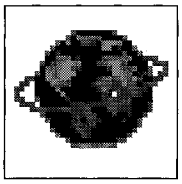
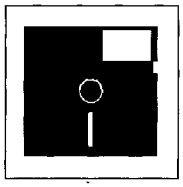




Orientierungshilfe zu Datenschutzfragen bei der Nutzung des Internet durch die öffentliche Verwaltung – Teil I

Der saarländische Landesbeauftragte für Datenschutz

Attraktivität globaler Netze

Seit einiger Zeit wächst in öffentlichen Stellen des Saarlandes der Wunsch nach einem Zugang zu globalen Datennetzen. In der Öffentlichkeit wird die Öffnung der Verwaltung auch für Möglichkeiten der elektronischen Kommunikation gefordert oder vorausgesetzt. Insbesondere das Internet ist durch seine weltweite Nutzung und die Kommunikationsmöglichkeiten unterschiedlichster Benutzer und Bereiche, die auch unter den Begriffen "Datenautobahn" und "globales Dorf" propagiert werden, sehr attraktiv. Durch Anbindung von Einzelplatz-PC oder Verwaltungsnetzen an das Internet können dort verfügbare Informationen gewonnen, eigene Informationen für andere zum Abruf bereitgestellt oder das Netz zum Transport von Verwaltungsdaten genutzt werden.

Zahlreiche Gefahren

Mit dem Zugang zum Internet sind jedoch Risiken verbunden, die größtenteils daraus resultieren, daß dieses Datennetz nicht unter Sicherheitsaspekten entwickelt wurde und historisch gewachsen ist. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Übertragungswegen und Rechnersystemen. So gibt es beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung im Netz. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Abgerufene Programme und Dokumente können bekannte und unbekannte Viren enthalten. Programme, Dokumente und Bilder können verfälscht sein. Dies ist besonders gravierend, weil aufgrund der riesigen Zahl von Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner und -netze bedrohen können, sehr groß ist.

Arbeitspapiere als Orientierungshilfe

Die vorliegende Orientierungshilfe auf der Basis von Arbeitspapieren des Arbeitskreises "Technik" der Datenschutzbeauftragten des Bundes und der Länder soll den für den Betrieb von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen, mit welchen Risiken bei einem Anschluß an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Die hier entwickelten Strategien zur Risikobegrenzung bedürfen im Einzelfall einer weiteren Konkretisierung, da angesichts einer sich ständig verändernden Gefährdungslage infolge des Auftretens neuer unerwarteter Sicherheitsprobleme ein permanenter Anpassungsbedarf besteht und ein Restrisiko nicht ausgeschlossen werden kann.

Empfehlungen aus Datenschutzaspekten

Für eine Nutzung des Internet werden aus datenschutzrechtlicher Sicht folgende Empfehlungen vorgelegt:

Voraussetzungen

1) Vor der Einrichtung von Internet-Zugängen ist der Kommunikationsbedarf festzustellen, an dem sich die Kommunikationsmöglichkeiten zu orientieren haben (datenschutzrechtlicher Erforderlichkeitsgrundsatz). Bei bestehenden Netzen ist auch zu prüfen, inwieweit diese in anschließbare, bedingt anschließbare und nicht anschließbare Teile segmentiert werden müssen.

2) Für den gegebenen Kommunikationsbedarf ist eine Risikoanalyse vorzunehmen und ein Sicherheitskonzept zu erstellen.

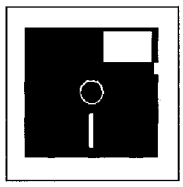
Allgemeine Anforderungen

3) Die Kommunikation der öffentlichen Verwaltung (Nachrichten-, Dateien- und Dokumentenaustausch) sollte über andere, sicherere Verbindungen (z. B. X400) abgewickelt werden.

4) Aus Sicherheitsgründen sollte ein Zugang zum Internet nur über isolierte Rechner oder speziell dafür ausgelegte und darauf beschränkte Netze erfolgen.

5) Auf eine sichere Konfiguration der Soft- und Hardware und den Einsatz aktueller, fehlerarmer Software ist zu achten. Benutzer und Administratoren sind laufend über Risiken und erkannte Fehler zu unterrichten.

Der saarländische Landesbeauftragte für Datenschutz. Referat für "Kommunikations-, Informations- und Bürotechnik".



