DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ
BADEN-WÜRTTEMBERG

Hinweise
zu
Internet und Datenschutz

Stand: 1. März 2006

Der Landesbeauftragte für den Datenschutz in Baden-Württemberg
Urbanstraße 32
70182 Stuttgart
Telefon 0711/615541-0
Telefax 0711/615541-15
E-Mail: poststelle@lfd.bwl.de
(Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.)
PGP-Fingerprint: A5A5 6EC4 47B2 6287 E36C 5D5A 43B7 29B6 4411 E1E4
Homepage: www.baden-wuerttemberg.datenschutz.de

Inhaltsverzeichnis

---

1. Was ist das Internet?

Das Internet ist ein weltweites Computernetz, das nicht nur von Unternehmen, Forschungseinrichtungen und Behörden, sondern auch von vielen Millionen Privatpersonen genutzt wird, um Informationen auszutauschen, abzurufen oder der Öffentlichkeit zum Abruf anzubieten. Die Internet-Teilnehmer können dazu unterschiedlichste Kommunikationsdienste nutzen. Gebräuchlich sind insbesondere:

- World Wide Web (WWW)
  Dieser Dienst ermöglicht es, Texte, Bilder und Videoanimationen in ansprechender Form im Internet zum Abruf bereitzustellen. Jede WWW-Seite kann Verweise (sog. Links) auf andere WWW-Seiten enthalten, die mitunter auf ganz anderen Computern gespeichert sind. Der Nutzer kann einen solchen Link mit der Maus anklicken und so von einer Seite zu einer anderen und von einem Computer zu einem anderen gelangen. Zum Teil sind mit einzelnen WWW-Seiten auch ausführbare Programme (sog. aktive Inhalte) verbunden, die gleichzeitig mit dem Seiteninhalt auf den PC des Nutzers geladen und automatisch gestartet werden.
- Elektronische Post (E-Mail)
  Diese ermöglicht den Versand von Texten, Tabellen, Programmen oder sonstigen Dokumenten an andere Internet-Nutzer.

- Dateiübertragung (Filetransfer)
  Damit lassen sich Dateien zwischen Computern austauschen. Ein Internet-Teilnehmer kann damit zum Abruf bereitgestellte Dateien von einem entfernten Computer auf seinen eigenen kopieren oder selbst Dateien zum Abruf bereitstellen.
- Terminaldienst (Telnet)
  Mit Hilfe des Terminaldienstes kann man sich an einem räumlich entfernten Computer anmelden und, soweit es die Benutzerberechtigungen zulassen, die auf diesem Computer zur Verfügung stehenden Dialogverfahren nutzen.
- News-Foren/Usenet-News
  Dieser Dienst stellt mit seinen zahlreichen themenbezogenen Rubriken, den sog. Foren, ein elektronisches "Schwarzes Brett" dar. In der Regel kann hierbei jeder Teilnehmer alle Beiträge lesen, die in den einzelnen Foren stehen und sich mit eigenen Beiträgen, etwa Fragen oder Kommentaren zu früheren Mitteilungen, an der weiteren Diskussion beteiligen. Diese Beiträge sind ihrerseits wieder für alle Internet-Teilnehmer les- und auswertbar.
- Dateifreigabe-Dienst (NetBIOS über TCP/IP)
  Dieser Dienst macht es möglich, Teilnehmern im lokalen Netz, aber auch im Internet, Zugriff auf Dateien zu gewähren, die auf einem lokalen Computer gespeichert sind. Umgekehrt kann man mit diesem Dienst auch auf freigegebene Dateien zugreifen, die auf am Internet angeschlossenen Computern gespeichert sind. Viele der im Internet realisierten Tauschbörsen nutzen beispielsweise diesen oder vergleichbare Dienste.
- Internet-Telefonie (Voice over IP, VoIP)
  Leistungsfähige Übertragungswege vorausgesetzt, kann man über Internet einen Sprachtelefondienst realisieren.
- Internet Relay Chat
  In sog. "Chat-Rooms" können Internet-Nutzer, die gleichzeitig im Internet aktiv sind, schriftlich in Echtzeit miteinander kommunizieren.
- Messaging Dienste
  Diese Dienste ermöglichen es einem Internet-Nutzer, zu erkennen, ob ausgewählte andere Internet-Nutzer (z. B. private Bekannte oder dienstliche Ansprechpartner) zur gleichen Zeit mit dem Internet verbunden sind. Diese können dann untereinander schriftliche Nachrichten austauschen.

2. Datenschutzrisiken

Wer das Internet nutzt, sollte sich darüber im Klaren sein, dass dies mit verschiedenen Datenschutzrisiken einhergeht:

2.1 Sicherheitsmängel der Internet-Übertragungsstandards

Bei der Festlegung der im Internet zu verwendenden Übertragungsstandards spielten Sicherheitsaspekte bislang nur eine untergeordnete Rolle. Unter dem Oberbegriff IP Security Protocol (IPSEC) wurden zwar mittlerweile auch Übertragungsstandards erarbeitet, die eine vertrauliche und unverfälschte Kommunikation unterstützen sollen, aber gegenwärtig dominieren noch die traditionellen Übertragungsstandards, die ohne ergänzende Sicherheitsmaßnahmen keinen verlässlichen Schutz vor Angriffen bieten können. Beispielhaft seien hier folgende grundlegende Sicherheitsdefizite genannt:

- Kein Schutz vor Verfälschung der IP-Adressen
  Jeder an das Internet angeschlossene Computer hat eine weltweit eindeutige Adresse, die sog. IP-Adresse. Verschickt nun ein Rechner ein Datenpaket, so wird seine IP-Adresse dort automatisch als Absenderangabe eingetragen. Wer es aber darauf anlegt, kann diese Absenderangabe fälschen. Da in manchen Fällen allein anhand der Absenderadresse entschieden wird, ob jemand die von einem Computer angebotenen Kommunikationsdienste nutzen darf oder nicht, kann die Adressverfälschung dazu führen, dass der Absender auf dem Zielrechner unter Umständen auch Daten lesen, verändern oder auf seinen Computer herunterladen kann, obwohl ihm dies bei unverfälschter Absenderangabe technisch verwehrt wäre.
- Konzeptionelle Mängel beim Austausch von Routing-Informationen
  Die als Netzknoten verwendeten Router informieren sich teilweise gegenseitig über neu am Internet angeschlossene Computer oder Netzwerke. Wenn ein Router auf diese Weise Informationen darüber erhält, auf welchem Weg er künftig die an einen Computer adressierten Datenpakete weiterleiten soll, so übernimmt er diese Informationen, ohne zu prüfen, ob der Absender dieser Informationen vertrauenswürdig ist. Damit besteht die Gefahr, dass jemand durch Verbreiten falscher Routing-Informationen Daten, die eigentlich für einen anderen Empfänger bestimmt waren, an seinen eigenen Computer umleitet.

– Konzeptionelle Mängel des Domain Name Services (DNS)
  Dieser Dienst ordnet die numerischen IP-Adressen den häufig zur Bezeichnung von Computern benutzten Namen, z. B. "www.datenschutz.de", zu und umgekehrt. Da sich, wenn man eine solche DNS-Anfrage stellt, nicht sicherstellen lässt, dass der DNS-Server, der die Antwort gibt, vertrauenswürdig ist, lässt sich nicht ausschließen, dass die Antwort auf die eigene Anfrage von einem Server stammt, auf dem bestimmten Computernamen absichtlich falsche IP-Adressen zugeordnet werden. Zudem bieten DNS-Server den Domain-Inhabern oft die Möglichkeit, die dort registrierten Daten online zu ändern. In der Vergangenheit gab es zum Teil gravierende Lücken bei der Prüfung der Zugriffsberechtigung mit der Folge, dass die DNS-Einträge hätten verfälscht werden können. In letzter Konsequenz bedeutet dies, dass Aufrufe bestimmter Internet-Adressen nicht zum rechtmäßigen Anbieter, sondern gezielt auf einen anderen Web-Server umgelenkt werden könnten.

