Mitarbeitervertretung der landeskirchlichen Angestellten in den Bezirken und Gemeinden

MAV-Info

Büroadresse: Wolfgang Lenssen – Köndringerstr. 11 - 79331 Heimbach - ☎ 07641 – 93 58 48
Fax: 07641 - 41 335 / **e-mail:** mav@gmx.de **/ internet:** http://www.ekiba.de/mav

Sondernummer Dienstvereinbarung * Intranet * 2005

Dienstvereinbarung ab 1. April 2005 in Kraft

Dienstvereinbarung zur „*Einführung des landeskirchenweiten Intranets in der Dienststelle*“ am 18. März 2005 beschlossen

Nach wirklich zähen Verhandlungen über den Text dieser Dienstvereinbarung ging es dann am Schluss erstaunlicherweise ganz schnell:
Letzte Differenzen konnten innerhalb weniger Tage und Dank der Möglichkeit des e-mail Verkehrs gelöst werden und so lag ein beschlussfähiger Textvorschlag pünktlich zur Sitzung der **MAV** am 18. März 2005 vor.
Einstimmig wurde dann erwartungsgemäß der Beschluss gefasst, diese Dienstvereinbarung abzuschließen.
Ein **Schreiben des EOK zur Dienstvereinbarung**, den Text der **Dienstvereinbarung**, die Texte der Anlagen (**Internet-Nutzungsvereinbarung** und **Internet-Sicherheitsvereinbarung**) sowie den Text des ***Tarifvertrag über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen mit Geräten der Informations- und Kommunikationstechnk (TV IuK)*** drucken wir in dieser Sondernummer ab.
Zusätzlich erhalten Sie / erhaltet Ihr einige aus der Sicht der **MAV** hilfreiche Informationen rund um das Thema Internet und Sicherheit.
In den kommenden **MAV** –Infos werden wir Sie / werden wir Euch auch weiterhin über den neuesten Stand der Dinge in Sachen „Intranet“ informieren.
Sollten Sie / solltet Ihr jedoch im alltäglichen Gebrauch Probleme, Unstimmigkeiten oder Schwierigkeiten mit der Anwendung der Dienstvereinbarung entdecken, so sind wir auf Ihre / Eure Rückmeldungen angewiesen – streng nach dem Motto:

Problem erkannt = Problem gebannt

Wolfgang Lenssen (Geschäftsführer)

Inhalt der Sondernummer

Evangelische Landeskirche in Baden
Evangelischer Oberkirchenrat

Evangelischer Oberkirchenrat · Postfach 2269 · 76010 Karlsruhe

An die landeskirchlichen Angestellten
in den Kirchenbezirken und Kirchengemeinden

Projekt: Vernetzung in der Landeskirche

Blumenstraße 1-7
76133 Karlsruhe

Telefon (0721) 9175-863
Telefax (0721) 9175-25-863

AZ: 14/6660 Vernetzung

Sachbearbeitung:
Manfred Schwan
manfred.schwan@ekiba.de
www.ekiba.de

21. Juli 2005

Abschluss einer Dienstvereinbarung über die Einführung des landeskirchenweiten Intranets

Sehr geehrte Damen und Herren,

mit dem Abschluss einer Dienstvereinbarung über die Einführung des landeskirchenweiten Intranets in den Dienststellen ist eine wichtige Grundlage für die Verbreitung des neuen Systems geschaffen worden.

Während im EOK bereits eine EDV-Dienstvereinbarung besteht, auf deren Grundlage die Einführung durchgeführt werden konnte, sind die unterschiedlichen Einsatzorte und Arbeitsstellen (Dienststellen) besonders zu betrachten.

Mit dem Zugang zum Intranet wird auch der Zugang zum Internet möglich bzw. erfolgt bereits über einen solchen Zugang. Die Teilnahme an diesem System ist besonders schutzwürdig und es bedarf daher einer Internet-Nutzungsvereinbarung.

Diese Internet–Nutzungsvereinbarung ist der Dienstvereinbarung angeschlossen und enthält umfangreichen Erläuterungen, die von jeder Benutzerin und von jedem Benutzer akzeptiert werden müssen.

Es empfiehlt sich, die Anlage sehr genau durchzulesen und aufzubewahren. Von der unterschriebenen Nutzungsvereinbarung sollte für den eigenen Nachweis eine Kopie gefertigt werden. Das Original ist an den Evangelischen Oberkirchenrat, Fachbereich IT, Blumenstr. 1-7, 76133 Karlsruhe zu senden. Der Fachbereich IT sammelt die Nutzungsvereinbarungen und halt diese für den Datenschutzbeauftragten vor.

Der Zeitpunkt des Anschlusses ist abhängig vom Zugang Ihrer Dienststelle bzw. von Ihnen persönlich. Sie erfahren hiervon rechtzeitig und umfassend und werden auch auf die Inhalte umfangreich geschult. Der genaue Plan wird derzeit erarbeitet.

Was ist konkret zu tun?

Die von der Mitarbeitervertretung und der Geschäftsleitung gemeinsam vereinbarte Dienstvereinbarung sollte zur Kenntnis genommen werden.

Die beigefügte Internet-Nutzungsvereinbarung ist auszufüllen und im Original an das Projekt Vernetzung - Evangelischer Oberkirchenrat – z. Hd. Herrn Wiederstein – Blumenstr. 1-7 - 76133 Karlsruhe zu senden. Die Internet-Sicherheitsvereinbarung ist zur Kenntnis zu nehmen und zu beachten. Dies kann bereits jetzt geschehen und hilft dem Projektteam sehr bei der Umsetzung, da vor Anlage der Zulassung im System die Vorlage der Vereinbarung geprüft wird.

Wir hoffen auf eine gute und vertrauensvolle Zusammenarbeit.

Mit freundlichen Grüßen

M. Schwan
Projektleiter

Dienstvereinbarung

In Wahrnehmung der gemeinsamen Verantwortung für den Dienst in der Kirche haben
die Evangelische Landeskirche in Baden, vertreten durch den Evangelischen Oberkirchenrat, im Folgenden „Dienststelle“ genannt,
und
die Mitarbeitervertretung der landeskirchlichen Angestellten in den Kirchenbezirken und –gemeinden, im Folgenden „Mitarbeitervertretung“ genannt,

gemäß § 36 in Verbindung mit § 40 Buchstaben i, j und k Mitarbeitervertretungsgesetz in der Fassung vom 21. Oktober 2004 (GVBl. S. 187) folgende

Dienstvereinbarung
über die Einführung des
landeskirchenweiten Intranets
in der Dienststelle

abgeschlossen:

Präambel
Zum Ende des Jahres 2005 soll für die Evangelische Landeskirche in Baden und ihre Kirchenbezirke und Kirchengemeinden sowie alle kirchlichen Einrichtungen eine moderne und einheitliche Kommunikationsstruktur durch ein landeskirchenweites Intranet hergestellt sein. Ziel ist eine vernetzte Kommunikation durch Einsatz moderner Kommunikationsmittel (E-Mail etc.). Dies soll nicht zuletzt den Arbeitsablauf in den kirchlichen Dienststellen erleichtern, insbesondere in der Kommunikation mit dem Evangelischen Oberkirchenrat in Karlsruhe.

Ziel des Intranet-Einsatzes ist es, ein Medium für schnellere und effizientere Kommunikation zur Verfügung zu stellen. Ziel des Intranet-Einsatzes ist es nicht, Leistung und Verhalten der Mitarbeiterinnen und Mitarbeiter zu überwachen. Ziel ist es auch nicht, Zahl oder Wertigkeit der Arbeitsplätze in der Dienststelle zu verringern oder Beschäftigungsbedingungen der Mitarbeiterinnen und Mitarbeiter in rechtlicher oder tatsächlicher Hinsicht zu verschlechtern.

Im Übrigen wird hinsichtlich der Aufgaben und Ziele des landeskirchlichen Intranets auf die entsprechenden Veröffentlichungen des Evangelischen Oberkirchenrats, auch auf seiner homepage, verwiesen (www.ekiba.de/vernetzung).

1. Geltungsbereich
Diese Dienstvereinbarung gilt für alle Mitarbeiterinnen und Mitarbeiter der Dienststelle im Sinne von § 5 Abs. 3 Unterabs. 2 Satz 1 Mitarbeitervertretungsgesetz.