6) Sensible Daten, insbesondere personenbezogene Daten, sind bei entsprechendem Schutzbedarf mit Hilfe hinreichend sicherer, kryptografischer Verfahren zu verschlüsseln; hierzu gehören auch Paßwörter und sonstige Authentifikationsdaten. Es sollte angestrebt werden, generell alle Transport- und Verkehrsdaten auf möglichst niedriger Protokollebene zu verschlüsseln und sichere Authentisierungsverfahren einzusetzen. Bei asymmetrischen Verschlüsselungsverfahren sollte eine vertrauenswürdige, zentrale Stelle mit der Funktion der Schlüsselerzeugung und -verwaltung (Trust-Center) beauftragt werden.
7) Übernommene Programme und Dokumente sind vorab mit einem aktuellen Virenscanner auf Virenfreiheit zu testen. Wenn möglich, sollte auch die Integrität der Daten überprüft werden, wozu z. B. Verfahren der elektronischen Unterschrift oder Prüfsummenverfahren genutzt werden können.

Anforderungen beim Netzanschluß
8) Falls ein Netzanschluß unbedingt erforderlich ist, sollte die Sicherheit der Verwaltungsnetze und der Schutz von personenbezogenen Daten, die auf vernetzten Systemen verarbeitet werden, durch den Einsatz geeigneter Schutzkonzepte mit Hilfe einer dazwischen geschalteten Prüf- und Filterfunktion (Firewall) gewährleistet werden.
9) Der ausschließliche Einsatz einer zentralen Firewall-Lösung ist nur dann vertretbar, wenn sich die Sicherheitsmaßnahmen an den Daten orientieren, die den höchsten Schutzbedarf haben.
10) Das Konzept gestufter Firewalls ist dann anzuwenden, wenn die Verwaltungsnetze aus einer Vielzahl verschiedener Teilnetze bestehen, in denen Daten unterschiedlicher Sensibilität verarbeitet werden. Die Anbindung an das Internet sollte nur über einen zentralen Zugang (Gateway) erfolgen.
11) Werden in den anzuschließenden Netzen sensible personenbezogene Daten verarbeitet, ist der hohe personelle und sachliche Aufwand für Firewall-Lösungen gerechtfertigt und geboten. Dabei ist es unverzichtbar, hochspezialisierte Kräfte für die Implementation und die systemtechnische Betreuung einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein. Firewall-Konzepte stellen erhöhte Anforderungen an die lokale Systemverwaltung, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben könnten, als bei isoliert betriebenen Rechnern.
12) Der Betrieb von Firewall-Systemen muß klaren Richtlinien folgen. Diese Richtlinien müssen neben Zuständigkeitsregelungen auch Vorgaben für die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und Sanktionen bei Sicherheitsverstößen enthalten.

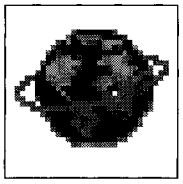
Erläuterungen zur Sachlage

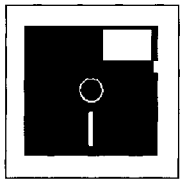
Inhaltsverzeichnis

Anmerkungen

Hintergrundinformationen

Die nachfolgenden Ausführungen sind Hintergrundinformationen zum besseren Verständnis der vorgenannten Empfehlungen aus Sicht des Datenschutzes. Dabei wird versucht, die wesentlichen Begriffe und Funktionen zu erläutern und die Risiken und entsprechende Maßnahmen zu ihrer Minimierung vorzustellen. Für detailliertere Informationen wird auf die angegebene Literatur verwiesen.





I Einleitung und Übersicht

Zugang zu globalen Netzen

Seit einiger Zeit wächst in öffentlichen Stellen des Saarlandes der Wunsch nach einem Zugang zu globalen Datennetzen. In der Öffendichkeit wird die Öffnung der Verwaltung auch für Möglichkeiten der elektronischen Kommunikation gefordert oder vorausgesetzt. Insbesondere das Internet ist durch seine weltweite Nutzung und die Kommunikationsmöglichkeiten unterschiedlichster Benutzer und Bereiche, die auch unter den Begriffen "Datenautobahn" und "globales Dorf" propagiert werden, sehr attraktiv. Durch Anbindung von Einzelplatz-PC oder Verwaltungsnetzen an das Internet sollen dort verfügbare Informationen gewonnen, eigene Informationen für andere zum Abruf bereitgestellt oder das Netz zum Transport von Verwaltungsdaten genutzt werden.