2.2 Aus dem Internet stammende Schadensprogramme

Bei der Nutzung einer Reihe von Diensten wie z. B. E-Mail, World Wide Web oder FTP besteht das Risiko, dass Computerviren, sog. Trojanische Pferde oder sonstige Schadensprogramme auf den eigenen Computer gelangen, deren Ausführung Daten von eigenen Computer unbemerkt an Empfänger im Internet sendet (sog. Spyware), die Hintertüren öffnen können, durch die Angreifer aus dem Internet Zugang zum eigenen Computer erlangen (Trojanische Pferde) oder die unerwünschte Veränderungen an gespeicherten Daten und Programmen bis hin zur Löschung ganzer Datenbestände hervorrufen können (sog. Malware). Ein Schadensprogramm kann aber mitunter auch bestimmte Daten der lokalen Festplatte auslesen und ohne Wissen des Computer-Nutzers über Internet an einen bestimmten Empfänger senden. Solche Schadensprogramme können auf folgende Weise auf einen Computer gelangen:

– Sorgloser Umgang mit empfangenen E-Mails
  Programme, die zur Textverarbeitung, Tabellenkalkulation und für andere Aufgaben eingesetzt werden, bieten vielfach die Möglichkeit, bestimmte regelmäßig wiederkehrende Arbeitsabläufe mit Hilfe eines Makro-Programms zu automatisieren. Ein solches Makro-Programm kann nicht nur nützliche, sondern auch unerwünschte Funktionen oder gar ein Virus enthalten. Problematisch ist dabei, dass jemand, der eine solche Datei erhält, nicht unmittelbar erkennen kann, ob sie ein Makro-Programm enthält oder nicht. Öffnet

man die Datei, um sie zu lesen, so kann dies bereits der Auslöser zum Start des Schadensprogramms sein.

- Anklicken von WWW-Seiten, die mit aktiven Inhalten verbunden sind
  Beim Aufruf einer WWW-Seite kann eine aktive Komponente, d. h. ein ausführbares Programm, etwa in Form eines JavaScript-Programms oder eines ActiveX-Controls aus dem Internet auf den eigenen Computer geladen und dort ohne weiteres Zutun des Nutzers gestartet werden. Sofern die dafür vorgesehenen Sicherheitsmechanismen nicht korrekt funktionieren, können auch Java-Applets Schadenswirkungen entfalten. Diese Applets können, wie die ActiveX-Controls, ebenfalls im Rahmen der WWW-Nutzung auf den lokalen Arbeitsplatzcomputer des Internet-Nutzers gelangen.
- Download eines Programms
  Schadensprogramme können übertragen werden, wenn ein Internet-Nutzer ein Programm per Filetransfer aus dem Internet auf seinen Computer herunterlädt, installiert und anschließend startet. Es kann sein, dass es als nützliches Hilfsmittel angepriesen wird, es kann aber neben oder anstelle der gewünschten eine unerwünschte, möglicherweise schadensstiftende Funktion haben (Trojanisches Pferd).

2.3 Hohe Zahl potentieller Angreifer

Angesichts der sehr großen Zahl von Internet-Teilnehmern muss auch von einer hohen Zahl potentieller Angreifer ausgegangen werden. Diese können Sicherheitslücken gängiger Betriebssysteme, Browser oder sonstiger Programme ausnutzen und mit Hilfe ihres Computers im Internet systematisch nach anderen Computern suchen, die die entsprechende Sicherheitslücke aufweisen. Das kann mitunter dazu führen, dass die Angreifer unbefugt auf personenbezogene Daten zugreifen.

2.4 Große Angriffsfläche

Die Größe des Netzes bringt nicht nur eine hohe Zahl von potentiellen Angreifern mit sich, sondern bietet diesen zudem schon rein quantitativ wesentlich mehr Angriffspunkte als ein kleines Netz. Wird eine Sicherheitslücke des Internets oder der Systemsoftware von gängigen, am Internet angeschlossenen Computern bekannt, ist sofort eine Vielzahl von Computern bedroht.

2.5 Abhören von Informationen

Da sämtliche Daten im Internet - ohne Einsatz entsprechender Zusatzprodukte - unverschlüsselt übertragen werden, besteht die Gefahr, dass sie unterwegs von Personen gelesen, gespeichert und genutzt werden, für die sie nicht bestimmt sind. Gefährdet sind nicht nur die jeweils übertragenen Inhaltsdaten, z. B. der Inhalt elektronischer Postsendungen, sondern auch Benutzerkennungen und Passwörter, die von manchen Diensten, wie z. B. Telnet oder FTP, im Klartext übertragen werden. Unberechtigte Zugriffe auf übertragene Daten können dabei - technisch gesehen - sowohl an Übertragungswegen (z. B. Kabeln oder Richtfunkstrecken) als auch an den Netzknoten ansetzen und entweder von deren Betreibern oder von Dritten, z. B. Hackern, durchgeführt werden, denen es gelingt, die Sicherheitsmaßnahmen der Betreiber zu überwinden. Diese Situation ist im Internet besonders problematisch, da der Absender in der Regel nicht weiß, auf welchem Weg die Daten zum Empfänger fließen. Mitunter kann es nämlich vorkommen, dass Absender und Empfänger zwar in der gleichen Stadt wohnen, die Daten aber gleichwohl beispielsweise über Netzknoten in den USA übertragen werden. Unbekannt bleibt außerdem in der Regel, wer die Netzknoten betreibt, über die die Daten fließen, welche Datenschutzvorschriften für diese Betreiber gelten und wie vertrauenswürdig die Betreiber sind.

2.6 Gefahr der Bildung von Persönlichkeitsprofilen

Sowohl die im Internet veröffentlichten Inhaltsdaten (z. B. Inhalt von Web-Seiten) als auch die zur technischen Übermittlung der Inhaltsdaten verwendeten Verbindungsdaten (diese lassen erkennen, welcher Computer über welchen Internet-Dienst Verbindung mit welchem anderen Computer aufnimmt) ermöglichen die Erstellung von Persönlichkeitsprofilen.

– Für die Erstellung von Persönlichkeitsprofilen auf der Grundlage von Inhaltsdaten sind vor allem die im Internet verfügbaren Suchmaschinen von Bedeutung. Diese sind in der Lage, unterschiedlichste WWW-Seiten sowie Beiträge in News-Gruppen zu ermitteln, in denen ein bestimmter Name oder eine E-Mail-Adresse vorkommt. Einzelne Suchmaschinen verfügen zugleich über ein Archiv, in dem WWW-Seiten oder Beiträge aus News-Foren monate- oder jahrelang gespeichert werden. Wer einmal eine Nachricht an eine News-Gruppe gesandt hat oder über wen personenbezogene Daten im World Wide Web veröffentlicht sind, der muss daher damit rechnen, dass alle diese Informationen auch lange nach der Veröffentlichung

noch mit Hilfe der Suchmaschinen und Archive zusammengeführt werden können.

- Nutzt ein Teilnehmer einen Internet-Dienst, fallen beispielsweise in den Netzknoten Verbindungsdaten an, ohne dass er dies bemerkt. Die Verbindungsdaten sind für die Dauer der jeweiligen Verbindung erforderlich, um die Daten im Netz übertragen und den richtigen Endgeräten zuordnen zu können. Nach dem Ende der Verbindung werden sie allenfalls noch für Abrechnungszwecke benötigt. Werden die Verbindungsdaten nach dem Ende der jeweiligen Verbindung dauerhaft gespeichert, lässt sich aus ihnen in vielen Fällen entnehmen, wer wann wo auf welche Angebote im Internet zugegriffen oder wer mit wem kommuniziert hat. Technisch machbar wäre, all diese einzelnen Datenspuren zu umfassenden Persönlichkeitsprofilen zusammenzuführen. Zwar fordern das Teledienstedatenschutzgesetz und der Mediendienste-Staatsvertrag von deutschen Diensteanbietern, dass diese die Verbindungsdaten unmittelbar nach Beendigung der jeweiligen Dienstenutzung löschen müssen, sofern die Daten nicht noch für Abrechnungszwecke benötigt werden. Für ausländische Diensteanbieter gelten diese Regelungen jedoch nicht.

2.7 Risiken spezieller Internet-Dienste

Neben den bislang genannten allgemeinen, mit der Internet-Nutzung verbundenen Risiken, bergen fast alle gebräuchlichen Dienste spezifische Risiken. Dazu nur einige Beispiele:

- FTP:
  Bei schlecht konfigurierten Servern besteht das Risiko, dass Internet-Teilnehmer Daten von dem jeweiligen Server abrufen können, die gar nicht zum Abruf bestimmt sind.
- NetBIOS über TCP/IP:
  Hierbei besteht das Risiko, dass Benutzer Dateien nur im lokalen Netz freigeben wollen, die hierzu vorgenommenen Einstellungen jedoch unter Umständen auch einen Zugriff über das Internet ermöglichen.
- Finger:
  Dieser Dienst ermöglicht es, Benutzerkennungen und andere Informationen über die an einem Computer angemeldeten Benutzer zu erfahren. Ist dieser Dienst unbeschränkt nutzbar, so können Angreifer auf diesem Weg gültige Benutzerkennungen erfahren.