2. Beteiligung am landeskirchenweiten Intranet

2.1 Die Dienststelle beteiligt sich ab 1. April 2005 am landeskirchenweiten Intranet (bislang: Projekt „Vernetzung der Landeskirche“). Die Dienststelle stellt den Mitarbeiterinnen und Mitarbeitern die nötigen Betriebsmittel zur Verfügung.

2.2 Die Dienststelle achtet darauf, dass Nachrichten, die personenbezogene Daten enthalten, per E-Mail nur über verschlüsselte Strecken oder Verbindungen verschickt werden.

2.3 Dienststelle und Mitarbeitervertretung stimmen darin überein, dass rechtsverbindliche Vorgänge sowie Vorgänge mit hohem Vertraulichkeitsgrad nur über besonders geschützte Verbindungen über das Internet im Intranet kommuniziert und/oder in zugriffsgeschützten Strukturen im Intranet abgelegt werden.

3. Qualifizierung
3.1 Die Dienststelle trägt dafür Sorge, dass die Mitarbeiterinnen und Mitarbeiter im Umgang mit dem landeskirchenweiten Intranet und zu dessen Nutzung innerhalb der allgemeinen Arbeitszeit ausreichend geschult werden.

3.2 Dienststelle und Mitarbeitervertretung stimmen darin überein, dass Schulungen nach Ziffer 3.1 dienstliche Fortbildungsmaßnahmen im Sinne von § 4 Abs. 2 Buchst. a der Arbeitsrechtsregelung zu Maßnahmen der beruflichen Fort- und Weiterbildung vom 24. März 2004 (AR-FWB) sind, sodass die Dienststelle etwaige Reisekosten trägt (§ 14 Abs. 1 AR-FWB).

3.3 Dienstelle und Mitarbeitervertretung sind darüber informiert, dass die Evangelische Landeskirche in Baden im Rahmen der Einführung des landeskirchenweiten Intranets die Kosten der Schulungen mit Ausnahme der Reisekosten trägt.

4. Datenauswertungen
4.1 Auswertungen von personenbezogenen Daten zur Systemevaluation sind zulässig.

4.2 Auswertungen von personenbezogenen Daten zum Zwecke der Leistungs- und/oder der Verhaltenskontrolle von Mitarbeiterinnen und Mitarbeitern der Dienststelle finden nur bei Verdacht einer Amtspflichtverletzung oder bei Verdacht einer Verletzung der arbeitsvertraglichen Pflichten statt. Die Mitarbeitervertretung und die betroffenen Mitarbeiterinnen bzw. Mitarbeiter sind vorab zu informieren. Ausnahmen hiervon sind nur bei Gefahr im Verzug möglich.

4.3 Erhält die Dienststelle zufällig oder unabsichtlich Kenntnis von Daten, die leistungs- oder verhaltensrelevant sein können, sind die Daten erst dann verwertbar, wenn im Sinne von 4.2 die Information der Mitarbeitervertretung und die Information des oder der Betroffenen erfolgt ist. Ausnahmen hiervon sind nur bei Gefahr im Verzug möglich.

5. Bestandsschutzabrede
Aus Anlass der Beteiligung der Dienststelle am landeskirchenweiten Intranet (Ziffer 2.1) und der Schulungen der Mitarbeiterinnen und Mitarbeiter (Ziffer 3.1) finden keine Änderungen hinsichtlich der Eingruppierung (einschließlich Festlegung der Fallgruppe, Wechsel der Fallgruppe, Umgruppierung) der Mitarbeiterinnen und Mitarbeiter statt.

6. Internet-Nutzungsvereinbarung
Die Dienststelle achtet darauf, dass alle Mitarbeiterinnen und Mitarbeiter eine Internet-Nutzungsvereinbarung unterzeichnen, die dem anliegenden Muster entspricht.

7. Nachwirkung
Sollte diese Dienstvereinbarung nach § 36 Abs. 5 Mitarbeitervertretungsgesetz gekündigt werden, wirkt sie nach, bis eine neue Dienstvereinbarung abgeschlossen ist.

8. In-Kraft-Treten
Diese Dienstvereinbarung tritt am 1. April 2005 in Kraft.

(Unterschriften)

Anlagen:
Internet-Nutzungsvereinbarung
Internet-Sicherheitsvereinbarung

Internet-Nutzungsvereinbarung

Von dem/der Antragsteller/in auszufüllen und dem/der Datenschutzbeauftragten bei der Evangelischen Landeskirche in Baden bzw. der personalverwaltenden Stelle zu übergeben.

Name:_____

Personal-Nr:_____

Dienststelle:_____

Abteilung:_____

Hiermit bestätige ich den Erhalt und die Kenntnisnahme der "Sicherheitsvereinbarung für die Nutzung des Internets" und der "Dienstvereinbarung über die Einführung des landeskirchenweiten Intranets" der Evangelischen Landeskirche in Baden. Mir ist bekannt, dass bei Verstößen gegen diese Vereinbarungen Maßnahmen entsprechend der Sicherheitsvereinbarung eingeleitet werden können.

Hierzu erkläre ich folgendes:

- Die für Anwender/innen relevanten Abschnitte der „Dienstvereinbarung über die Einführung des landeskirchenweiten Intranets“ und die „Sicherheitsvereinbarung für die Nutzung des Internets“ werden von mir eingehalten
- Ich handele bei der Nutzung des Internets im Sinne und Interesse der Evangelischen Landeskirche in Baden
- Meine Internet-Nutzung steht grundsätzlich in Zusammenhang mit meinem Auf-gabenumfeld
- Die Gefahren und Risiken bei der Internet-Nutzung sind mir bekannt

Datum:_____

Unterschrift:_____

Anlage:
Internet-Sicherheitsvereinbarung

Internet-Sicherheitsvereinbarung

1 Ziel und Zweck
Ziel und Zweck dieser Sicherheitsvereinbarung ist es, allen (internen und externen) Mitarbeiterinnen und Mitarbeitern einen Leitfaden in die Hand zu geben, damit sie sich bei der Nutzung des Internets verantwortungsbewusst im Sinne der Evangelischen Landeskirche in Baden verhalten können.
Bitte senden Sie die beigefügte Internet-Nutzungsvereinbarung im Original unterschrieben an den/die Datenschutzbeauftragte/n bei der Evangelischen Landeskirche in Baden.

2 Geltungsbereich
Diese Internet-Sicherheitsvereinbarung gilt für alle Mitarbeiterinnen und Mitarbeiter der Evangelischen Landeskirche in Baden im Sinne von §5 Abs. 3 Mitarbeitervertretungsgesetz, sofern sie einen Internet-Zugang nutzen. Sie ist Bestandteil der Dienstvereinbarung über die Einführung des landeskirchenweiten Intranets in der Evangelischen Landeskirche in Baden.

3 Hintergrund der Sicherheitsmaßnahmen
Das Internet ist ein rasant wachsendes Kommunikationsnetz mit allen Vor- und Nachteilen eines offenen weltweiten Netzes. Nützliche wie auch unwichtige, sogar kriminelle Informationen sind verfügbar.
Die erste Priorität der unternehmensweiten Sicherheit beim Internet hat zum Ziel, Mitarbeiterinnen und Mitarbeitern ein Höchstmaß an Transparenz für das Internet bei gleichzeitigem Schutz unternehmensinterner Systeme und Informationen zu bieten.

4 Gefahrenpotential
Es ist wichtig, sich der Tatsache bewusst zu sein, dass
das Internet auch von Personen benutzt wird, die nicht immer das Wohl des Unter-nehmens im Auge haben;
alle über das Internet (über ungeschützte Verbindungen) ausgetauschten Informationen von einer Vielzahl unbekannter Personen (Kriminelle, Spione, Saboteure, Geheimdienste etc.) gelesen und missbraucht werden können;
die Computer-Viren, Computer-Würmer, Trojanische Pferde oder sonstige Schädlinge über das Internet unkontrolliert verbreitet und große materielle und immaterielle Schäden verursachen können.

5 Sicherheitsmaßnahmen der Evangelischen Landeskirche in Baden
Ein Schutz vor den möglichen Gefahrenpotentialen in der Evangelischen Landeskirche in Baden kann nur dann gewährleistet werden, wenn alle betroffenen Mitarbeiterinnen und Mitarbeiter mit PC-Arbeitsplätzen und Internet-Zugang diese Sicherheitsvereinbarung beachten und danach handeln.