Das Internet

Internet ist das bekannteste weltumspannende Datennetz, ein Zusammenschluß vieler lokaler Computernetze. Die Grundlagen für das Internet wurden mit der Entwicklung des Ethernet-Konzepts und des TCP/IP-Protokolls (Transmission Control Protocol/Internet Protocol) Ende der 60er Jahre bei der Fa. Xerox in den USA gelegt. Informationen werden in Pakete zerlegt, die voneinander unabhängig auf verschiedenen Wegen zum Ziel kommen können und dort wieder in der ursprünglichen Reihenfolge zusammengesetzt werden. Verlorene TCP-Pakete werden automatisch wieder nachgefordert.

Aufbau seit 1969

Die Robustheit gegenüber Störungen und Ausfällen wurde vom US-Verteidigungsministerium genutzt, um im Jahre 1969 mit dem Aufbau des ARPA-Netzes (Advanced Research Projects Agency) und des DARPA-Netzes (Defense ARPA) zu beginnen. Es kamen überwiegend UNIX-Rechner zum Einsatz, doch ist das TCP/IP-Protokoll ähnlich wie OSI als Schichtenmodell angelegt, so daß unterschiedliche Hardware eingesetzt werden kann. Beim Wechsel des Leitungstyps sorgen Umsetzer (Repeater, Bridges, Router) für die Anpassung, die unbemerkt vom Benutzer automatisch durchgeführt wird. Anfang der 80er Jahre wurde das Wissenschaftsnetz CSnet über Gateways angebunden. Ende der 80er Jahre erfolgte der Übergang zum NSFnet (National Science Foundation). Der amerikanische Vizepräsident Al Gore erklärte Anfang der 90er Jahre das Projekt des "data-highway" zur nationalen Zukunftsaufgabe, was auch in anderen Staaten zu ähnlichen Initiativen geführt hat.

Rund 40 Millionen Nutzer

Die Zahl der Benutzer des Internet wird auf etwa 40 Millionen geschätzt (Stand: Oktober 1995). Pro Monat werden ca. 10.000 neue Rechner angeschlossen. Entsprechend wächst auch der Umfang der verfügbaren Informationen, die Zahl der Nutzer und auch die Bedrohung durch Mißbrauch. Die Infrastruktur ist einem permanenten Wandel unterworfen, während die Funktionalität erhalten bleibt.

Organisation

Obwohl das Netz sehr amorph ist, gibt es eine gewisse Organisation für die Regelung von Einzelfragen. Die IANA (Internet Assigned Numbers Authority) definiert, welche Teile des TCP/IP-Protokolls wie sockets und ports für welche Dienste reserviert werden. Für die weltweit eindeutige Zuordnung von IP-Adressen sind die NIC's (Network Information Centers) zuständig. Das INTERNIC betreut den amerikanischen, das APNIC den asiatischen und das RIPE (Réseaux IP Européens) in Amsterdam den europäischen Bereich und die angrenzenden Regionen mit Ausnahme des deutschen Bereichs, für den das DENIC beim Rechenzentrum der Universität Karlsruhe zuständig ist.

Jeder Rechner im Internet erhält eine eindeutige numerische Adresse aus 4 Bytes, die IP-Adresse. Da diese numerischen Adressen schwer zu behalten sind, wird ihnen ein sprechenderer Name zugeordnet, der in der Regel die Form hat:

<Rechner>.<Bereich>.<Institution>.<Land>

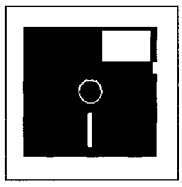
So hat z. B. ein Internet-Zugangsrechner der Uni Saarbrücken den Namen