Eine umfassende Übersicht über Sicherheitsrisiken der meisten der unter Nr. 1 erwähnten sowie einer Reihe weiterer Internet-Dienste findet sich in der im Auftrag des BSI erstellten Studie "Gesicherte Verbindungen von Computernetzen mit Hilfe einer Firewall", abrufbar unter

www.bsi.bund.de/literat/studien/firewall/fwstud.htm

3. Was ist zu tun?

Auf Grund der beschriebenen Risiken ist beim Umgang mit dem Internet stets besondere Sorgfalt geboten:

- Wer einen eigenen Computer oder ein eigenes Netzwerk mit dem Internet koppelt, muss ausreichende Sicherheitsmaßnahmen ergreifen, um unberechtigte Zugriffe von Internet-Teilnehmern auf interne Daten zu verhindern.
- Wer personenbezogene oder andere schutzbedürftige Daten über das Internet überträgt, muss Schutzmaßnahmen gegen deren unberechtigte Kenntnisnahme und Manipulation ergreifen.
- Wer im World Wide Web surft, sollte wissen, was er tun kann, um unerwünschte Datenspuren zu vermeiden.
- Wer Informationsdienste im Internet anbietet, muss sowohl bei der Auswahl der veröffentlichten Inhalte als auch beim Umgang mit den bei der Nutzung anfallenden Verbindungsdaten auf die einschlägigen Datenschutzvorschriften achten.

4. Schutz eigener Computer vor Angriffen aus dem Internet

In dieser Frage ist zu unterscheiden, ob man ein Netzwerk an das Internet anschließen will oder nur einzelne PC.

4.1 Schutz vor Angriffen auf ein eigenes Computernetzwerk

Angesichts der zahlreichen Risiken, die der Anschluss eines Computernetzwerks an das Internet mit sich bringt, ist es unverzichtbar, vor der Realisierung eines solchen Anschlusses ein Sicherheitskonzept mit folgenden Bestandteilen zu erarbeiten:

- Es gibt an, welche Mitarbeiter und welche Organisationseinheiten welche Internet-Dienste benötigen (Kommunikationsbedarf).
- Es stellt dar, wie das an das Internet anzuschließende interne Netz strukturiert ist.

- Es dokumentiert und bewertet die mit der Nutzung der erforderlichen Internet-Dienste einhergehenden Risiken und die drohenden Schäden.
- Es legt dar, welche technischen und organisatorischen Maßnahmen erforderlich sind, um den Risiken entgegenzuwirken.

Nach Inbetriebnahme des gesicherten Internet-Anschlusses ist darauf zu achten, dass das Konzept regelmäßig überprüft und bei Bedarf den veränderten Nutzungsanforderungen sowie neu aufgetretenen Sicherheitslücken angepasst wird.

Der Konzeption der Sicherheitsmaßnahmen sind folgende Ziele zugrunde zu legen:

a) Filterung
   Die technischen Kommunikationsmöglichkeiten der einzelnen Nutzer sind auf den ermittelten, notwendigen Kommunikationsbedarf zu beschränken.

b) Verbergen der internen Netzstruktur
   Informationen über die Struktur des internen Netzes, z. B. Namen interner Computer, Informationen über registrierte Software, freigegebene Festplatten-Verzeichnisse, müssen gegenüber dem Internet verborgen werden.

c) Protokollierung
   Sicherheitsrelevante Ereignisse sind zu protokollieren. Wichtig ist daneben, dass Systemverwalter, etwa durch Alarmmeldungen, umgehend über sicherheitsrelevante Ereignisse informiert werden.

Hard- und Softwarekomponenten, die an einer zentralen Übergangsstelle zwischen zwei Netzen, für die unterschiedliche Sicherheitsanforderungen gelten (z. B. zwischen internem Netz und dem Internet), angesiedelt sind und die Schutzfunktionen für mindestens eines der Netze bieten, werden als **Firewall** bezeichnet.

Zur technischen Umsetzung der genannten Firewall-Grundfunktionen ist noch Folgendes zu sagen:

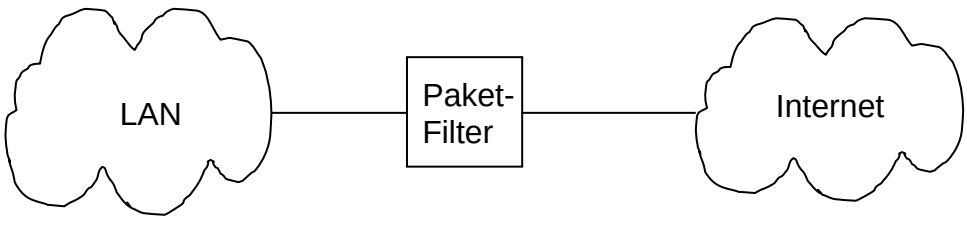
zu a) Filterung
   Um den Datenaustausch mit dem Internet auf das zulässige Maß beschränken zu können, muss die Firewall eine Filterfunktion bieten: Anhand hinterlegter Regeln entscheidet sie, welche Datenpakete sie

durchlässt und welche sie abweist. Die Filterung sollte dabei in jedem Fall nach dem Prinzip organisiert sein, dass alles verboten ist, was nicht ausdrücklich erlaubt wurde. Die Filterung kann auf drei Ebenen erfolgen:

- Statische Paketfilterung:
  Die Filterung erfolgt auf den Schichten 3 und 4 des OSI-Modells für offene Kommunikation. Für die Filterung stehen die Adressen der an der Kommunikation beteiligten Computer, die Port-Nummern sowie die Information über das verwendete Übertragungsprotokoll zur Verfügung.
- Dynamische Paketfilterung:
  Abhängig vom Kommunikationsverlauf kann bei der dynamischen Filterung eine Situations- bzw. kontextbasierte Filterung erfolgen. Damit lässt sich beispielsweise festlegen, dass nur dann ein Datenpaket eines externen Computers ins interne Netz durchgelassen wird, wenn genau dieser externe Computer zuvor mit einem Datenpaket spezieller Art von einem internen Computer angesprochen wurde.
- Anwendungsfilterung:
  Gegenüber einem Paketfilter kann ein Anwendungsfilter (Application Gateway) alle Informationen heranziehen, die auf der Anwendungsebene (OSI-Schicht 7) vorhanden sind, insbesondere Benutzerkennungen.

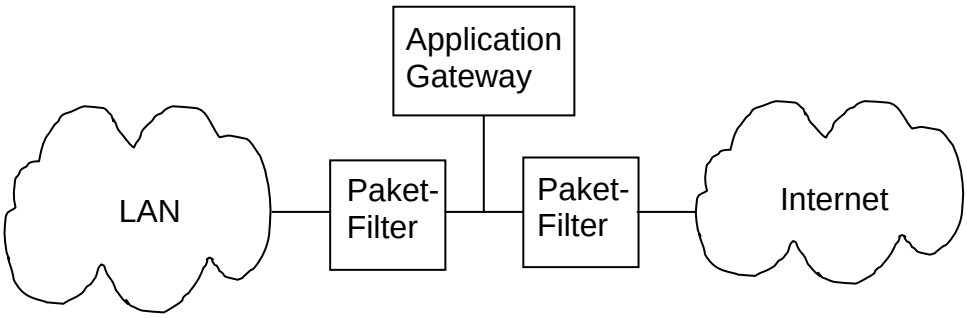
Damit lassen sich unterschiedliche Firewall-Architekturen realisieren:

- Ausschließlicher Einsatz eines Paketfilters:



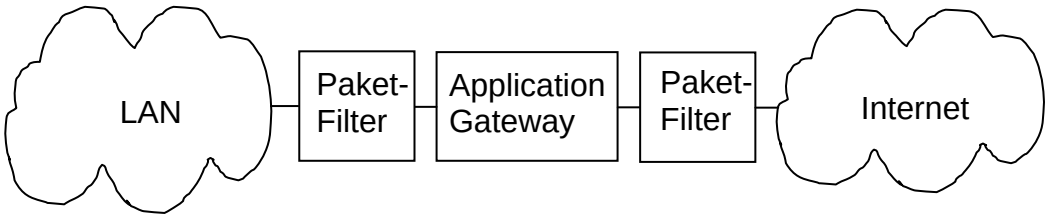
  Statische Paketfilter dieser Art werden häufig durch Router realisiert.

– Screened Subnet:
  Hierbei handelt es sich um eine Kombination aus einem Application Gateway und einem oder zwei Paketfiltern, die ein separates Teilnetz bilden.



  Die Filterregeln der Paketfilter müssen dabei so gewählt werden, dass die zwischen LAN und Internet ausgetauschten Datenpakete stets über den Gateway-Rechner geleitet werden.