6 Verantwortlichkeit für den Computer-Arbeitsplatz
Jeder Computer-Arbeitsplatz ist einer Benutzerin bzw. einem Benutzer zugeordnet. Für jeden Arbeitsplatz gibt es mindestens eine verantwortliche Person, in der Regel ist das die Besitzerin, bzw. der Besitzer. Die Besitzerin / der Besitzer ist für die Beachtung der Vorschriften und Arbeitsanweisungen des Unternehmens verantwortlich.

7 Nutzung von zugelassener Hard- und Software
Jeder Computer-Arbeitsplatz darf grundsätzlich nur die vom Unternehmen zugelassene bzw. genehmigte Hard- und Software beinhalten. Diese sind alle offiziell erworbenen, lizenzierten, überlassenen bzw. selbstentwickelten Hard- und Softwareprodukte. Erweiterungen, die Fremdanschlüsse schaffen, sind genehmigungspflichtig (siehe Genehmigungen).

8 Schutz vor unbefugtem Zugriff
Jede/r Mitarbeiter/in hat ihren/seinen Computer-Arbeitsplatz vor unbefugtem Zugriff mittels Passwort zu schützen. Das Passwort ist vertraulich zu behandeln.

9 Internet-Zulassung
Aufgrund der schnell verändernden Internet-Technologien muss jeder neue Dienst durch die Netzwerk-Betreiber auf Sicherheitsrelevanz überprüft werden, bevor er zum Einsatz kommt.
Für die Internet-Zulassung muss die/der Benutzer/in die Internet-Sicherheitsvereinbarung anerkennen. Es sind sinngemäß folgende Verpflichtungserklärungen abzugeben:
die Benutzerin /der Benutzer handelt im Sinne und im Interesse des Unternehmens,
die Benutzung steht grundsätzlich im Zusammenhang mit dem Aufgabenumfeld,
der Benutzerin /dem Benutzer sind die Gefahren und Risiken im Internet bekannt.

10 Berechtigung für Internet-Dienste
Zum Internet gehören verschiedene Internet-Dienste, z.B.:

- E-Mail
- WWW
- FTP
- News
- Telnet

Die Benutzerin / der Benutzer ist nach Anerkennung der Internet-Sicherheitsvereinbarung berechtigt, die zugelassenen Dienste entsprechend ihrem jeweiligen Zweck in Anspruch zunehmen.

11 Speicherung von Internet-Zugriffen

11.1 Jede Benutzeraktivität bzw. Transaktion im Internet wird gespeichert (protokolliert) und für die Zeitdauer von 6 Monaten aufbewahrt. Somit ist die Nutzung, das Speichern und Herunterladen von Software, Dateien und Internet-Seiten nachweisbar. Dieses Logging-Verfahren ist notwendig, um potentielle Angriffe (Hacking, Spionage, Sabotage, etc.) festzustellen und an die zuständigen Strafverfolgungsbehörden weiterleiten zu können (siehe Auswertung).
11.2 Die Inhalte von E-Mails und Dateien sind von der Protokollierung unberührt.
11.3 In einem Servicefall ist die EDV-Betreuung berechtigt, den jeweiligen PC zu überprüfen und ggf. Änderungen vorzunehmen.

12 Auswertung von Internet-Zugriffen
Die gespeicherten Internet-Zugriffe (Protokolldaten) dürfen laut Bundesdatenschutzgesetz (BDSG § 31) und kirchliches Datenschutzgesetz sowie Mitarbeitervertretungsgesetz (div. Mitbestimmungsrechte) Dienstvereinbarung über die Einführung des landeskirchenweiten Intranets nicht zur Auswertung personenbezogener Daten verwendet werden.
Im Hinblick auf die Wahrung der Interessen der Mitarbeiterinnen und Mitarbeiter und im Sinne des Datenschutzes werden folgende Maßnahmen ergriffen:

12.1 Zugriff auf gespeicherte Daten
Es wird gewährleistet, dass nur autorisierte Personen in begründeten Fällen die gespeicherten Daten einsehen und auswerten. Die Auswertung der gespeicherten Daten erfolgt unter Einbindung der Mitarbeitervertretung und der Geschäftsleitung bzw. einer von ihr beauftragten Person. Über die Auswertung wird die/der betroffene Mitarbeiter/in informiert. Es wird ein ausführliches Protokoll über die Auswertung erstellt. Die/der betroffene Mitarbeiter/in erhält eine Kopie dieses Protokolls.

12.2 Speicherungsdauer der Daten
Die gespeicherten Daten werden vor dem Zugriff nicht autorisierter Personen geschützt aufbewahrt. Die Aufbewahrungsdauer der Daten beträgt maximal 6 Monate. (Auswertungen sind jedoch nur in den ersten 90 Tagen nach Speicherung zulässig.) Sofern aufgrund allgemeiner Vorgaben (z.B. gesetzliche Auflagen) eine längere Aufbewahrungsfrist erforderlich wird, wird diese der Mitarbeitervertretung rechtzeitig vorher unter Angabe der Gründe mitgeteilt. Nach Ablauf der Aufbewahrungsfrist werden die gespeicherten Daten im Sinne des Bundesdatenschutzgesetzes gelöscht.
12.3 Leistungs- und Verhaltenskontrolle
Eine Verhaltens- oder Leistungskontrolle der Mitarbeiterinnen und Mitarbeitern durch Auswertung der gespeicherten Daten erfolgt nur aus konkretem Anlass und in Abstimmung mit der Mitarbeitervertretung. Die betroffenen Mitarbeiterinnen und Mitarbeiter sind zu informieren. (vergl. Abschnitt 3 der Dienstvereinbarung über die Einführung des landeskirchenweiten Intranets).

13 Maßnahmen bei Verstößen gegen die Arbeitsanweisung
13.1 Die Zugangsberechtigung erlischt, wenn das Internet fahrlässig und unzulässig für solche Zwecke eingesetzt wird, die das Unternehmen materiell bzw. immateriell schädigen, und damit gegen diese Internet-Sicherheitsvereinbarung verstoßen wird.
13.2 Bei schweren Verstößen oder Missbrauchsfällen können neben dem Internet-Zulassungsentzug disziplinarrechtliche oder arbeitsrechtliche Maßnahmen eingeleitet werden. Zum schweren Verstoß gehört die grobe Fahrlässigkeit bzw. Missbrauch bezogen auf die Nutzung, die Speicherung und die Weitergabe der folgenden Daten:

- sittenwidrige, obszöne und respektlose Angebote,
- menschenverachtende und rassistische Propagandadaten,
- Sekten-Propaganda bzw. -Mitgliederwerbung jeder Art,
- unbefugtes Software-Herunterladen für Privatzwecke, wenn dadurch grob fahrlässig Lizenzrechte verletzt werden (widerrechtliche Nutzung gebührenpflichtiger Software).
-

14 Definitionen der Begriffe
Autorisierte Personen
Die "autorisierten Personen" für die Auswertung im Sinne dieser Internet-Sicherheitsvereinbarung sind die Systemadministrator/innen der Evangelischen Landeskirche in Baden.

Auswertung
Eine Auswertung im Sinne dieser Internet-Sicherheitsvereinbarung ist notwendig, sofern die gespeicherten Internet-Zugriffe zur Feststellung der potentiellen Angriffe (z.B. Hacking, Spionage, Sabotage) bzw. der schweren Verstöße gegen diese Internet-Nutzungsvereinbarung es erforderlich machen, grobe Fahrlässigkeit bzw. den Missbrauchsfall unter Einbindung der Mitarbeitervertretung und der Geschäftsleitung bzw. einer von ihr beauftragten Person zu überprüfen bzw. nachzuweisen.

Besitzer/in
Besitzer/in eines Computer-Arbeitsplatzes ist in der Regel ein Mitarbeiter oder eine Mitarbeiterin.
Computer-Arbeitsplatz
Computer-Arbeitsplätze sind Systeme im Sinne dieser Internet-Nutzungsvereinbarung, wenn sie in festen bzw. mobilen Arbeitsumgebungen Zugriff auf das Internet haben (PC, Notebook, Laptop, NC, usw.).