"sbusol.rz.uni-sb.de"

der zur numerischen Internetadresse "134.96.7.7" gehört. Die Zuordnung der numerischen zum sprechenderen, alphanumerischen Kürzel wird in sogenannten Nameservern verwaltet. Das zuständige NIC überwacht und koordiniert die Nameserver-Funktionen der einzelnen Einrichtungen und betreibt den nationalen Nameserver, bei dem Adreßanfragen aus dem Ausland zuerst auflaufen. Zusätzlich zum Rechnernamen wird für die Benutzer die Internet-Adresse vor dem Rechnernamen mit dem Benutzernamen ergänzt, der mit einem "@"-Zeichen abgetrennt wird. So lautet z. B. die vollständige Internet-Adresse eines Nutzers der Universität Saarbrücken "amüller@sbusol.rz.uni-sb.de". Ein wichtiger Nameserver ist auch der lokale DNS (Domain Name Server), der in den lokalen Netzen für die Zuordnung der lokalen Namen zu Internetadressen zuständig ist.

Versand von Datenpaketen

Die zu übertragenden Daten werden in Pakete zerlegt, die u.a. mit der Absender- und der Empfänger-IP-Adresse versehen werden. Die Datenpakete werden zumeist über eine Vielzahl von Zwischenstationen weitergeleitet, die den Weg zum Zielrechner aufgrund der



Ein Provider wird benötigt.

Adreßinformationen bestimmen (Routing). Die Zwischenstationen tauschen die Daten über Wähl- oder Standverbindungen im Telefonnetz (per Kabel oder Satellit) aus.
Um an das Internet angeschlossen zu werden, benötigt man eine Verbindung (auch eine Wählverbindung per Modem über das normale Telefonnetz ist möglich) zu einem der bestehenden Zugangsanbieter ISP (Internet Service Provider). Diese Provider haben eine eigene Netzinfrastruktur, die an das Internet angeschlossen ist und verfügen damit auch über internationale Anbindungen. Die Saarländische Landesverwaltung wird die Universität Saarbrücken in Verbindung mit ihrem Service-Provider zum Internet-Zugang nutzen. Die Zugangs-/Leitungskosten zum ISP trägt der Nutzer direkt, die Kosten des Providers für dessen Infrastruktur (Personal, Hard- und Software) und die Leitungen mit internationaler Konnektivität oder zum nächsten Provider mit entsprechenden Leitungen trägt der Nutzer über Monatspauschalen (25–500 DM) und/oder mengenabhängige Gebühren (ca. 1 Gigabyte kosten ca. 600 DM/Monat) und zusätzlichen Anschluß- und Leitungsgebühren (64-Kbits/s-Zugang 750–5.000 DM). Im kostengünstigsten Fall kann man als Nutzer lediglich Daten und Dienste aus dem Internet beziehen; selbst als Anbieter nach außen aufzutreten, ist entsprechend teurer. Einen einfachen und kostengünstigen Zugang zum Internet stellt die Deutsche Telekom AG im Rahmen ihres T-Online-Dienstes (früher Bildschirmtext/Btx/Datex-J- bereit, bei dem Zugänge zum Ortstarif in jedem Ortsnetz möglich sind und lediglich zeitabhängige Gebühren anfallen.

Aufwendige Gestaltung von Beiträgen

Abgesehen von wenigen deutschen Anbietern und Foren wird die internationale Kommunikation (E-Mail, Textbeiträge in Diskussionsforen, Angebote aller Art) in englischer Sprache abgewickelt. Der internationale Zeichensatz enthält keine deutschen Umlaute und Sonderzeichen (z. B. "ß"), die auch durch die vorhandenen Editoren nicht unterstützt werden; das Schreiben von E-Mails und Textbeiträgen ist deswegen etwas gewöhnungsbedürftig. Sollen deutsche Texte mit vollem Zeichensatz über das Netz verschickt werden, müssen sie wie Programme vor dem Versand mit Hilfe von Systemprogrammen (z. B. UUDECODE, UUENCODE) erst an die 7-Bit-Struktur des Netzcodes angepaßt und nach dem Erhalt zurückgewandelt werden. Die Erstellung von WWW-Seiten ist sehr aufwendig (Seitenbeschreibungssprache HTML) und wird von derzeit verfügbaren Editoren noch nicht komfortabel genug unterstützt. Ein Abruf von Seiten mit Modems unter 28.800 Bit/s ist wegen der langen Grafik-Ladezeiten zeitaufwendig und kann das "Surfen im Netz" frustrierend gestalten.