– Dual Homed Gateway:



  Ein Dual Homed Gateway besteht aus dem Application Gateway, das auf einem mit zwei Netzwerkanschlüssen ausgestatteten Computer installiert ist und das durch einen oder, wie in der Abbildung dargestellt, durch zwei Paketfilter flankiert wird. Der Gateway-Computer muss dabei so konfiguriert sein, dass kein Datenpaket unverändert in das interne Netz gelangen kann. Dies lässt sich durch Abschalten des IP-Forwardings realisieren.

zu b) Verbergen der internen Netzstruktur
  Um die intern verwendeten IP-Adressen nach außen hin verbergen zu können, ist es erforderlich, in der Firewall eine Adressumsetzung (Network Adress Translation NAT) vorzunehmen. Die Adressen interner

Rechner werden dabei durch die Adresse der Firewall ersetzt. Darüber hinaus kann es je nach Architektur der Firewall notwendig sein, auch die Adressen externer Server etwa für E-Mail oder World Wide Web bekannt zu machen.

zu c) Protokollierung

Neben der Ausgabe von Warnmeldungen bei Ereignissen von besonderer sicherheitsrelevanter Bedeutung ist eine aussagekräftige Protokollierung ein ganz wesentliches Element einer Firewall. Die Protokollierung kann einen Beitrag dazu leisten, Angriffe wenigstens im Nachhinein noch feststellen und darauf reagieren zu können. Insbesondere sollten folgende sicherheitsrelevante Ereignisse von der Firewall protokolliert werden:

- abgewiesene Verbindungsversuche (z. B. Versuche, auf nicht freigegebene IP-Adressen oder Port-Nummern zuzugreifen);
- Hinweise auf systematische Eindringversuche (z. B. Nachweis des Einsatzes von Port-Scannern);
- Versuche, vom Internet aus Datenpakete durch die Firewall zu schleusen, die als Absenderangabe die Internet-Adresse eines internen Computers tragen (sog. IP-Spoofing-Attacken);
- erfolgreiche und abgewiesene Versuche des Systemverwalterzugriffs auf Firewall-Komponenten.

Bei der Planung einer Firewall sollte auf folgende weitere Punkte besonderes Augenmerk gerichtet werden:

4.1.1 Nicht allein auf statische Paketfilterung vertrauen

Statische Paketfilterung kann die Dienstenutzung zwar beschränken und die Verbreitung von Informationen über das interne Netz eindämmen. Gleichwohl weisen Paketfilter systembedingte Schwächen auf, die sich nicht ausräumen lassen:

- Eine benutzerbezogene Filterung ist nicht möglich.
- Die Abschottung des internen Netzes gelingt nicht vollständig, denn alle Datenpakete, die ein Paketfilter von innen nach außen passieren lässt, tragen nach wie vor interne Adressen als Absenderadressen. Auf diese Weise werden die Adressen interner Computer im Internet bekannt.

- Die von Paketfiltern erstellten Protokolldaten lassen sich oft nur mit Mühe nachvollziehen.

4.1.2 Application Gateways einsetzen

Die genannten Schwächen der Paketfilter lassen sich durch den Einsatz eines Application Gateways ausräumen, denn:

- Berechtigungen zur Nutzung einzelner Dienste lassen sich für jeden Benutzer individuell festlegen.
- Zum Internet hin müssen nur der Gateway-Rechner sowie etwaige für die Nutzung aus dem Internet bestimmte Server bekannt gemacht werden. Informationen über die übrige interne Netzstruktur lassen sich auf diesem Weg vollständig verbergen.
- Eine aussagekräftige Protokollierung ist möglich.

Um diese Vorteile in der Praxis voll ausschöpfen zu können, ist es wichtig, die Möglichkeiten zur Vergabe differenzierter Zugriffsberechtigungen restriktiv zu verwenden und Protokolldateien regelmäßig auszuwerten.

4.1.3 Mehrfachauslegung von Filtern

Sowohl bei der eingesetzten Hard- und Software als auch bei der Implementierung der Filterregeln können Fehler auftreten. Daher empfiehlt es sich, sicherheitsrelevante Funktionen einer Firewall nicht bloß einfach, sondern mehrfach, und zwar auf technisch unterschiedliche Art und Weise, zu realisieren. Bei dieser Vorgehensweise wird ein Angreifer aus dem Internet, der einen Fehler einer Firewall-Komponente ausnutzen kann, noch durch eine zweite Barriere davon abgehalten, ins interne Netz einzudringen.

4.1.4 "Datenschleichwege" versperren

Der mit der Einrichtung einer Firewall angestrebte Schutz stellt sich nur dann ein, wenn tatsächlich alle Verbindungen zwischen internen und externen Computern über die Firewall laufen. Das bedeutet, dass beispielsweise auch Modem- oder ISDN-Verbindungen nicht an der Firewall vorbei geführt werden dürfen. Um dem Risiko der Einrichtung und Nutzung derartiger "Datenschleichwege" zu begegnen, muss jede Stelle, die eine Firewall betreibt, ihre Mitarbeiterinnen und Mitarbeiter klipp und klar darauf hinweisen, dass es unzulässig ist, solche Verbindun-

gen an der Firewall vorbei herzustellen. Einen gewissen Schutz vor unerlaubten Kommunikationsverbindungen zwischen dem internen Netz und dem Internet bietet in diesem Zusammenhang die Verwendung sog. nicht-offizieller IP-Adressen für Rechner des internen Netzes. Hierbei handelt es sich um Adressen, die ausdrücklich für die Verwendung in nicht allgemein zugänglichen Netzen vorgesehen sind und die in der Regel im Internet nicht weitergeleitet (geroutet) werden.

4.1.5 Administration sicherheitsrelevanter Komponenten

Zu einem datenschutzgerechten Firewall-Betrieb gehört, dass sich Unberechtigte keine Informationen über deren Administration verschaffen können und auch keine Möglichkeit einer missbräuchlichen Nutzung von Administrationsfunktionen besteht. Dies erfordert unter anderem,

- dass auch für den Administrationszugang eine strenge Zugriffskontrolle realisiert wird, die den üblichen Anforderungen an Passwörter gerecht wird. Näheres zur Gestaltung eines datenschutzgerechten Passwortschutzes ist unserem Merkblatt zum Umgang mit Passwörtern unter

  www.baden-wuerttemberg.datenschutz.de/service/lfd-merkblaetter/passwort.htm

  zu entnehmen;
- dass ferner eine Terminalbeschränkung für die Administration existiert, die sicherstellt, dass eine Anmeldung als Firewall-Administrator nur von wenigen ausgewählten Arbeitsplätzen aus möglich ist und
- dass ein Abhören der zur Administration benutzten Daten verhindert wird. Dies lässt sich beispielsweise durch Verschlüsselung erreichen oder dadurch, dass durch Segmentierung des internen Netzes sichergestellt wird, dass am Teilnetz, durch das die Administrationsdaten fließen, nur Administrations-Arbeitsplätze angeschlossen sind.

4.1.6 Schutz vor Schadensprogrammen

Beim Download von Programmen oder beim Bearbeiten elektronischer Post-Sendungen, die aus dem Internet stammen, besteht das Risiko, dass diese Schadensfunktionen enthalten. Zur Verringerung dieser Gefahr ist der Einsatz von Virenschutzprogrammen erforderlich, die

möglichst in die Firewall integriert werden sollten. Zum Schutz vor schadensstiftenden Funktionen in Java-Applets, JavaScript-Programmen oder ActiveX-Controls ist Folgendes zu beachten:
Zur Vermeidung unberechtigter Zugriffe auf lokal gespeicherte Daten verfügt Java über Sicherheitsmechanismen nach dem sog. Sandbox-Modell, die beispielsweise dafür sorgen, dass Schreib- und Lesevorgänge von aus dem Internet erhaltenen Applets auf bestimmte Verzeichnisse der lokalen Festplatte beschränkt bleiben. In der Vergangenheit konnte dieses Sicherheitskonzept allerdings zeitweise aufgrund fehlerhafter Programmierung unterlaufen werden. Bei der Ausführung von JavaScript-Programmen oder ActiveX-Controls gibt es im Gegensatz dazu keine Möglichkeit, deren Zugriffsmöglichkeiten zu begrenzen. Ein Benutzer kann zwar dafür sorgen, dass nur solche ActiveX-Controls zur Ausführung kommen können, die eine Zertifizierungsstelle digital signiert hat. Die Sicherheitsprobleme löst dies jedoch nicht: Eine digitale Signatur bescheinigt lediglich, dass der Hersteller des Controls bekannt ist und es beim Empfänger unverfälscht zur Ausführung kommt; sie sagt jedoch nichts über Inhalt und Funktionsweise des Programms aus. Wie ein Beispiel aus der Praxis belegt, können selbst signierte ActiveX-Controls eine unerwünschte Funktion enthalten. Vor diesem Hintergrund ist es geboten, auf die ActiveX-Funktionalität zu verzichten. Empfehlenswert ist daher, ein zentrales Filterprogramm einzusetzen, das ActiveX-Controls aus dem Datenstrom herausfiltert oder nur mit Browsern zu arbeiten, die die ActiveX-Technologie nicht unterstützen oder in denen diese Unterstützung abgeschaltet wurde. Entsprechend sollte auch verhindert werden, dass JavaScript-Programme ausgeführt werden. Da sich auch beim Umgang mit Java-Applets Risiken nicht restlos vermeiden lassen, empfiehlt sich auch hier ein restriktiver Umgang.