Computer-Viren
Computer-Viren gehören zu den Programmen mit

Schadensfunktionen. Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender/von der Anwenderin nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Ein Virus infiziert andere Programme mit einer Kopie von sich selbst. Bösartige Viren beschädigen andere Programme oder Daten, löschen die Plattenverzeichnisstruktur oder richten andere Schäden an. Die verschiedenen Virentypen sind:
Programm-Viren: Fügen sich als bestehende Programmdateien auf Speichermedien ein und werden beim Aufruf des Wirtsprogramms ausgeführt.
System-Viren: Befallen Systembereiche (Bootsektor, Master-Boot-Sektor, Partitionstabelle) von Disketten oder Festplatten.
Direct-Action-Viren: Infizieren bei der Ausführung des infizierten Programms sofort weitere Programmdateien, führen sofort eine Schadensroutine aus und geben dann wieder die Kontrolle an das Gast-Programm ab.
Stealth-Viren: Versuchen ihr Vorhandensein im System zu verbergen. Dazu überwachen sie die Systemaktivitäten und verschleiern ihre Existenz.
Polymorphe-Viren: Verschlüsseln infizierte Programmteile, um zu verhindern, dass Antiviren-Programme die Virus-typischen Merkmale entdecken. Manche Viren verwenden eine Technik ("Tunneling") um die Antiviren-Überwachungsprogramme zu umgehen.
Slow-Viren: Führen erst nach einem längeren Zeitraum ihre Schadensroutine aus.
Makro-Viren: Werden auf der Basis der in vielen Software-Produkten integrierten Makro-Sprachen entwickelt. Sie "klinken" sich z.B. in Formatvorlagen von Textverarbeitungssystemen (z.B. WinWord-Dokument) ein. Sie sind nicht in der Lage, ohne eine spezifische Makro-Ausführungumgebung zu laufen.
Computer-Würmer: Bei Computer-Würmern handelt es sich um Störprogramme, die sich selbstständig in einem Computer-Netzwerk ausbreiten. Diese Störprogramme können sich reproduzieren und mit Hilfe von Netzwerkfunktionen sich selbst auf andere Computer kopieren. Die Programm-Kopien können sogar andere Funktionen übernehmen als das Ursprungsprogramm.
Datenträgermedium und -laufwerk Datenträgermedium ist das Speichermedium für die Daten und Programme (Festplatte, Floppy-, Diskette, PCMCIA, CD, Zip-Medium, Jaz-Medium, Streamer-Cassette, Magneto-Optische Platte usw.). Datenträgerlaufwerk ist das jeweilige Steuerungsinstrument des Datenträgers zum Lesen und Speichern von Daten und Programmen.

Firewall
Ein Firewall als zentraler Übergang zum Internet ist eine Kombination von Hardware- und Software-Komponenten, der eine sichere Verbindung zwischen einem Netzwerk und anderen Netzwerken erlaubt. Die Systemkonfiguration und die Filterregeln müssen gewährleisten, dass nur die erlaubten Verbindungen zugelassen werden.

Fremdanschlüsse
Möglichkeit, über definierte Kommunikations-schnittstellen (z.B. externe/interne Modems und ISDN-Geräte) externe DV-Einrichtungen (z.B. Rechnersysteme, Internet) zu erreichen bzw. von ihnen erreicht zu werden. Fremdanschlüsse sind alle nicht Primär- oder Sekundär-Datennetze zu den Benutzer/innen der Evangelischen Landeskirche in Baden. Fremdanschlüsse sind von der Evangelischen Landeskirche in Baden zu genehmigen.

Internet-Dienste
WWW (World Wide Web) - Leicht bedienbare Anwenderprogramme, die den Zugriff auf Informationen mit Hilfe des Protokolls HTTP (HyperText Transfer Protocol) ermöglicht
E-Mail (Electronic Mail) - Ein Internet-Dienst zum Versenden und Empfangen von elektronischen Nachrichten
FTP (File Transfer Protocol) - Ein Internet-Dienst zur Übertragung von Dateien von und zu entfernten Rechnern
News - Ein Internet-Dienst als Diskussionsforum zu verschiedenen Themen, an denen jede/r Internet-Benutzer/in teilnehmen kann
Telnet - Ein Internet-Dienst zum Einloggen und Arbeiten auf einem entfernten Rechner

Modem und ISDN-Gerät
Modems (Modulator-Demodulator) und ISDN-Geräte (Integrated Services Digital Network) sind Datenübertragungsgeräte. Sie ermöglichen die Übertragung von Dateien über die Telefonleitung, indem sie diese mit dem PC verbinden.

Nettikette
Das Internet ist kein anonymes Medium, auch wenn der Eindruck entstehen mag. Die „Nettikette“ ist ein Verhaltenskodex für die Nutzung des Internets und erinnert daran, dass das Internet öffentlich ist. Daneben beschreibt und erläutert sie gebräuchliche Abkürzungen und Symbole, die in Newsgroups verwendet werden.
Newsgroup
Newsgroup ist die englische Bezeichnung für Diskussionsforen bzw „Schwarze Bretter“ im Internet. Diese Diskussionsforen sind ein spezieller Internet-Dienst, der neben dem World Wide Web der Diskussion und Information bestimmter Themen dient. Inzwischen finden sich im Netz mehrere Zig-Tausend Newsgroups zu allen erdenklichen Themen.

Protokollierung
Die Protokollierung im Sinne dieser Internet-Sicherheitsvereinbarung liegt vor, sofern die Daten über die Internet-Zugriffe gespeichert und verwendet werden, um diese später auswerten zu können.

Trojanische Pferde
Trojanische Pferde sind Sabotage-Programme, die unter falschem Namen bzw. falscher Identität ins Computersystem gelangen. Somit ermöglichen sie einer unberechtigten Person den Zugriff auf Daten im Netz oder auf einem PC.

siehe auch *Bildschirmarbeitsverordnung* **aufgrund des** *Arbeitsschutzgesetzes* **vom 7.8.96**
zu finden im Internet unter **http://www.ekiba.de/mav/bapv.htm**

Tarifvertrag über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen mit Geräten der Informations- und Kommunikationstechnik

vom 25. Januar 1990

zwischen
der Tarifgemeinschaft deutscher Länder, vertreten durch den Vorsitzenden des Vorstandes,
einerseits
und
der Gewerkschaft Öffentliche Dienste, Transport und Verkehr (ÖTV), Bezirk Baden-Württemberg
andererseits
wird folgendes vereinbart:

§ 1 Geltungsbereich

Dieser Tarifvertrag gilt für Arbeitnehmer des Landes Baden-Württemberg, die unter den Geltungsbereich
a) des Bundes-Angestelltentarifvertrages (BAT) fallen oder
b) des Manteltarifvertrages für Arbeiter der Länder(MTLII) fallen und deren arbeitsvertraglich vereinbarte durchschnittliche regelmäßige wöchentliche Arbeitszeit mindestens 18 Stunden beträgt,

wenn sie auf Arbeitsplätzen mit Geräten der Informations- und Kommunikationstechnik eingesetzt werden bzw. ihr Einsatz auf solchen Arbeitsplätzen vorgesehen ist.

Niederschriftserklärung:

Zwischen den Tarifvertragsparteien besteht Einvernehmen, daß auf Angestellte, die aufgrund des § 3 q BAT vom Geltungsbereich des BAT und damit auch aus dem Geltungsbereich der vorliegend vereinbarten Tarifverträge ausgenommen sind, die 0 4 und 6 Abs. 3 und 4 sowie die ff 7 und 8 (Baden-Württemberg und Niedersachsen) bzw. die ff 5 und 7 Abs. 3 und 4 sowie die §§ 8 und 9 (Schleswig-Holstein) anzuwenden sind, wenn die Teilzeitarbeit ganztägig abgeleistet wird und die Angestellten überwiegend am Bildschirmarbeitsplatz eingesetzt sind.

Niederschrift über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23. 2. 1990: § 1 abschließend

§ 2 Begriffsbestimmungen

(1) Als Geräte der Informations- und Kommunikationstechnik im Sinne dieses Tarifvertrages werden angesehen:
a) Bildschirmgeräte aller Art
und
b) Datenverarbeitungsanlagen,
die auf elektronischem Wege Zeichen aufnehmen, speichern und/oder verarbeiten und/oder wiedergeben und/oder weitergeben.

