohne Anschluss an das Internet bestehen
  Social Engineering

Vorteile von Firewalls

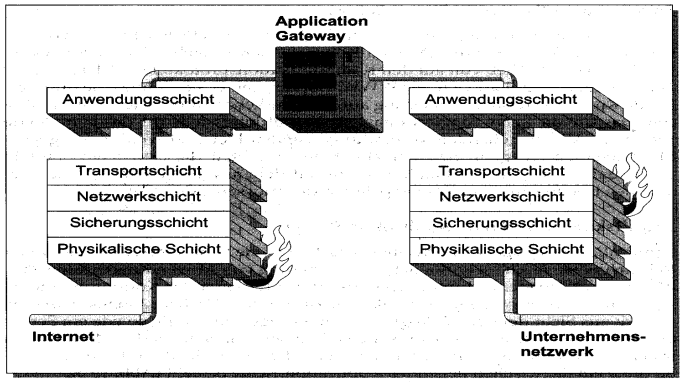
- Konzentration des Risikos auf ein einziges System
- Konzentration der Sicherheitsmaßnahmen
- Überwachungs- und Kontrollmechanismen nur auf einem Rechner / wenigen Rechnern
- Alle Verbindungen über einen/wenige Rechner => Überwachung (Logbuch) und Kontrolle

Architektur des Firewallsystems Paketfilter



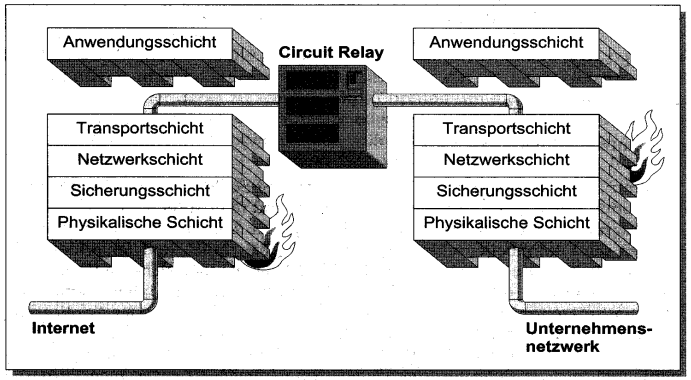
Quelle: Kyas, O., Sicherheit im Internet, 2. Auflage, Bonn 1998

Architektur des Firewallsystems Application Gateway



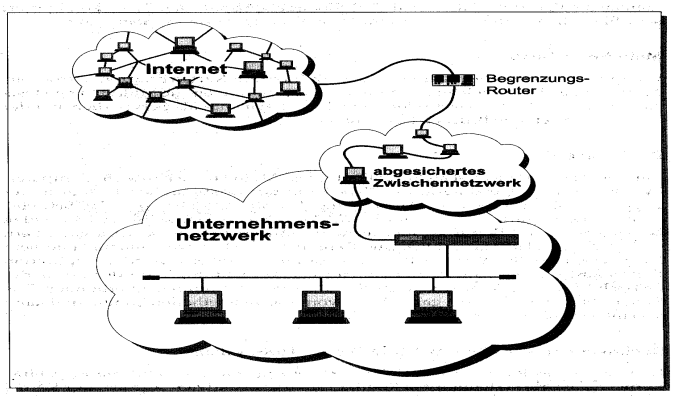
Quelle: Kyas, O., Sicherheit im Internet, 2. Auflage, Bonn 1998

Architektur des Firewallsystems Circuit Relay



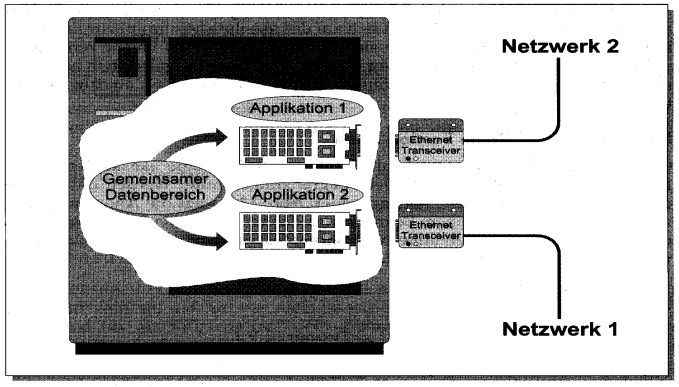
Quelle: Kyas, O., Sicherheit im Internet, 2. Auflage, Bonn 1998

Topologie des Firewallsystems Router (mit abgesichertem Zwischennetz)