Abschließend ist darauf hinzuweisen, dass die Anbindung eines internen Netzes an das Internet in jedem Fall die Datenschutzrisiken für die im internen Netz gespeicherten Daten erhöht. Selbst wenn man eine nach allen Regeln der Kunst gestaltete Firewall einsetzt, lässt sich damit also lediglich die Zunahme der Risiken begrenzen.

4.2 Schutz einzelner PC, die über einen unmittelbaren Internet-Zugang verfügen

Nicht immer ist es notwendig, den Internet-Zugang für ein Netzwerk einzurichten, sondern es genügt, dies für einzelne PC zu tun. Der Internet-Anschluss wird in diesen Fällen in der Regel via Modem- oder ISDN-Verbindung direkt, d. h. ohne eine Firewall realisiert, die den in Nr. 4.1 genannten Anforderungen gerecht wird. Auch und besonders in diesen Fällen ist vor der Realisierung des Anschlusses zu prüfen, welche Risiken mit dem geplanten Anschluss einhergehen und wie sie minimiert werden können. In der Praxis sind zwei Arten des direkten Internet-Anschlusses anzutreffen: Zum einen gibt es die Fälle, in denen Stand-alone-PC ans Internet angeschlossen werden. Zum anderen gibt es PC, die zwar direkt mit dem Internet gekoppelt sind oder gekoppelt werden können, aber gleichzeitig oder wahlweise auch eine Verbindung zum internen Netz haben können.

4.2.1 Anschluss eines nicht vernetzten PC (Stand-alone-PC) an das Internet

Schließt man einen unvernetzten PC via Modem- oder ISDN-Verbindung an das Internet an, so besteht hierbei das Risiko, dass Internet-Teilnehmer auf schutzbedürftige Daten zugreifen können, die lokal auf dem PC gespeichert sind. Deshalb sollten auf einem derartigen PC möglichst keine personenbezogenen oder anderen schutzbedürftigen Daten gespeichert und verarbeitet werden. Um unberechtigten Zugriffen von Seiten des Internets technisch entgegenzuwirken, sollte darauf geachtet werden, dass keine Datei-Verzeichnisse oder gar der Inhalt ganzer Laufwerke für einen Zugriff über Netz freigegeben sind. Daten, die nicht für die Allgemeinheit bestimmt sind, können durch verschlüsselte Speicherung vor unberechtigter Kenntnisnahme geschützt werden. Im Übrigen sind auch bei einem mit dem Internet verbundenen Stand-alone-PC Maßnahmen zum Schutz vor Schadensprogrammen zu ergreifen. Hierzu ist ein Virenschutzprogramm einzusetzen und die Möglichkeit zur Ausführung von aktiven Inhalten zu unterbinden. Sollen auf dem PC auch schutzbedürftige Daten gespeichert werden, so ist zusätzlich der Einsatz eines darauf abgestimmten Firewallsystems (sog. Personal Firewall) erforderlich.

4.2.2 Anschluss von PC, die außer mit dem Internet auch mit einem internen Netz verbunden sein können

Der Anschluss von PC, die via Modem- oder ISDN-Verbindung direkt mit dem Internet und außerdem mit einem internen Netz verbunden sein können, ist mit besonderen Datenschutzrisiken verbunden:

- Bei dieser Anschlussart ist nicht nur der PC gefährdet, der über den Internet-Anschluss verfügt, sondern auch die übrigen, am lokalen Netz angeschlossenen Computer. Falls der PC gleichzeitig mit dem Internet und dem internen Netz verbunden sein kann, ist dieses Risiko größer als in dem Fall, in dem der PC entweder mit dem Internet oder dem internen Netz verknüpft ist. Aber auch dann ist nicht ausgeschlossen, dass beispielsweise ein Computervirus auf dem am Internet angeschlossenen PC gespeichert wird, und sich dieser im lokalen Netz ausbreitet, sobald der PC wieder daran angeschlossen wird.
- Ferner besteht bei dieser Anschlussart auch ein erhöhtes Risiko, dass Internet-Teilnehmer auf schutzbedürftige Daten zugreifen können. Da der PC, von dem aus das Internet genutzt wird, gelegentlich auch im lokalen Netz betrieben wird, sind mitunter einzelne Dateiverzeichnisse oder Laufwerke dieses PC für einen Zugriff über das lokale Netz freigegeben. Wird dieser PC dann mit dem Internet gekoppelt und die Freigabe nicht widerrufen, so besteht auch für Internet-Teilnehmer die Möglichkeit, auf die freigegebenen Daten zuzugreifen.

Aufgrund dieser spezifischen Risiken ist von einer Installation abzuraten, bei der ein PC sowohl an das Internet als auch an das lokale Netz angeschlossen werden kann.

4.3 Computerviren - ein hartnäckiges Problem

Computerviren sind zu einer erheblichen Bedrohung für die Computersicherheit geworden. Ständig entstehen neue Viren oder tauchen Varianten bereits bekannter Viren auf. Nicht selten sind innerhalb weniger Stunden nach dem ersten Auftauchen weltweit bereits viele Millionen Computer infiziert. Häufig trifft es Computer, die mit dem Betriebssystem Windows, gelegentlich auch in Kombination mit dem Programm Outlook, ausgestattet sind. Akut bedroht sind daher auch entsprechende Computer öffentlicher Stellen. Um zu illustrieren,

wie die Verbreitung eines solchen Virus vonstatten geht, hier ein Blick auf den "I-love-you"-Virus, der im Jahr 2000 weltweit große Schäden anrichtete: Seinerzeit landeten E-Mails mit dem Betreff "I love you" in einer Vielzahl elektronischer Postfächer. Der verlockenden Botschaft "Ich liebe dich" konnten Millionen Computernutzer nicht widerstehen, zumal es sich beim jeweiligen Absender der Mail um keinen Unbekannten handelte, sondern um jemanden, von dem man in der Regel bereits früher elektronische Nachrichten erhalten hatte. Sie öffneten die als Anhang zu dieser E-Mail versandte Datei, begierig darauf zu erfahren, was sich denn hinter der elektronischen Liebeserklärung verbirgt. Damit nahm dann das Unheil seinen Lauf. Die Datei enthielt, obwohl sie wie ein harmloser Text daherkam, ein sog. Makro-Programm, das nach dem Öffnen der Datei sofort ausgeführt wurde: Das Programm sandte Kopien der ursprünglichen "I-love-you"-Nachricht an alle Mail-Adressen, die der Empfänger in seinem Outlook-Adressbuch hinterlegt hatte. Die Lawine kam in Gang. Zudem löschte das Virus bestimmte Dateien.

Es ist unerlässlich, dass die für die Datenverarbeitung verantwortlichen Stellen Vorkehrungen gegen derartige Virusinfektionen treffen. Darüber hinaus muss aber auch jeder einzelne Internet-Nutzer für die Viren-Gefahren sensibilisiert werden und lernen, sich richtig zu verhalten. Ein Schaden entsteht nämlich in der Regel erst dann, wenn die Benutzer erhaltene elektronische Post öffnen. Insbesondere sollten sie Folgendes beachten:

- Bei jeder eingegangenen elektronischen Post sollte der Empfänger den Betreff sorgfältig lesen. Vorsicht ist bei auffälligen Betreff-Angaben geboten. Dazu gehören englischsprachige Betreffs wie "I love you", "Important Message from..." oder "Pics for you", selbst wenn diese von ihm bekannten Absendern stammen. Derartigen E-Mails angeschlossene Anlagen dürfen unter keinen Umständen geöffnet werden; stattdessen ist umgehend der Systemverantwortliche zu benachrichtigen.
- Vorsicht ist ebenfalls geboten, wenn man von einem deutschen Absender plötzlich elektronische Post mit einem englischsprachigen Betreff erhält. Auch in solchen Fällen dürfen die Anlagen der eingegangenen elektronischen Post nicht geöffnet werden.
- Wer als Anlage zu einer elektronischen Postsendung ein ausführbares Programm erhält (Dateien mit den Endungen .com, .bat, .sys, .bin, .exe, .vbs etc.) sollte dieses nur starten, wenn der Versand der Anlage mit dem Absender zuvor abgestimmt wurde. Unangekündigt eingegangene ausführba-

re Programme sollten dagegen nicht in Gang gesetzt werden. Stattdessen ist entweder Kontakt mit dem Absender der elektronischen Post aufzunehmen oder der Systemverantwortliche der Dienststelle zu unterrichten. In der gleichen Weise sollte der verfahren, der per elektronischer Post komprimierte Dateien erhält und beim Dekomprimieren feststellt, dass ausführbare Programme übersandt wurden.

– Das Herunterladen von Freeware- oder Shareware-Programmen aus dem Internet und das Herunterladen von Spielen sollten grundsätzlich unterbleiben.