(2) Bildschirmgeräte sind Geräte zur veränderlichen Anzeige von Zeichen oder graphischen Bildern, wie Bildschirmgeräte mit Kathodenstrahl- oder Plasmaanzeige oder vergleichbare Geräte. Als Bildschirmgeräte im Sinne dieses Tarifvertrages gelten auch Mikrofilm-Lesegeräte für Rollfilme, Mikrofiches und vergleichbare Systeme.

(3) Nicht zu den Bildschirmgeräten im Sinne dieses Tarifvertrages gehören Fernsehgeräte, Monitore und Digitalanzeigegeräte sowie vergleichbare Anzeige- und Überwachungsgeräte, es sei denn, sie werden in bestimmendem Maße für die digitale Daten- und Textverarbeitung eingesetzt.

(4) Bildschirm-Arbeitsplätze sind Arbeitsplätze, bei denen die Tätigkeiten, die mit und an Bildschirmgeräten zu erledigen sind, bestimmend für die gesamte Tätigkeit der Arbeitnehmer sind. Dies ist der Fall, wenn die Arbeitnehmer mit durchschnittlich mindestens der Hälfte ihrer Wochenarbeitszeit an diesen Geräten eingesetzt werden. Bildschirmarbeiten sind alle Tätigkeiten, die fast dauernden Blickkontakt zum Bildschirm oder laufenden Blickwechsel zwischen Bildschirm und Vorlage voraussetzen.

(5) Arbeitsplätze mit Bildschirmunterstützung sind alle Arbeitsplätze, bei denen mit Bildschirmgeräten gearbeitet wird, aber die Tätigkeiten mit und an Bildschirmgeräten nicht bestimmend für die gesamte Tätigkeit der Arbeitnehmer sind.

(6) Mischarbeitsplätze sind Arbeitsplätze, an denen sowohl Tätigkeiten mit und an Bildschirmgeräten als auch andere Tätigkeiten zu erledigen sind.

Protokollnotiz zum Absatz 1 Buchst. a:

Zu den Bildschirmgeräten im Sinne des Absatzes 1 Buchst. a gehören auch textverarbeitende Systeme. Ein textverarbeitendes System ist ein Bürogerät oder eine Büroanlage für die Ein- und Ausgabe und die Textverarbeitung mit mindestens folgenden Einrichtungen:

- Eingabeeinrichtung,

- Einrichtung, die mit Hilfe von Programmen die Textverarbeitung durchführen kann,
- Textträger zur Speicherung von Texten,
- Ausgabeeinrichtung.

Ein textverarbeitendes System im vorstehenden Sinne erfordert mindestens einen Halbseitenbildschirrn (ca. 20 bis 24 Zeilen).

Protokollnotiz zum Absatz 1 Buchst. b:

Für Datenverarbeitungsanlagen im Sinne des Absatzes 1 Buchst. b gilt die in den Allgemeinen Vorbemerkungen des Teils II Abschn. B der Anlage 1a zum BAT enthaltene Begriffsbestimmung.

Niederschrift über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23. 2. 1990: § 2 abschließend

§ 3 Ausstattung und Gestaltung der Arbeitsplätze

(1) Bildschirm-Arbeitsplätze und Arbeitsplätze mit Bildschirmunterstützung müssen den allgemein anerkannten Regeln der Technik unter Beachtung der gesicherten arbeitsmedizinischen und ergonomischen Erkenntnisse entsprechen. Auf diese Arbeitsplätze sind die "Sicherheitsregeln für Bildschirm-Arbeitsplätze im Bürobereich (GUV 17.8)", herausgegeben vom Bundesverband der Unfallversicherungsträger der öffentlichen Hand e.V., BAGUV, anzuwenden.

Niederschrift über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23. 2. 1990: § 3 Abs. 1 abschließend

(2) Bildschirm-Arbeitsplätze sollen, soweit dies arbeitsorganisatorisch sinnvoll ist, als Mischarbeitsplätze (§ 2 Abs. 6) so gestaltet werden, daß Bildschirmarbeit mit anderen Arbeiten in ähnlichem Umfang abwechselt.

Protokollnotiz zu Absatz 1:

Von den Anforderungen kann abgesehen werden, wenn ein Bildschirmgerät von den jeweiligen Arbeitnehmern nur gelegentlich zu kurzen Eingaben oder Abfragen benutzt wird.

Niederschrift über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23. 2.1990:

§ 3 Abs. 2: nicht abschließend (ergänzende Regelungen in Dienstvereinbarungen sind zulässig, soweit es um die Einrichtung von Mischarbeitsplätzen geht, bei denen dies arbeitsorganisatorisch sinnvoll ist).

§ 4 Ärztliche Untersuchungen

(1) Vor der Aufnahme einer nicht nur vorübergehenden Tätigkeit auf einem Bildschirm-Arbeitsplatz oder einem Arbeitsplatz mit Bildschirmunterstützung ist eine ärztliche Untersuchung der Augen durchzuführen. Der Arbeitnehmer ist verpflichtet, sich auf Veranlassung des Arbeitgebers der ärztlichen Untersuchung der Augen zu unterziehen.

(2) Eine erneute Untersuchung der Augen ist nach dreijähriger Tätigkeit auf einem Bildschirm-Arbeitsplatz oder einem Arbeitsplatz mit Bildschirmunterstützung seit der jeweils letzten Untersuchung, sonst bei gegebener Veranlassung, vorzunehmen.

(3) Die Untersuchungen nach den Absätzen 1 und 2 werden vom personalärztlichen oder betriebsärztlichen Dienst durchgeführt, der erforderlichenfalls eine weitergehende augenärztliche Untersuchung veranlaßt. Besteht kein personalärztlicher oder betriebsärztlicher Dienst, ist die Untersuchung durch einen Augenarzt am Beschäftigungsort bzw. dem nächstgelegenen Ort nach Wahl des Arbeitnehmers durchzuführen.

(4) Die Kosten der Untersuchung trägt der Arbeitgeber, soweit kein anderer Kostenträger zuständig ist. Dies gilt auch für die notwendigen Kosten der Beschaffung von Sehhilfen, die aufgrund der Untersuchung ausschließlich für die Tätigkeit am Bildschirmgerät erforderlich werden.

Protokollnotiz zu Absatz 4:

Als notwendig gelten in der Regel die Kosten, die die örtliche zuständige Allgemeine Ortskrankenkasse bzw. die zuständige Betriebskrankenkasse jeweils tragen würde.

Niederschrift über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23.2.1990: § 4 abschließend

§ 5 Einweisung und Einarbeitung

Vor Aufnahme der Tätigkeit an Geräten der Information- und Kommunikationstechnik sowie vor technischen und organisatorischen Änderungen beim Einsatz dieser Geräte sind die betroffenen Arbeitnehmer rechtzeitig und umfassend über ihre Aufgabe, die Arbeitsmethode und die Handhabung der Geräte theoretisch und praktisch zu unterrichten. Den Arbeitnehmern ist für die Einarbeitung ausreichend Zeit und Gelegenheit zu geben. Die Unterrichtung und die Einarbeitung sollen während der Arbeitszeit stattfinden. Finden sie ausnahmsweise außerhalb der Arbeitszeit statt, sind sie auf die Arbeitszeit anzurechnen. Etwaige Kosten trägt der Arbeitgeber.

Niederschrift über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23. 2. 1990:

§ 5: nicht abschließend (**ergänzende Regelungen in Dienstvereinbarungen sind zulässig**, soweit es um die Mitbestimmungstatbestände des **§ 79 Abs. 3 Nr. 6 oder 7 LPVG** geht).

§ 6 Schutzvorschriften

(1) Der geplante erstmalige Einsatz auf einem Bildschirm-Arbeitsplatz bedarf der Zustimmung des Arbeitnehmers, wenn dieser das 55. Lebensjahr bereits vollendet hat. Die Zustimmung kann innerhalb einer Frist von 12 Monaten nach Arbeitsaufnahme schriftlich widerrufen werden. Nach erfolgtem Widerruf darf der Arbeitnehmer für die Dauer von drei Monaten auf dem Bildschirm-Arbeitsplatz weiterbeschäftigt werden.