Quelle: Kyas, O., Sicherheit im Internet, 2. Auflage, Bonn 1998

Dual Home (Bastion) Host

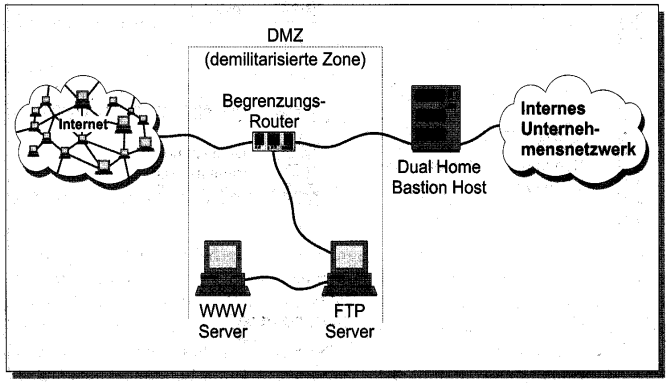


Quelle: Kyas, O., Sicherheit im Internet, 2. Auflage, Bonn 1998

Grenzen von Firewalls

- Keine Blockademöglichkeit für Daten, die innerhalb von Protokollen versteckt transportiert werden (Tunneling)
- Kein Schutz gegen unautorisierte physikalische Zugriffe (Anzapfen von Leitungen, FunkLAN)
- Weitere Lösung: VPN (Virtual Private Network)

Dual Home Bastion Host und DMZ



Quelle: Kyas, O., Sicherheit im Internet, 2. Auflage, Bonn 1998

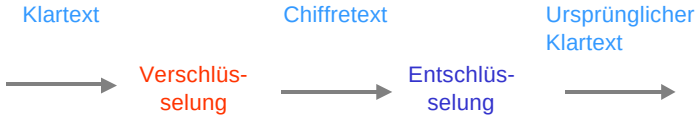
Sicherheitsanforderungen an Kommunikationsprozesse

1. Authentifizierung
   - Ermittlung der Identität des Kommunikationspartners
   - Ist mein Kommunikationspartner der, der er vorgibt zu sein?
2. Vertraulichkeit
   - Verhindern, dass Dritte etwas über den Inhalt oder die Art der Kommunikationsbeziehung erfahren
3. Datenintegrität
   - Erkennen von Verfälschungen der Nachricht
4. Nicht-Abstreitbarkeit / Verbindlichkeit
   - Beweis der Herkunft und Zustellung von Nachrichten

Konkrete Probleme

- Unverschlüsselte Datenübertragung bei allen gängigen Internet-Diensten
  => IP-Datagramme können in jedem weiterleitenden Knoten im Internet eingesehen werden.
- keine fixe Verbindung zwischen IP-Adresse und Nutzer
  =>Versand gefälschter Datenpakete möglich
  => IP-Adresse zur eindeutigen Authentifizierung der Kommunikationspartner nicht geeignet

Verschlüsselung



Kryptographie

Konkrete Probleme

- zahlreiche Sicherheitslücken im Domain Name Service (DNS)
  => DNS-Spoofing: Ein Anbieter kann unter einem beliebigen Domainnamen im Internet auftreten.
- Jeder weiterleitende Knoten kann IP-Data-gramme herausfiltern oder modifizieren.
  => Datenintegrität nicht gewährleistet

kryptographische Algorithmen

- Mathematische Funktionen der Ver- und Entschlüsselung = Chiffrierung
- Eingeschränkte Algorithmen
- Uneingeschränkte Algorithmen
  - Ein-Schlüssel-Verfahren
  - Mehr-Schlüssel-Verfahren

Eingeschränkte Algorithmen

Beispiele

- Steganographie: unauffällige Beimischung von Daten in Bildern / Audio / Video / ASCII
- Substitution: Ersetze jeden Buchstaben des Alphabets durch einen beliebigen anderen Buchstaben. (Caesar)
- Transposition: Vertauschen von Klartext-Zeichen untereinander
- Rotormaschinen: Enigma

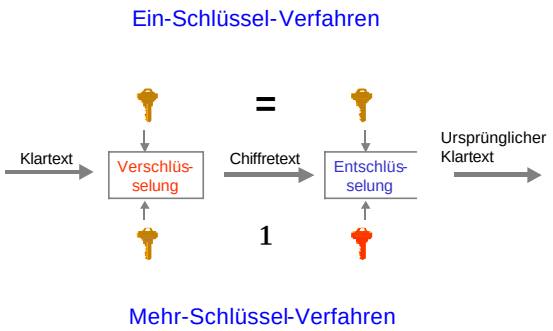
uneingeschränkte Algorithmen

- Verwendung von Schlüsseln aus einem Schlüsselraum
- Trennung von Verschlüsselungsalgorithmus und Schlüssel
- Sicherheit hängt von der Geheimhaltung des Schlüssels ab, Algorithmus wird veröffentlicht
- meist bekannt und standardisiert sowie expliziten Angriffen ausgesetzt
- Ein-Schlüssel-Verfahren
  Mehr-Schlüssel-Verfahren