4.4 Höhere Sicherheit vor Viren und anderen Schadensprogrammen

Virenattacken à la "I love you" lösten auch Diskussionen um die Sicherheit von Firewalls aus. Denn sie machten deutlich, dass selbst Firewalls keinen ausreichenden Schutz vor Computerviren, die aus dem Internet stammen und via E-Mail versandt werden, bieten können. Unzulänglich schützen Firewalls aber auch vor sog. aktiven Inhalten, die beim Surfen im World Wide Web (WWW) auf interne PC gelangen können und dort vielfach automatisch ausgeführt werden. Es handelt sich dabei um Schadensprogramme, die als JavaScript-Anwendungen, Java-Applets oder Active-X-Controls realisiert sein können. Nicht auszuschließen ist, dass Viren und aktive Inhalte gezielt dazu eingesetzt werden, den Firewall-Schutz zu durchlöchern und schutzbedürftige Daten heimlich ins Internet zu schleusen. Es gilt daher, die Sicherheitstechnik so fortzuentwickeln, dass sie auch solchen Angriffen standhalten kann. Ansätze hierfür sind vorhanden, unter anderem:

– Signatur für Makros
  Mittlerweile lassen sich einige Programme, mit denen Computerbenutzer ihre elektronischen Postfächer leeren, so einstellen, dass ein in einem E-Mail-Anhang enthaltenes Makroprogramm nur dann ausgeführt wird, wenn es durch eine digitale Signatur als vertrauenswürdig gekennzeichnet ist. Nichtsignierte Makros werden dagegen nicht ausgeführt.

– Auslagerung des Browsers
  Aktive Inhalte des World Wide Web können Schaden anrichten, wenn sie auf einen internen Computer gelangen und dort von dem Browser ausgeführt werden, den man zum Surfen im World Wide Web benutzt. Eine Möglichkeit, Schaden durch aktive Inhalte des World Wide Web abzuwehren, beruht auf der Idee, den Internet-Browser aus dem internen Netz zu ver-

bannen und auf einen Computer zu verlagern, der außerhalb des internen Netzes angesiedelt ist und auf dem keine sicherheitsrelevanten oder schutzbedürftigen Daten gespeichert sind. Damit das Internet-Surfen aber weiterhin auch von internen Computern aus möglich ist, wird auf den internen Computern ein Programm eingesetzt, das lediglich den Bildschirminhalt des auf dem externen Computer installierten Browsers, letztlich also eine Menge von Bildpunkten, wiedergibt. Entscheidend ist dabei, dass aktive Inhalte auf diesem Weg gar nicht erst ins interne Netz gelangen können.

– Verschlüsselung schutzbedürftiger Daten
  Eine anderer Ansatz zum Schutz der im internen Netz gespeicherten personenbezogenen Daten geht davon aus, dass ein hundertprozentiger Schutz vor Angriffen aus dem Internet nicht zu erreichen ist und setzt deshalb auf die Verschlüsselung aller im internen Netz gespeicherten personenbezogenen Daten. Selbst wenn es einem Angreifer gelänge, sich diese Daten zu verschaffen, so wären diese Informationen für ihn wertlos, da er sie nicht im Klartext lesen könnte.

5. Was ist bei der Nutzung der Internet-Dienste zu beachten?

Wer - sei es dienstlich oder privat - Internet-Dienste nutzt, sollte dabei Folgendes beachten:

5.1 Vorsicht beim Download

Um dem Risiko entgegenzuwirken, dass aus dem Internet heruntergeladene Programme mit unerwünschten Schadensfunktionen auf einem eigenen PC ausgeführt werden, sollte jeder Benutzer für dieses Risiko sensibilisiert sein.

5.2 Übertragung schutzbedürftiger Daten

Sofern personenbezogene oder andere schutzbedürftige Daten zu übertragen sind, sollte dies nur verschlüsselt geschehen. Eine nach dem Stand der Technik vorgenommene Verschlüsselung bietet dabei die Gewähr, dass die Daten nicht von Unberechtigten zur Kenntnis genommen werden können. Werden die Daten zusätzlich digital signiert, lässt sich auch die Identität des Absenders zuverlässig nachweisen. Ferner ist anhand der digitalen Signatur zu erkennen, ob die Daten während der Übertragung manipuliert wurden.

Wollen mehrere am Internet angeschlossene Teilnehmer oder Einrichtungen untereinander schutzbedürftige Daten austauschen, so bietet sich hierfür die Einrichtung eines sog. virtuellen privaten Netzwerks (VPN) an.

5.3 Hinweise rund um das Web

Surft man durch das World Wide Web und ruft dabei einzelne Informationsseiten ab, so können sowohl im Internet als auch auf dem PC des Nutzers Datenspuren zurückbleiben. Die auf dem PC zurückbleibenden Spuren sind besonders problematisch, wenn sie in Verzeichnissen gespeichert werden, auf die alle Nutzer des PC Zugriff haben.

5.3.1 Cookies

Ruft man Informationen im World Wide Web ab, so kann es sein, dass der Informationsanbieter auf dem PC des Internet-Nutzers eine kleine Datei, eben das Cookie, speichert. Ruft der Surfer von seinem PC aus später das Web-Angebot erneut auf, so wird das Cookie vom heimischen PC zurück an den Informationsanbieter übertragen, der anhand der darin enthaltenen Informationen einen Zusammenhang zwischen dem früheren und dem aktuellen Abruf herstellen kann. Vielfach geht die Speicherung von Cookies sogar unbemerkt vom Surfer vonstatten. Zwar stellen Cookies, im Gegensatz zu Viren, keine ausführbaren Programme dar und können daher den betroffenen PC nicht unmittelbar schädigen. Unbedenklich ist der Einsatz von Cookies gleichwohl nicht. Mit ihrer Hilfe lassen sich nämlich Interessenprofile erzeugen. Besonders aussagekräftige Profile entstehen bei Internet-Werbeunternehmen, die sog. Werbebanner in Web-Angebote anderer Informationsanbieter einblenden. Das geht wie folgt vor sich:
Ruft ein Internet-Nutzer das Angebot z. B. eines Gebrauchtwagenhändlers auf, auf dessen Web-Seiten Banner eines Werbeunternehmens eingeblendet werden, so kann dieses Unternehmen auf dem PC des Surfers ein Cookie anlegen und darin festhalten, dass sich dieser für Gebrauchtwagen interessiert. Besucht dieser Internet-Nutzer danach von seinem PC aus das WWW-Angebot eines Warenhauses, das vom gleichen Werbeunternehmen mit Banner-Werbung bestückt wird, so sendet der PC das bereits vorhandene Cookie an das Werbeunternehmen. Dieses kann ihm entnehmen, dass sich der Surfer zuvor für Gebrauchtwagen interessiert hat. Es kann dann an diesem PC gezielt da-

für werben. Interessiert sich der Internet-Nutzer beim Besuch des Warenhaus-Angebotes besonders für Jugendstilmöbel, so kann das Werbeunternehmen auf dem PC des Internet-Nutzers ein Cookie speichern, in dem neben dem bereits vorher bekannten Interesse für "Gebrauchtwagen" nun auch das für "Jugendstilmöbel" dokumentiert wird.
Zwar erfährt das Werbeunternehmen auf diese Weise nicht, welche Person die Informationen abrief, gleichwohl entsteht, einem Mosaik gleich, Stück für Stück ein Interessenprofil. Dass große Werbeunternehmen mit vielen tausend Inhaltsanbietern zusammenarbeiten, lässt erahnen, wie detailliert diese Mosaike werden können. Teilt der Surfer, beispielsweise bei der Teilnahme an einem Internet-Preisausschreiben, dann noch seinen Namen mit, so können auch diese Angaben in das Profil aufgenommen und dieses damit unmittelbar auf den Surfer bezogen werden. Aber auch wenn die Interessenprofile zunächst noch keinen unmittelbaren Personenbezug aufweisen, ist dies problematisch, da nicht auszuschließen ist, dass dieser später hergestellt wird. Dabei ist auch zu bedenken, dass für die im Ausland ansässigen Internet-Werbeunternehmen mitunter wesentlich geringere Datenschutzanforderungen gelten als dies hierzulande der Fall ist. Daher empfiehlt sich aus Sicht des Datenschutzes generell ein restriktiver Umgang mit Cookies. Die einfachste Möglichkeit dazu ist, den eigenen Internet-Browser so einzustellen, dass er keine Cookies annimmt.
Manche Internet-Angebote setzen sie aber auch sinnvoll ein, etwa wenn es beim Tele-Shopping darum geht, beim Händler verschiedene Waren gleichzeitig zu bestellen. Ohne den Einsatz von Cookies könnten diese nicht quasi in einem Warenkorb auf einmal, sondern jeweils nur einzeln geordert werden. Will man solche Angebote nutzen, sollte man den Browser so einstellen, dass der Surfer über den Cookie-Einsatz informiert wird und ihn im Zweifel ablehnen kann. Hat man einmal Cookies akzeptiert, so sollte man diese nach Abschluss der Internet-Recherche löschen.