Keine zentrale Kontrollinstanz

Bisher wurde das Internet (auch als "Mutter aller Netze" bezeichnet) hauptsächlich von wissenschaftlichen Einrichtungen wie Universitäten genutzt. Da hier der freie Austausch von Informationen Vorrang hat, ist eine sehr flexible und von einer zentralen Verwaltung unabhängige Struktur entstanden. Inzwischen hat sich der Nutzerkreis ausgeweitet, und es ist eine fortschreitende Nutzung für private und kommerzielle Zwecke und in ersten Ansätzen auch schon für Zwecke der öffentlichen Verwaltung zu beobachten. Da es eine zentrale Kontrollinstanz, die jeglichen Mißbrauch verhindert, nicht geben kann, ist eine umfassende Information der Systembetreiber und Nutzer unerläßlich, um mögliche Risiken abschätzen und individuelle Sicherheitsmaßnahmen treffen zu können.

Weitere Datennetze

Neben dem Internet gibt es weitere Datennetze, die mit eigenen Protokollen arbeiten, z.B. CompuServe, America Online, Microsoft Network oder der BTX-/Datex-J-Nachfolger T-Online, auf die im folgenden nicht eingegangen werden soll, bei denen aber ähnliche Techniken Sicherheit gewährleisten können.

II Dienste im Internet

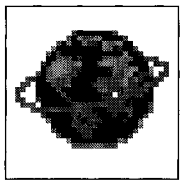
Die wichtigsten Dienste, die das Internet bietet, werden im folgenden beschrieben:

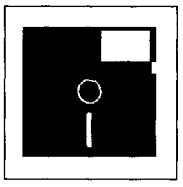
E-Mail

Elektronische Mail (kurz E-Mail oder Email) ermöglicht das Verschicken von "elektronischen Briefen" (wegen der Offenheit eher mit Postkarten zu vergleichen) zwischen mehreren Computerbenutzern. Die Nachrichten können aus Texten, Programmen, Grafiken, Tönen oder Bildern bestehen. Sender und Empfänger müssen jeweils eine eindeutige E-Mail-Adresse besitzen (Form: Name@Anschrift), die ähnlich der postalischen Anschrift funktioniert. Mit Hilfe von Mailing-Listen können auch zu bestimmten Diskussionsthemen geschlossene Benutzergruppen gebildet werden, deren Teilnehmer sich erst einschreiben müssen, um danach die Beiträge der Gruppe zu erhalten. Der Versand von E-Mails in andere Datennetze wird für den Nutzer unbemerkt über Gateways abgewickelt, die den Übergang von einem System zum anderen handhaben. Neben dem Internetprotokoll "smtp" gewinnt auch das OSI X400-Protokoll immer mehr an Bedeutung.

Usenet-News

Öffendiche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (Newsgroups) ausgetauscht. Dieser News-Dienst wird auch als Usenet (Kurzform von Users' Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zur Zeit gibt es etwa 10.000 verschiedene Newsgroups, in denen pro Monat





rund 3,2 Millionen Artikel mit einem Datenvolumen von ca 14 GB geschrieben werden (Stand: August 1995). Die Artikel werden auf zentralen Rechnern (News-Servern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreader-Programme. Jeder kann die in den Foren enthaltenen Beiträge lesen und selbst eigene Beiträge zusteuern. Es gibt einen im Netz abrufbaren und weitgehend auch eingehaltenen Verhaltenscodex, die sogenannte "Netiquette". Bei einigen News-Gruppen ist auch eine Moderation vorhanden, die für eine gewisse "Sauberkeit" bei den Texten sorgt.

Telnet Mit Hilfe von Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login). Dazu benötigt man einen Account (Nutzerkennung und Paßwort) oder einen öffentlichen Zugang auf dem anderen Rechner. So kann man zum Beispiel Informationssysteme wie Datenbanken oder Bibliotheken nutzen, Terminkalender abfragen oder Textverarbeitung vornehmen. Auch eine Fernwartung des Rechners ist möglich. Mit Telnet sind nur textorientierte Anwendungen nutzbar.