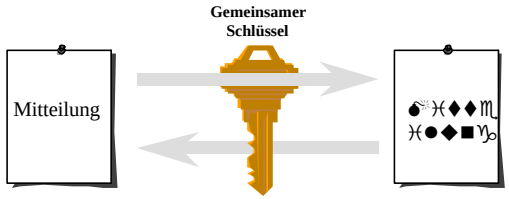
Eingeschränkte Algorithmen

- Sicherheit hängt von der Geheimhaltung des Verfahrens ab
- lediglich noch von historischer Bedeutung
- nachteilig bei der Verwendung in Gruppen mit wechselnden Teilnehmern
- erlauben keine Qualitätskontrolle und keine Standardisierung
- trotz der Mängel bei vielen Anwendern beliebt

Ein-/Mehrschlüsselverfahren

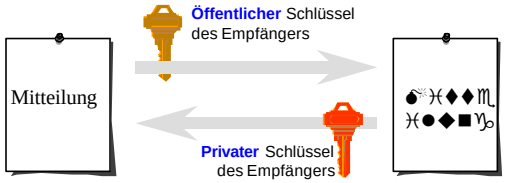


Ein-Schlüssel-Verfahren



- Symmetrische Verschlüsselung, d.h. Algorithmus arbeitet mit einem einzigen Schlüssel
- Sender benutzt gleichen Schlüssel zum Verschlüsseln wie Empfänger zum Entschlüsseln
- Secret Key

Mehr-Schlüssel-Verfahren



- asymmetrische Algorithmen, benutzen verschiedene Schlüssel für die Codierung und Decodierung
- Private Key (geheim) und Public Key (veröffentlicht)
  zwei Bruchstücke einer Münze, die zusammen passen
- Einweg-Funktion / Trapdoor One-Way Function

Symmetrische Verschlüsselung

- Beispiele: DES (Data Encryption Standard), RC2, RC4, IDEA
- Angriffe durch Ausprobieren von Schlüsseln: Brute-Force-Attack

  Dauer abhängig von Schlüssellänge, Beispiele (1999):
  - DES 40 Bit 0,4 Sekunden
  - DES 64 Bit 74 Stunden, 40 Minuten
  - DES 128 Bit 157.129.203.952.300.000 Jahre
- Probleme
  - sicherer Austausch des Schlüssels
  - je 2 Teilnehmer in einem Sicherheitsnetz benötigen einen geheimen Schlüssel
    2 TN -> 1 Schl, 3 TN -> 3 Schl, 4 TN -> 6 Schl etc.

Asymmetrische Verschlüsselung

- Sender verschlüsselt mit Public Key des Empfängers, der entschlüsselt mit seinem dazu passenden Private Key
  =>Vertraulichkeit
- Sender verschlüsselt mit seinem Private Key, der nur mit seinem dazu passenden Public Key entschlüsselt werden kann
  =>Authentizität + Integrität + Verbindlichkeit des Absenders (Digitale Unterschriften)

Asymmetrische Verschlüsselung

- Beispiele: RSA (Rivest Shamir Adelman), DSA (Digital Signature Algorithm), DAS / Pretty Good Privacy
- Faktor 100 langsamer als symmetrische Verfahren
- basiert auf Faktorisierungsproblem: Es ist einfach, das Produkt zweier großer Primzahlen zu bilden, aber es dauert sehr lange, die Primfaktoren einer Zahl zu ermitteln.
- Brechen eines 512-Bit-Schlüssels: 8 Monate, ca. 1 Mio $ (Quelle: RSA Data Security) => üblich daher mindestens 1024 Bit

Wie lang muss ein öffentlicher Schlüssel sein (RSA)?

- lang genug, um Sicherheit zu gewährleisten
- kurz genug, um in praktischen Berechnungen verwendbar zu sein
- Empfehlungen (keine sicheren Aussagen!)