5.3.2 Cache-Speicherung

Jede Angebotsseite, die ein Nutzer im World Wide Web abruft, wird auf der Festplatte seines PC im sog. Cache-Bereich des Browsers abgespeichert. Dies hat folgenden Vorteil: Will der Nutzer auf eine Angebotsseite zugreifen, die bereits auf der Festplatte hinterlegt ist, muss er

sie nicht erneut aus dem Internet anfordern, sondern sie lässt sich schnell von der Festplatte laden. Die Kehrseite dieser Medaille ist freilich, dass alle diejenigen, die Zugriff auf diesen Cache-Bereich haben, feststellen können, auf welche Internet-Angebote frühere Nutzer des PC zugegriffen haben. Wer dies verhindern will, muss die im Cache gespeicherten Seiten löschen, nachdem er seine Arbeit im Internet beendet hat. Manche Browser lassen sich auch so einstellen, dass abgerufene Seiten gar nicht erst im Cache auf der lokalen Festplatte gespeichert werden.

5.3.3 History-Liste/Liste zuletzt aufgerufener Web-Seiten

In der History-Liste sowie in der Liste der zuletzt aufgerufenen Web-Seiten vermerken gängige Browser, welche Web-Seiten in der zurückliegenden Zeit abgerufen wurden. Will man erneut eine Seite laden, die man vor einigen Minuten, Stunden oder Tagen bereits abgerufen, deren genaue Adresse man sich aber nicht notiert hatte, so kann man darin nachsehen und einfach den entsprechenden Eintrag anklicken. Ähnlich wie die Cache-Speicherung birgt dieses Vorgehen das Risiko, dass andere Personen diese Daten lesen und damit erfahren können, für welche Internet-Angebote sich frühere Nutzer interessierten. Wer sich dieser Gefahr nicht aussetzen möchte, sollte die Einträge aus der History-Liste sowie der Liste zuletzt aufgerufener Web-Seiten löschen oder diese Listen deaktivieren.

5.4 Passwort für Internet-Zugang und für Web-Services nicht auf dem PC speichern

Die für den Zugang zum Internet verwendeten Programme bieten mitunter die Möglichkeit, die hierfür erforderlichen Passwörter sowie Passwörter für die Nutzung zugriffsbeschränkter Internet-Dienstleistungen auf dem PC abzuspeichern. Da diese Passwörter mitunter nur unzureichend vor unberechtigter Nutzung geschützt sind, sollte man davon keinen Gebrauch machen.

6. Hinweise für Stellen, die eigene Informationsangebote im Internet bereitstellen

Wer mit einem eigenen Informationsangebot im Internet präsent sein will, sollte aus Sicht des Datenschutzes folgende Punkte bei der Gestaltung des Angebots und beim Betrieb der hierfür erforderlichen Informationsserver beachten:

6.1 Anordnung der Server

Wer über ein eigenes Netzwerk verfügt, das über eine Firewall mit dem Internet gekoppelt ist, und mit Hilfe eines WWW- oder eines FTP-Servers Informationen im Internet anbieten will, steht vor der Frage, wo die dafür notwendigen Informationsserver anzuordnen sind. Folgendes ist dabei zu berücksichtigen:

- Anordnung im internen Netz
  Bindet man den Informationsserver in das interne Netz ein, so lässt er sich über die Firewall vor Angriffen aus dem Internet schützen. Die Notwendigkeit, viele externe Zugriffe auf einen oder mehrere interne Rechner rund um die Uhr zulassen zu müssen, stellt gleichzeitig jedoch einen Nachteil dar, denn es widerspricht dem Ziel, Zugriffe von außen auf das zu schützende Netz so weit wie möglich zu minimieren.
- Anordnung auf dem Gateway-Rechner
  Gegen die technisch mögliche Installation eines Informationsservers auf dem Gateway-Rechner spricht, dass ein solcher Rechner nur für die sicherheitsrelevanten Aufgaben eingesetzt werden sollte, die er unbedingt erbringen muss, also im Wesentlichen für die Filterung von Datenpaketen, zur Adressumsetzung sowie zur Protokollierung. Dies trägt dem Umstand Rechnung, dass jedes Mehr an Programm-, Daten- und Befehlsumfang auf diesem Computer Sicherheitsrisiken mit sich bringt, etwa aufgrund von Programmfehlern oder weil es die Überwachung des Firewall-Betriebs erschwert.
- Anordnung in einem geschützten Bereich
  Eine weitere Möglichkeit besteht darin, Informationsserver in einem geschützten Bereich ("demilitarisierte Zone") zwischen Gateway-Rechner und äußerem Paketfilter so anzuordnen, dass das Paketfilter zwar WWW- oder FTP-Anfragen aus dem Internet an diesen Server weiterreicht, nicht dagegen andere Zugriffe. Unter Berücksichtigung der Vor- und Nachteile der einzelnen Alternativen stellt diese Möglichkeit die sicherheitstechnisch sinnvollste Lösung dar.

6.2 Gestaltung der Web-Angebote/Privacy-Policy

Das Teledienstegesetz sowie der Mediendienste-Staatsvertrag verpflichten zumindest alle Anbieter geschäftsmäßiger Informationsangebote, ein Impressum in ihr Angebot aufzunehmen und darin den Namen des für den Inhalt Verantwortlichen sowie dessen Postanschrift zu nennen. Es empfiehlt sich, in diesem Zusammenhang, auch gleich über die Verwendung aktiver Inhalte zu in-

formieren sowie darauf hinzuweisen, ob personenbezogene Daten der Nutzer gespeichert werden und, wenn ja, für welchen Zweck dies geschieht und wann die Daten wieder gelöscht werden. Dies ist auch der Ort, um über den Einsatz von Cookies zu unterrichten.

6.3 Elektronische Dienstleistungen für den Bürger

Immer mehr Behörden informieren die Öffentlichkeit in eigenen Internet-Angeboten darüber, welches Amt für welche Anliegen zuständig ist, wo es zu finden ist, wie die Sprechzeiten sind und welche Unterlagen etwa bei einer Ummeldung, der Zulassung eines Kraftfahrzeugs oder der Aufgebotsbestellung im Falle einer Heirat vorzulegen sind. Mitunter besteht für den Antragsteller gleich noch die Möglichkeit, Antragsformulare beispielsweise zur Ummeldung nach einem Umzug oder zur Reservierung eines Kfz-Wunschkennzeichens vom heimischen PC aus abzurufen, auszufüllen und auf elektronischem Weg wieder an die Behörde zu senden, die die Formulare dann ausdruckt. Dabei darf die Information der Bürger über ihre Rechte und die mit dem Datentransport im Internet verbundenen Risiken nicht zu kurz kommen:

- Stellt eine Behörde im Internet amtliche Formulare zum Abruf bereit, so muss sie dafür sorgen, dass die im gedruckten Formular enthaltenen Hinweise zum Datenschutz dem Bürger auch dann gegeben werden, wenn er das Formular über Internet abruft. Das war bisher jedenfalls nicht immer selbstverständlich.
- Soweit im Internet elektronische Formulare verwendet werden, deren Gestaltung amtlich vorgeschrieben ist, wie dies beispielsweise für die Meldung des Zuzugs, Wegzugs oder Umzugs beim Einwohnermeldeamt der Fall ist, ist Folgendes zu beachten: Das amtliche Vordruckmuster enthält nicht nur die Fragen, die man beantworten muss, nebst zugehörigen Erläuterungen, sondern auch Hinweise darauf, in welchen Fällen der Einwohner der Weitergabe seiner Daten durch das Einwohnermeldeamt widersprechen kann. Diese Datenschutzhinweise dürfen natürlich auch im Fall elektronischer An-, Um- oder Abmeldung nicht fehlen; die Behörde muss vielmehr dafür sorgen, dass die Bürger sie zur Kenntnis nehmen, bevor sie ihre Daten elektronisch an die Behörde senden.
- Unverschlüsselt im Internet übertragene Daten sind nicht vor unberechtigter Kenntnisnahme geschützt. Daher sollte jede Stelle, die elektronische Bürgerdienste anbietet, bei denen auch personenbezogene Daten übertragen

werden, vorsehen, dass dies verschlüsselt erfolgt. Solange eine solche Möglichkeit nicht zur Verfügung steht, muss sie die Bürger darüber informieren, dass die Daten unverschlüsselt übertragen werden und welche Risiken damit verbunden sind. Damit der Bürger es selbst in der Hand hat, von einem elektronischen Versand seiner Daten Abstand zu nehmen, muss ihn die Information natürlich erreichen, bevor er seine Daten eingibt und elektronisch versendet. Sofern medizinische oder andere sensible personenbezogene Daten übertragen werden sollen, stellt die Verschlüsselung eine unverzichtbare Anforderung dar.