(2) Die Umstellung der Tätigkeit eines Arbeitnehmers auf eine Tätigkeit an einem Gerät der Informations- und Kommunikationstechnik soll so vorgenommen werden, daß die bisherige Eingruppierung nicht beeinträchtigt wird.
(3) Kann ein Arbeitnehmer aufgrund einer erneuten Untersuchung nach § 4 Abs. 2 nicht mehr auf einem Bildschirm-Arbeitsplatz oder einem Arbeitsplatz mit Bildschirmunterstützung oder aufgrund eines Widerrufs nach Absatz 1 Satz 2 nicht mehr auf einem Bildschirm-Arbeitsplatz eingesetzt werden, ist er auf einen anderen, möglichst gleichwertigen Arbeitsplatz umzusetzen. Dem Arbeitnehmer ist ausreichend Zeit und Gelegenheit zur Einarbeitung auf dem neuen Arbeitsplatz zu geben; Maßnahmen der Fort- oder Weiterbildung sind durchzuführen.
(4) Werdende Mütter sollen auf ihren Wunsch von der Bildschirmarbeit befreit werden, soweit dies arbeitsorganisatorisch möglich ist. Sie dürfen an Bildschirmgeräten nicht beschäftigt werden, soweit nach ärztlichem Zeugnis eine Gesundheitsgefährdung besteht. Nach Beendigung der Schutzfristen nach dem Mutterschutzgesetz oder nach Ablauf des Erziehungsurlaubs nach dem Bundeserziehungsgeldgesetz sollen sie die Möglichkeit erhalten, auf einen vergleichbaren Bildschirm-Arbeitsplatz zurückzukehren.
(5) Die tariflichen Vorschriften über den Rationalisierungsschutz werden durch diesen Tarifvertrag nicht berührt.

Protokollnotiz zu Absatz 3:
Für den Begriff gleichwertiger Arbeitsplatz" gilt § 3 Abs. 2 Unterabs. 2 des Tarifvertrages über den Rationalisierungsschutz für Angestellte vom 9. Januar 1987

Niederschrift Über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23. 2. 1990:
§ 6: abschließend mit Ausnahme des § 6 Abs. 3 letzter Satz (siehe zu § 5). Schreiben des Finanzministeriums vom 9. März 1990 an die ÖTV-Bezirksverwaltung Aktenzeichen P 7060 – 11188
Zu § 6 Abs. 2 des Tarifvertrages bestand in der Besprechung Übereinstimmung, daß ggf. die Mitbestimmung nach **§ 76 Abs. 1 Nr. 2 LPVG** unberührt bleibt.

§ 7 Verhaltens- und Leistungskontrolle
(1) Technische Möglichkeiten, mit denen Geräte und Programme der Informations- und Kommunikationstechnik vom Hersteller angeboten werden und die sich zur Kontrolle der Leistung oder des Verhaltens der Bedienungskräfte eignen, die jedoch nicht zur Aufgabenerfüllung vorgesehen werden sollen, werden nicht genutzt, soweit sich nicht aus den Absätzen 2 und 3 etwas anderes ergibt.
(2) Personenbezogene Daten, die ausschließlich zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage mit Hilfe von Geräten der Informations- und Kommunikationstechnik gespeichert werden, dürfen nicht zur individuellen Leistungskontrolle der Bedienungskräfte und zur Kontrolle ihres Verhaltens nur insoweit verwendet werden, als dies zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage erforderlich ist.
(3) Die Einschränkungen für Kontrollmaßnahmen gelten nicht, wenn Tatsachen bekannt werden, die den Verdacht einer Dienst- bzw. Arbeitspflichtverletzung rechtfertigen.

Niederschrift über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23. 2. 1990:
§ 7: abschließend, soweit die Leistungs- und Verhaltenskontrolle dort tatbestandlich konkretisiert ist; ergänzende Regelungen in **Dienstvereinbarungen im Rahmen der Mitbestimmung** nach **§ 79 Abs. 3 Nr. 9 und 13 LPVG** sind zulässig.

§ 8 Arbeitsunterbrechungen
(1) Einem Arbeitnehmer auf einem Bildschirm-Arbeitsplatz ist jeweils nach 50minütiger Tätigkeit, die einen fast dauernden Blickkontakt zum Bildschirm oder einen laufenden Blickwechsel zwischen Bildschirm und Vorlage erfordert, Gelegenheit zu einer Unterbrechung dieser Tätigkeit von zehn Minuten zu geben. Unterbrechungen nach Satz 1 entfallen, wenn Pausen und sonstige Arbeitsunterbrechungen sowie Tätigkeiten, die die Beanspruchungsmerkmale des Satzes 1 nicht erfüllen, anfallen.
Die Unterbrechungen dürfen nicht zusammengezogen und nicht an den Beginn oder das Ende einer Pause oder der täglichen Arbeitszeit des Arbeitnehmers gelegt werden.
(2) Unterbrechungen nach Absatz 1 Unterabs. 1 Satz 1 werden auf die Arbeitszeit angerechnet.
(3) Die Absätze 1 und 2 gelten für Arbeitnehmer auf Arbeitsplätzen mit Bildschirmunterstützung entsprechend, sofern die Tätigkeit am Bildschirm im Sinne des Absatzes 1 Satz 1 über eine fortlaufende Zeit von wenigstens zwei Stunden auszuüben ist.

Niederschrift über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23. 2. 1990: § 8 abschließend

§ 9 Übergangs- und Schlußvorschriften
(1) Bildschirmgeräte und Arbeitsmittel, die den Anforderungen des § 3 Abs. 1 nicht entsprechen, können bis zum Ablauf ihrer Nutzungsdauer weiter verwendet werden. Möglichkeiten, eine den allgemein anerkannten Regeln der Technik entsprechende Umrüstung mit einem wirtschaftlich vertretbaren Aufwand durchzuführen, sollen im Rahmen der zur Verfügung stehenden Mittel genutzt werden. Wird

festgestellt, daß Mängel eines Bildschirmgerätes zu gesundheitlichen Beeinträchtigungen führen, darf das Gerät nicht mehr genutzt werden.
(2) Die ärztliche Untersuchung der Augen nach § 4 Abs. 1 ist bei Arbeitnehmern, die beim Inkrafttreten dieses Tarifvertrags bereits auf einem Bildschirm-Arbeitsplatz oder einem Arbeitsplatz mit Bildschirmunterstützung tätig sind, nachzuholen, wenn eine ärztliche Untersuchung der Augen nach den bisher geltenden Regelungen noch nicht durchgeführt worden ist. Ist die ärztliche Untersuchung bei den in Satz 1 genannten Arbeitnehmern vor Inkrafttreten dieses Tarifvertrags durchgeführt worden, so rechnen die Fristen für die erneute Untersuchung ab dieser Untersuchung.

Niederschriftserklärung:

Zwischen den Tarifvertragsparteien besteht Einvernehmen, daß die nach dem jeweiligen Personalvertretungsgesetz oder dem Betriebsverfassungsgesetz zulässigen Dienst- oder Betriebsvereinbarungen durch das Inkrafttreten dieser Tarifverträge nicht berührt werden.

Niederschrift über die Besprechung mit dem Finanzministerium Baden-Württemberg am 23. 2. 1990:

§ 9: abschließend mit Ausnahme des § 9 Abs. 1 Satz 2 (ergänzende Regelungen in Dienstvereinbarungen zur Frage der Umrüstung von Bildschirmgeräten und Arbeitsmitteln nach den allgemein anerkannten Regeln der Technik sind zulässig).

§ 10 Inkrafttreten, Laufzeit

(1) Dieser Tarifvertrag tritt am 1. Mai 1990 in Kraft.
(2) Dieser Tarifvertrag tritt außer Kraft, sobald ein Tarifvertrag für den Bereich der Tarifgemeinschaft deutscher Länder abgeschlossen wird, der Arbeitsbedingungen beim Einsatz von Geräten der Informations- und Kommunikationstechnik regelt. Für diesen Fall wird die Nachwirkung nach §4 Abs. 5 des Tarifvertragsgesetzes ausgeschlossen. Im übrigen kann der Tarifvertrag mit einer Frist von drei Monaten zum Ende eines Kalenderjahres schriftlich gekündigt werden.