Jahr	geg. Einzelperson	geg. Unternehmen	geg. Regierung
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

Symmetrische vs. asymmetrische Verschlüsselung

- Problem symmetrisch (Ein-Schlüssel): sicherer Austausch des Schlüssels
- Problem asymmetrisch (Mehr-Schlüssel): langsame Algorithmen
- Lösung: Nachricht symmetrisch verschlüsselt, zum Entschlüsseln mitgeschickter Schlüssel asymmetrisch verschlüsselt

Zeit- und Kostenabschätzung eines Brut-force-Angriffs (1995)

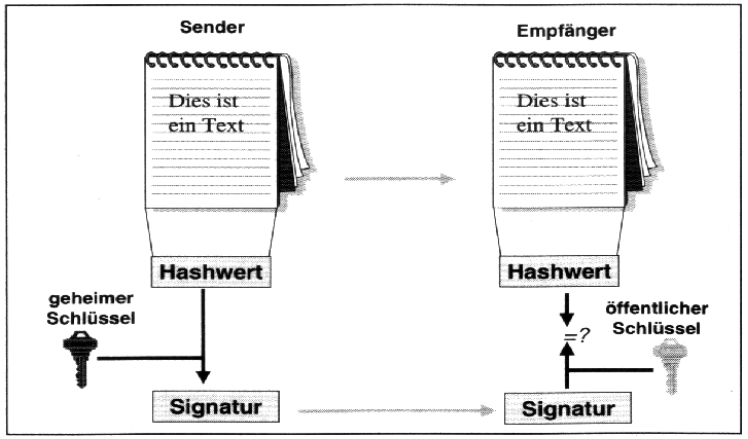
	Schlüssellänge in Bit					
Kosten (Dollar)	40	56	64	80	112	128
100.000	2 s	35 h	1 J	70000 J	10^{14} J	10^{19} J
1.000.000	0,2 s	3,5 h	37 T	7000 J	10^{13} J	10^{18} J
10.000.000	0,02 s	21 min	4 T	700 J	10^{12} J	10^{17} J
100.000.000	2 ms	2 min	9 h	70 J	10^{11} J	10^{16} J
1.000.000.000	0,2 ms	13 s	1 h	7 J	10^{10} J	10^{15} J
10.000.000.000	0,02 ms	1 s	5,4 min	245 T	10^{9} J	10^{14} J
100.000.000.000	2 ms	0,1 s	32 sec	24 T	10^{8} J	10^{13} J
10^{12}	0,2 ms	0,01 s	3 sec	2,4 T	10^{7} J	10^{12} J
10^{13}	0,02 ms	1 ms	0,3 sec	6 h	10^{6} J	10^{11} J

Zum Vergleich: Alter der Erde 10^9 Jahre

Wie lang muss ein Schlüssel sein?

- Abhängig von der Beantwortung der Fragen:
- Wie wertvoll sind Ihre Daten?
- Wie lange müssen sie geschützt werden?
- Über welche Ressourcen verfügen Ihre Gegner?
- Grundlegende Überlegung:
  Aufwand (Knacken) vs. Wert (Inhalt)
  Zeit (Knacken) vs. Aktualität (Inhalt)

Digitale Signatur mit Hashwerten



Digitale Signatur

- algorithmisches Verfahren ermittelt Authentikator, der Bestandteil der digitalen Nachricht wird („Prüfsumme“)
- geheimer Schlüssel(teil) des Autors (“Signaturschlüssel”) für Erzeugung
- öffentlicher Schlüssel(teil) für Überprüfung des Authentikators
- Beleg für Authentizität, Integrität, Verbindlichkeit der Nachricht gegenüber Dritten, für jedermann nachvollziehbar

Digitale Signatur: Funktionsweise

- **Sender** verschlüsselt seine Nachricht mit seinem Private Key, Hashing-Verfahren
- Empfänger entschlüsselt mit Public Key des **Senders**
- Dokument ist nicht authentisch/integer, wenn Entschlüsselung fehlschlägt

Digitale Signatur - Probleme

- Nichtabstreitbarkeit des Empfangs
- Lösung: Digital unterschriebene Bestätigung des Empfängers
- Verfahren: Digital Signature Standard (DSS)

Digitale Signatur - Probleme

- Woher weiß man, dass ein Schlüssel authentisch ist?
- Lösung: Digitale Signatur für Schlüssel (Zertifikat) durch Zertifizierungsstelle (Certification Authority - CA)
- bestätigt die Bindung des Schlüssels an Person durch Zertifikat (ähnlich Personalausweis)