– Sollen die elektronisch übermittelten Antragsdaten einen eigenhändig unterschriebenen Antrag ersetzen, so muss sich die Behörde Gewissheit über die Identität des Antragstellers verschaffen. Ansonsten wäre dem Missbrauch Tür und Tor geöffnet: Anträge ließen sich dann unter falschem Namen stellen mit der Folge, dass möglicherweise auf deren Grundlage Verwaltungsentscheidungen getroffen und im Zusammenhang damit falsche Angaben über Bürger gespeichert werden, die unter Umständen finanzielle (Verwaltungsgebühren, Mahnkosten) oder andere Nachteile für die vermeintlichen Antragsteller zur Folge haben können.
  Bei einem herkömmlichen Antrag auf Papier lässt sich im Zweifelsfall anhand der eigenhändigen Unterschrift entscheiden, ob dieser tatsächlich von dem genannten Antragsteller stammt. Als elektronisches Pendant zur eigenhändigen Unterschrift bietet sich die digitale Signatur an: Das zu unterzeichnende elektronische Dokument wird dabei mit Hilfe eines kryptografischen Verfahrens in besonderer Weise gekennzeichnet; jeder kann anhand einer solchen Kennzeichnung überprüfen, von wem diese vorgenommen wurde. Um die gewünschte Fälschungssicherheit und Zuverlässigkeit beim Umgang mit digitalen Signaturen erreichen zu können, müssen zuvor zahlreiche technische und organisatorische Festlegungen über die Erzeugung, Ausgabe und Verwendung der Signaturschlüssel getroffen werden. Hierzu gehören beispielsweise Sorgfaltsregeln für die Stellen (Trust-Center), die die Signaturschlüssel herstellen, Vorgaben zur Frage, wie lange einmal vorgenommene Signaturen als sicher angesehen werden können und auf welche Weise man Signaturschlüssel erkennt, die für eine weitere Verwendung gesperrt wurden. Nun muss nicht jede Stelle, die digitale Signaturen nutzen will, alle diese Maßnahmen selbst festlegen. Entscheidet man sich für die im Signaturgesetz definierte qualifizierte Signatur, so kann man eine

Reihe aufeinander abgestimmter und sich gegenseitig ergänzender Maßnahmen zurückgreifen, die im Signaturgesetz und der dazugehörigen Signaturverordnung dargestellt sind und ein verhältnismäßig hohes Maß an Sicherheit bieten. Zusätzliche Sicherheit lässt sich erreichen, wenn das Trust-Center ein Akkreditierungsverfahren bei der Regulierungsbehörde für Post und Telekommunikation durchlaufen hat. Will man von diesen Standards abweichen, ist darauf zu achten, dass die Sicherheit des Signaturverfahrens am Ende nicht auf der Strecke bleibt.

6.4 Sicherheitsinteressen der Internet-Nutzer beachten

Wie oben bereits dargestellt, gehen Internet-Nutzer, die in ihrem Browser die Ausführung aktiver Inhalte wie Java-Applets, JavaScript-Anwendungen oder ActiveX-Controls gestatten, erhebliche Sicherheitsrisiken ein. Jede Stelle, die ein eigenes Web-Angebot gestaltet, sollte auf die Verwendung dieser Inhalte nach Möglichkeit verzichten. Web-Angebote oder zumindest deren Teile, in denen lediglich Informationen präsentiert werden, sollten grundsätzlich ohne aktive Inhalte auskommen. Wenn die Nutzung dieser Funktionen unverzichtbar ist, sollte Java bevorzugt werden, da es für die Ausführung von Java-Applets ein Sicherheitsmodell gibt, das allerdings in der Vergangenheit wiederholt fehlerhaft programmiert war. Ferner sollten die Nutzer darauf hingewiesen werden, welche Funktionen des Angebots auf diese Weise realisiert werden und weshalb deren Einsatz überhaupt erforderlich ist. In den Teilen des Angebots, in denen die aktiven Inhalte nicht benötigt werden, ist auf deren Einsatz zu verzichten.

6.5 Datenschutzgerechte Protokollierung der Abrufe

Wer eigene Angebote ins Internet einstellt, will in aller Regel wissen, wie oft welche Angebotsseiten abgerufen wurden. Mitunter protokollieren die Betreiber der WWW-Server hierzu nicht nur, wann welche Angebotsseite abgerufen wurde, sondern registrieren auch die Netzadresse des abrufenden Computers, die sog. IP-Adresse.
Bei dieser Vorgehensweise ist Folgendes zu bedenken:
Der numerischen IP-Adresse eines am Internet angeschlossenen Computers lässt sich mit Hilfe des DNS-Dienstes ein Name zuweisen. Daraus geht häufig hervor, in welchem Land der Rechner installiert ist. Zudem gibt der Rechnername oft auch Aufschluss über die Stelle, die den Rechner betreibt, beispielsweise ein Universitätsinstitut. Schon allein dies lässt einen Rückschluss auf

den Kreis derjenigen zu, die mit diesem Rechner arbeiten. Vollends zu einem persönlichen Merkmal werden Rechnername und Netzadresse, wenn der Internet-Nutzer immer mit demselben Computer arbeitet, diesen Rechner allein nutzt und die Adresse dieses Computers im Internet verwendet wird. Mit anderen Worten: IP-Adressen können personenbezogen sein. Für die Anbieter von WWW-Angeboten hat dies folgende Konsequenz: Da sie mit ihren Angeboten in der Regel Tele- oder Mediendienste anbieten, müssen sie die Datenschutzregelungen des Teledienstedatenschutzgesetzes oder des Mediendienste-Staatsvertrags der Länder beachten. In beiden heißt es klipp und klar, dass der Diensteanbieter personenbezogene Daten über die näheren Umstände des einzelnen Abrufs spätestens mit dem Beenden der Verbindung löschen muss, es sei denn, er benötigt die Daten noch für Zwecke der Abrechnung. Da die IP-Adressen je nach konkretem Einsatz personenbezogen sein können, dürfen IP-Adressen nach erfolgtem Web-Seiten-Zugriff allenfalls für Abrechnungs- nicht aber für andere Zwecke gespeichert werden.

7. Weitere Informationen zum Themenbereich Internet, e-Government und Datenschutz

Datenschutz bei der Nutzung von Internet und Intranet
Orientierungshilfe des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder, Stand: 15. Dez. 2000, herausgegeben vom Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern
www.baden-wuerttemberg.datenschutz.de/service/gem-materialien/intranet.pdf

Vom Bürgerbüro zum Internet
Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Stand 21. Nov. 2000, hrsg. vom Landesbeauftragten für den Datenschutz Niedersachsen
www.baden-wuerttemberg.datenschutz.de/service/gem-materialien/buergerbuero.zip

Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz vom 8. März 2002
www.baden-wuerttemberg.datenschutz.de/service/gem-materialien/oh-arbeitsplatz.htm

CERT

Hinweise über aktuelle Sicherheitslücken und Gegenmaßnahmen finden sich in den Internet-Angeboten der Computer Emergency Response Teams (CERT), z. B.

- CERT des Deutschen Forschungsnetzes (DFN-CERT):
  www.cert.dfn.de
- CERT der Universität Stuttgart:
  www.cert.uni-stuttgart.de
- CERT für Bundesbehörden (CERT-Bund):
  www.bsi.bund.de/certbund/index.htm

BSI

Das Bundesamt für Sicherheit in der Informationstechnik hält zahlreiche Informationen und Materialien zum Thema IT-Sicherheit zum Abruf bereit
www.bsi.bund.de

IT-Grundschutzhandbuch des BSI

Eine umfangreiche Zusammenstellung sicherheitsrelevanter Aspekte beim Einsatz von Computern, darunter auch solche, die die Realisierung von Internet-Anschlüssen betreffen, sowie entsprechende Maßnahmenkataloge finden sich im IT-Grundschutzhandbuch des BSI.
www.bsi.bund.de/gshb/index.htm

Studien des BSI aus den Jahren 2001 und 1997 zu Firewallprodukten
www.bsi.bund.de/literat/studien/firewall/fwstud.htm

e-Government-Handbuch des BSI

Im e-Government-Handbuch gibt das BSI unter anderem auch einen umfassenden Überblick über die mit eGovernment-Projekten einhergehenden Sicherheitsfragen.
www.bsi.bund.de/fachthem/egov/6.htm

Virtuelles Datenschutzbüro

Weitere Informationen rund um das Thema Datenschutz finden sich im Internet-Angebot des virtuellen Datenschutzbüros, das von zahlreichen nationalen und internationalen Datenschutzbeauftragten getragen wird
www.datenschutz.de