Auszug aus dem Landespersonalvertretungsgesetz Baden-Württemberg:

(Anmerkung zum Verweis des § 6 TV IuK: Der Verweis entspricht § 42 Buchst. c bis f MVG)

§ 76 Mitbestimmung in Personalangelegenheiten der Angestellten und Arbeiter

(1) Der Personalrat hat mitzubestimmen in Personalangelegenheiten der Angestellten und Arbeiter bei

1. Einstellung und, soweit tarifvertraglich nichts anderes bestimmt ist, Eingruppierung,
2. nicht nur vorübergehender Übertragung einer Tätigkeit, die den Tätigkeitsmerkmalen einer höheren oder einer niedrigeren Vergütungs- oder Lohngruppe entspricht als die bisherige Tätigkeit, übertariflicher Eingruppierung, Herabgruppierung im Einverständnis mit dem Angestellten oder Arbeiter,
3. Versetzung zu einer anderen Dienststelle,
4. Umsetzung innerhalb der Dienststelle, wenn sie mit einem Wechsel des Dienstorts verbunden ist,
5. (gestrichen)
6. (gestrichen)
7. Weiterbeschäftigung über die Altersgrenze hinaus,
8. Anordnungen, welche die Freiheit in der Wahl der Wohnung beschränken,
9. Versagung oder Widerruf der Genehmigung einer Nebentätigkeit.

(2) Absatz 1 Nr. 1 findet keine Anwendung, wenn das Arbeitsverhältnis voraussichtlich nicht länger als drei Monate bestehen wird. In den Fällen des Absatzes 1 Nr. 3, gilt § 75 Abs. 2 entsprechend.

§ 79 Mitbestimmungen in sonstigen Angelegenheiten

(1) Der Personalrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, mitzubestimmen über

1. Beginn und Ende der täglichen Arbeitszeit und der Pausen sowie die Verteilung der Arbeitszeit auf die einzelnen Wochentage,
2. Zeit, Ort und Art der Auszahlung der Dienstbezüge und Arbeitsentgelte,
3. Aufstellung des Urlaubsplans,
4. Festsetzung der zeitlichen Lage des Erholungsurlaubs für einzelne Beschäftigte, wenn zwischen dem Leiter der Dienststelle und den beteiligten Beschäftigten kein Einverständnis erzielt wird,
5. Fragen der Lohngestaltung innerhalb der Dienststelle, insbesondere durch Aufstellung von Entlohnungsgrundsätzen, die Einführung und A nwendung von neuen Entlohnungsmethoden und deren Änderung sowie die Festsetzung der Akkord- und Prämiensätze und vergleichbarer leistungsbezogener Entgelte einschließlich der Geldfaktoren,
6. Bestellung von Vertrauens- und Betriebsärzten als Angestellte,
7. (gestrichen)
8. Maßnahmen zur Verhütung von Dienst- und Arbeitsunfällen, Berufskrankheiten und sonstigen Gesundheitsschädigungen,
9. Maßnahmen zur Hebung der Arbeitsleistung und Erleichterung des Arbeitsablaufs,
10. Einführung grundsätzlich neuer Arbeitsmethoden,
11. Aufstellung von Sozialplänen einschließlich Plänen für Umschulungen zum Ausgleich oder zur Milderung von wirtschaftlichen Nachteilen, die dem Beschäftigten infolge von Rationalisierungsmaßnahmen entstehen,
12. Regelung der Ordnung in der Dienststelle und des Verhaltens der Beschäftigten,

13. Grundsätze über die Bewertung von anerkannten Vorschlägen im Rahmen des behördlichen Vorschlagwesens.

Muss für Gruppen von Beschäftigten die tägliche Arbeitszeit (Satz 1 Nr. 1) nach Erfordernissen, die die Dienststelle nicht voraussehen kann, unregelmäßig und kurzfristig festgesetzt werden, so beschränkt sich die Mitbestimmung auf die Grundsätze für die Aufstellung der Dienstpläne, insbesondere für die Anordnung von Dienstbereitschaft, Mehrarbeit und Überstunden.

(2) Arbeitsentgelte und sonstige Arbeitsbedingungen, die durch Tarif geregelt sind oder üblicherweise geregelt werden, können nicht Gegenstand einer Dienstvereinbarung (§ 73) ein. Dies gilt nicht, we nn ein Tarifvertrag den Abschluss ergänzender Dienstvereinbarungen ausdrücklich zulässt.

(Anmerkung zum Verweis des § 5 TV IuK: Der Verweis muss inhaltlich die Nummer 11 betreffen, entsprechend § 39 Buchst. c MVG)

(Anmerkung zum Verweis des § 7 TV IuK: Der Verweis muss inhaltlich die Nummern 12 und 14 betreffen, entsprechend § 40 Buchst. g bis j MVG)

(3) Der Personalrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, ferner mitzubestimmen über

1. Bestellung und Abberufung von Vertrauens- und Betriebsärzten,
2. Bestellung und Abberufung von Beauftragten für den Datenschutz, Fachkräften für Arbeitssicherheit, Sicherheitsbeauftragten, Beauftragten für biologische Sicherheit und Fachkräften sowie Beauftragten für den Strahlenschutz,
3. Geltendmachung von Ersatzansprüchen gegen einen Beschäftigten,
4. Inhalt von Personalfragebogen mit Ausnahme von solchen im Rahmen der Rechnungsprüfung,
5. Beurteilungsrichtlinien,
6. Inhalt und Verwendung von Formulararbeitsverträgen,
7. Erlass von Richtlinien über die personelle Auswahl bei Einstellungen, Versetzungen, Umgruppierungen und Kündigungen,
8. Erlass von Richtlinien über Ausnahmen von der Ausschreibung von Dienstposten für Beamte und Aufstellung von allgemeinen Grundsätzen über die Durchführung von Stellenausschreibungen für Angestellte und Arbeiter einschließlich Inhalt, Ort und Dauer,
9. Durchführung der Berufsausbildung bei Angestellten und Arbeitern einschließlich der Bestellung und Abberufung der Ausbilder und Ausbildungsleiter bei Ausbildungen im Sinne des Berufsbildungsgesetzes, des Krankenpflegegesetzes und des Hebammengesetzes, mit Ausnahme der Gestaltung der Lehrveranstaltungen,
10. allgemeine Fragen zur Durchführung der Berufsausbildung der Beamten einschließlich der Bestellung und Abberufung der Ausbilder und Ausbildungsleiter,
11. allgemeine Fragen der beruflichen Fortbildung, Weiterbildung, Umschulung und Unterweisung in einer anderen Laufbahn,
12. Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten und die Leistung der Beschäftigten zu überwachen,
13. Gestaltung der Arbeitsplätze,
14. Einführung, Anwendung oder wesentliche Änderung oder wesentliche Erweiterung technischer Einrichtungen und Verfahren der automatisierten Verarbeitung personenbezogener Daten der Beschäftigten,
15. Personalangelegenheiten der Angestellten und Arbeiter bei
    a. Übertragung der auszuübenden Tätigkeiten bei der Einstellung,
    b. Zeit- oder Zweckbefristung des Arbeitsverhältnisses,
    c. Höher- oder Rückgruppierung,
    d. Änderung der vertraglich vereinbarten Arbeitszeit,
    e. Ablehnung eines Antrags auf Teilzeitbeschäftigung oder Urlaub ohne Fortzahlung des Arbeitsentgelts,
    f. Abordnung für die Dauer von mehr als zwei Monaten,
    g. Zuweisung entsprechend § 123 a des Beamtenrechtsrahmengesetzes für eine Dauer von mehr als zwei Monaten.
16. Erstellung und Anpassung des Frauenförderplans,
17. Bestellung der Frauenvertreterin, sofern die Bestellung nicht auf Grund einer Wahl der Beschäftigten erfolgt, und deren Abberufung.

(4) In den Fällen des Absatzes 3 Nr. 3 bestimmt der Personalrat nur mit, wenn der Beschäftigte dies beantragt. In den Fällen des Absatzes 3 Nr. 3 und 15 Buchst. f und g gilt § 75 Abs. 2 entsprechend.

Hinweise des Finanzministeriums Baden-Württemberg zum TV IuK

1 Durch den Tarifvertrag vom 25. Januar 1990 werden mit Wirkung ab 1. Mai 1990 die bisherigen Richtlinien des Finanzministeriums zur Regelung von Arbeitsbedingungen für Arbeitnehmer auf Bildschirmarbeitsplätzen abgelöst.