FTP FTP (File Transfer Protocol) dient dem Übertragen von Dateien zwischen Rechnern mit Hilfe eines normierten Befehlssatzes. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Voraussetzung sind Accounts auf beiden Rechnern oder eine öffentliche Zugriffsmöglichkeit auf dem FTP-Server durch "Anonymous FTP", wodurch ein eingeschränkter Zugriff auf bestimmte Dateien des entfernten Rechners ermöglicht werden kann. Weltweit gibt es tausende Anonymous-FTP-Server, die Programme, Texte, Grafiken oder Tondateien zum Abruf und Kopieren auf den eigenen Rechner bereithalten (z. B. auch die aktuellen Versionen des McAfee-Virenscanners).

Archie Archie ist ein mächtiger Dienst für die weltweite Suche nach Dateien auf FTP-Servern, der selbst auf ca. 25 Archie-Servern angeboten wird. Der Zugriff erfolgt über Telnet, E-Mail oder einen eigenen Archie-Client. Als Suchergebnis liefert Archie entweder Server-, Verzeichnis- und Dateinamen oder eine Kurzbeschreibung zu gesuchten Dateien, die genutzt werden können, um dann mit FTP diese Dateien auf den eigenen Rechner zu laden.

WWW Der jüngste Internet-Dienst WWW (World Wide Web) kann nahezu alle anderen Dienste integrieren. Durch einen multimediaorientierte, Windows-ähnliche Oberfläche wird eine einfache Bedienbarkeit erreicht. Per Mausklick lassen sich Texte, Bilder, Grafiken und Videoclips als Hypertext-Dokumente abrufen. Dabei können Dokumente aus Elementen der unterschiedlichen Darstellungsformen zusammengefaßt werden, die aus verschiedenen Informationsknoten, auch verteilten Servern stammen können. Als Client-Software für den grafikorientierten Zugriff werden sogenannte "Browser" verwendet, bei denen die Produkte "Netscape Navigator" und "NCSA Mosaic" derzeit einen Marktanteil von ca. 90 % haben. Der Kommunikation zwischen einem WWW-Client und den WWW-Servern, die die multimedialen Daten anbieten, liegt das Protokoll HTTP (HyperText Transport Protocol) zugrunde. Die WWW-Dokumente werden mit der Definitionssprache HTML (HyperText Markup Language) erstellt. Ein Update für das Textsystem Winword zur Erstellung von HTML-Seiten ist verfügbar. Für die Generierung interaktiver WWW-Seiten können CGI (Common Gateway Interface)-Skripte installiert werden.

Gopher Gopher ist ein menü-orientiertes Werkzeug zur Recherche, das unabhängig davon eingesetzt werden kann, auf welchem Rechner die gesuchten Informationen zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkeiten (FTP, Telnet, WAIS usw.) existieren. Jeder Gopher-Server ist öffentlich zugänglich. Benutzer können mit ihrem Gopher-Client nur lesend auf die angebotenen Daten zugreifen. Gopher ist im WWW integriert und erleichtert dort auch die Suche nach Informationen, da die Grafikanteile der WWW-Seiten ausgeblendet werden und dadurch die Übertragung wesentlich schneller ablaufen kann. Während der Gopher-Zugriff nur auf einem lokal verfügbaren Server erfolgt, gibt es mit dem Produkt Veronica eine rechnerübergreifende Suchhilfe, die eine Suche über alle Gopher-Server des Internet durchführt.

WAIS WAIS (Wide Area Information Server) ermöglicht eine Volltextsuche in ca. 500 Datenbanken, ohne komplizierte Abfragesprachen beherrschen zu müssen. WAIS-Abfragen können mit Telnet, E-Mail, einem eigenen WAIS-Client oder über WWW durchgeführt werden.

Finger Finger ist ein Werkzeug zur Suche nach Informationen über Personen und Rechner, die an der Kommunikation im Internet beteiligt sind. Es können sowohl personenbezogene Daten (Name, E-Mail-Adresse, Telefonnummer, Arbeitszeit, öffentliche Schlüssel usw.) als auch sicherheitsrelevante Informationen über angeschlossene Rechner in Erfahrung gebracht werden.

Whois Whois wurde speziell zur Recherche nach personenbezogenen Daten von im Internet registrierten Nutzern entwickelt. Das Vorhaben, eine Datenbank mit weltweit allen Internet-Nutzern aufzubauen, konnte nicht realisiert werden. Zur Zeit existieren eine Vielzahl von einzelnen Whois-Servern, auf die mit Telnet oder mit eigener Client-Software zugegriffen werden kann.