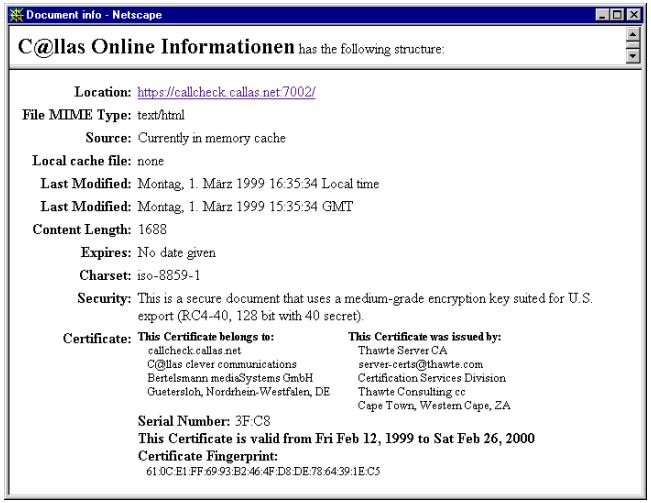
Digitale Signatur - Probleme

- Woher kennt man die öffentlichen Schlüssel eines Benutzers?
- Lösung: Durch Übermittlung vom Benutzer oder Zentrales Key-Verzeichnis
- Verfahren: integriert in Directory Services (LDAP), NAB

Digitale Signatur - Probleme

- Wer soll die Schlüssel generieren?
- Lösung: Trust-Center
  TeleSec (Deutsche Telekom AG), D-Trust (Debis, Bundesdruckerei), TC-Trust (Commerzbank), WWUCA etc.
- Wurzel-Trust-Center: Regulierungsbehörde für Telekom und Post (REGTP)
- Signaturgesetz (SigG): § 5 Erzeugung und Speicherung von Signaturschlüsseln und Identifikationsdaten

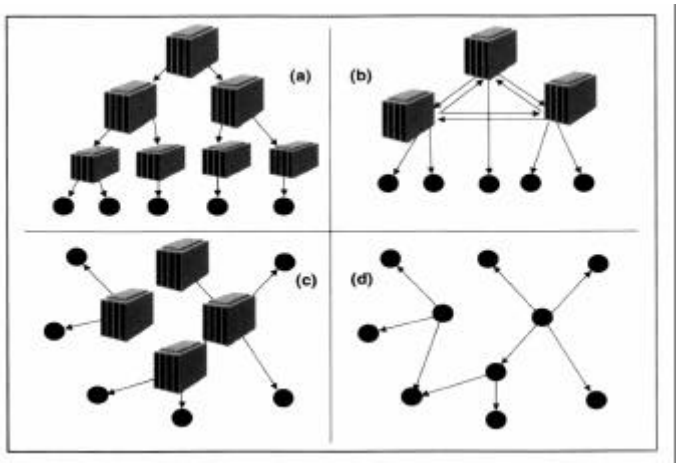
Beispiel für Zertifikat



konkrete Verfahren zur Verschlüsselung

OSI-Schicht	Sicherungsverfahren
Anwendungsschicht	• Privacy Enhanced Mail (PEM) • Secure MIME (S/MIME) • Secure HTTP (SHTTP) • Secure Electronic Transaction (SET) • Pretty Good Privacy (PGP)
Transportschicht	• Secure Socket Layer (SSL)
Vermittlungsschicht	IP Security Protocol mit den Bestandteilen • Authentication Header (AH) • Encapsulated Security Payload (ESP)

Vertrauensnetze - PKI



PGP

- nutzt RSA-Verfahren
- zur Verschlüsselung und digitalen Unterschrift
- Funktionen zur Schlüsselverwaltung
- auch zur Verschlüsselung von Dateien geeignet
- siehe auch:
  www.uni-muenster.de/ZIV/PGP/welcome.htm

SSL

- Ab 1994 von Netscape entwickelt,
- z.Z. häufigstes Sicherungsverfahren (Banken, Onlineshops), in vielen Browsern integriert
- Nutzt symmetrische und asymmetrische Verschlüsselung
- Webseiten:
  - https: statt http:
  - Symbole: Schlüssel (Navigator) bzw. Vorhängeschloss (IE)
  - Warnung des Browsers (sofern so konfiguriert)

Literaturhinweise

- *Kryptologie*
  Wobst, R.: Abenteuer Kryptologie - Methoden, Risiken und Nutzen der Datenverschlüsselung, 2. Auflage, Bonn/Reading 1998
- *Firewalls (Grundlagen,Produkte)*
  Strobel, S.: Firewalls für das Netz der Netze: Sicherheit im Internet, Heidelberg 1997
- *Internet und Sicherheit (Übersicht)*
  Fuhrberg, K.:Internet-Sicherheit: Browser, Firewalls und Verschlüsselung, München/Wien 1998
- *Internet und Sicherheit (detailliert)*
  Kyas, O.: Sicherheit im Internet, 2. Auflage, Bonn 1998
- *SSL*
  Kollakowski, M. / Bensberg, F.: *Sichere Datenübertragung mit SSL*

SSL-Check