2 Im Zusammenhang mit dem Abschluß desTarifvertrages haben die Tarifvertragsparteien niederschriftlich folgende gemeinsamen Erklärungen abgegeben:

2.1 Die Tarifvertragsparteien gehen bei demTarifabschluß davon aus, daß beim Einsatz von Geräten der Informations- und Kommunikationstechnik Möglichkeiten genutzt werden sollen, die insbesondere geeignet sind,

- die Handlungs- und Entscheidungsspielräume der an den Geräten der Informations- und Kommunikationstechnik eingesetzten Beschäftigten zu erweitern,
- den Anteil an schematischen Arbeitsabläufen zu verringern,
- die Fähigkeiten der an den Geräten der Informations- und Kommunikationstechnik eingesetzten Beschäftigten weiter zu entwicklen und ihre Kenntnisse zu erweitern und zu vertiefen,
- die Zusammenarbeit zu verbessern,
- Möglichkeiten zu sozialen Kontakten zu erhalten.

2.2 Zwischen den Tarifvertragsparteien besteht Einvernehmen, dass auf Angestellte die aufgrund des § 3 q BAT vomGeltungsbereich des BAT und damit auch aus dem Geltungsbereich des vorliegend vereinbarten Tarifvertrags ausgenommen sind, die §§ 4 und 6 Abs. 3 und 4 sowie die §§ 7 und 8 anzuwenden sind, wenn die Teilzeitarbeit ganztägig abgeleistet wird und die Angestellten überwiegend am Bildschirmarbeitsplatz eingesetzt sind.

2.3 Zwischen den Tarifvertragsparteien besteht Einvernehmen, daß die nach dem jeweiligen Personalvertretungsgesetz oder dem Betriebsverfassungsgesetz zulässigen Dienst- oder Betriebsvereinbarungen durch das Inkrafttreten dieser Tarifverträge nicht berührt werden.

3. Zur Frage der Beteiligung des Personalrats im Zusammenhang mit der Einrichtung von Bildschirmarbeitsplätzen wird auf § 79 LPVG (s. Gl.Nr. 11) hingewiesen.

4. Zur Frage des Abschlusses von Dienstvereinbarungen bei Einführung neuer Techniken (IuK) wird auf das entsprechende Merkblatt des Innenministeriums hingewiesen.

Anlage 1: Rundschreiben des FM vom 10. November 1997 (1-03929-07/1)

Kosten der Beschaffung einer Sehhilfe und der augenärztlichen Untersuchung Die Verordnung zur Umsetzung von EG-Einzelrichtlinien zur EG-Rahmenrichtlinie Arbeitsschutz vom 4. Dezember 1996 (BGBl. I S. 1841) ist am 20. Dezember 1996 in Kraft getreten. Nach § 6 Abs.1der Verordnung hat der Arbeitgeber den Beschäftigten vor Aufnahme ihrer Tätigkeit an Bildschirmgeräten, anschließend in regelmäßigen Zeitabschnitten sowie bei Auftreten von Sehbeschwerden, die auf die Arbeit am Bildschirmgerät zurückgeführt werden können, eine angemessene Untersuchung der Augen und des Sehvermögens durch eine fachkundige Person zu bieten. Erweist sich aufgrund der Ergebnisse einer Untersuchung nach Satz 1 eine augenärztliche Untersuchung als erforderlich, ist diese zu ermöglichen. Den Beschäftigten sind nach § 6 Abs. 2 der Verordnung im erforderlichen Umfang spezielle Sehhilfen für ihre Arbeit an Bildschirmgeräten zur Verfügung zu stellen, wenn die Ergebnisse einer Untersuchung nach Abs. 1 ergeben, daß spezielle Sehhilfen notwendig und normale Sehhilfen nicht geeignet sind. Der Bundesausschuß der Ärzte und Krankenkassen hat sich mit den Konsequenzen in Bezug auf die Heilmittel- und Hilfsmittel-Richtlinien befaßt und am 20. Februar 1997 eine Änderung beschlossen. Sie wurde im Bundesanzeiger Nr. 66 vom 9. April 1997 (S. 4682) veröffentlicht und trat am 10. April 1997 in Kraft.

Die alte Fassung der Heilmittel- und Hilfsmittel-Richtlinien besagte folgendes (Abschn. 55.3.3):

"Die zusätzliche Verordnung einer Brille für dieTätigkeit an Bildschirmgeräten kann zu Lasten der gesetzlichen Krankenkassen vorgenommen werden, . . .".

Die neue Fassung der Heilmittel- und Hilfsmittel-Richtlinien lautet wie folgt (Abschn. 58.10):

"Nicht verordnungsfähig sind: Brillengläser für die Tätigkeit an Bildschirmarbeitsplätzen."

Mit dieser Änderung der Heilmittel-Richtlinien haben sich die Spitzenverbände der Krankenkassen zum Leistungsrecht am 25. Juni 1997 befaßt und folgendes Besprechungsergebnis erzielt:

"Die Spitzenverbände der Krankenkassen vertreten die Auffassung, daß eine Verordnung von Brillengläsern zu Lasten der gesetzlichen Krankenversicherung ausscheidet, wenn sie

- zusätzlich oder
- allein

für die Tätigkeit an Bildschirmarbeitsplätzen erforderlich werden. Des weiteren gehen die Kosten solcher augenärztlicher Untersuchungen nicht zu Lasten der gesetzlichen Krankenversicherung, die ausschließlich wegen einer - ggf. erforderlichen - Verordnung einer Sehhilfe für die Tätigkeit an Bildschirmarbeitsplätzen durchgeführt werden."

Die Kosten sind in diesen Fällen imRahmen der Protokollnotiz zu § 4 Abs. 4TVIuK vom Land als Arbeitgeber zu tragen. Diese sind ggf. bei Titel 546 49 - vermischte Verwaltungsausgaben - um jeweiligen Kapitel der Verwaltung zu buchen. Außerdem hat sich die Tarifgemeinschaft deutscher Länder mit der Angelegenheit befaßt, nachdem die Kosten für ein Brillengestell seit dem 1. Januar 1997 nicht mehr zu dem Sachleistungskatalog der gesetzlichen Krankenkassen gehören. Unter Berücksichtigung dieses Besprechungsergebnisses erhebt das Finanzministerium keine Einwendungen, wenn die Dienststellen und Betriebe des Landes in den Fällen des § 6 Abs. 2 der Bildschirmarbeitsverordnung für die Beschaffung des Brillengestells einen Betrag von 20 DM als notwendig im Sinne der Protokollnotiz zu § 4 Abs. 4 TVIuK anerkennen.

Das Rundschreiben vom 15. April 1991 wird aufgehoben.

Neue Beschwerdestelle über illegale Online-Inhalte

Surfer zeigen Zähne

Eine direkte Beschwerdemöglichkeit über illegale und schädigende Inhalte im Internet bietet seit kurzem der Verband der deutschen Internetwirtschaft eco an:
Unter **www.internet-beschwerdestelle.de** nimmt eco gemeinsam mit FSM, der "Freiwilligen Selbstkontrolle Multimediadiensteanbieter", Beschwerden über Inhalte im WWW, aber auch in E-Mails, Tauschbörsen, Chats oder Diskussionsgruppen entgegen. Bis zu 150 Beschwerden gehen alleine zu den Bereichen "Spam" und "Newsgroups" täglich ein, so Rechtsanwalt Frank Ackermann, der diese Themenfelder für eco bearbeitet.

Die Inhalte des folgenden Artikels sind der Seite **www.bsi-fuer-buerger.de** entliehen:

Beim Geräte-Entsorgen Daten löschen

Lesbarer Müll

Alte elektronische Geräte werden nach dem Willen der EU in Zukunft kostenlos entsorgt. Auch in Deutschland wird im Sommer 2005 ein System in Kraft treten, das die Hersteller zur Rücknahme verpflichtet. PCs, Monitore oder Laptops werden in Zukunft das Symbol einer durchgestrichenen Mülltonne tragen und als Elektronikmüll vom Handel zurückgenommen. Allerdings darf in diesem Zusammenhang der Sicherheitsaspekt nicht vernachlässigt werden.
Vor dem Aussondern alter Geräte sollten mit geeigneten Tools [**http://www.bsi-fuer-buerger.de/toolbox/tblinks.htm**] alle Informationen gelöscht werden. Auch bei elektronischen Medien mit sensiblen Inhalten wird oft zu wenig darauf geachtet, diese vor dem Wegwerfen zu vernichten. So sollten etwa Daten-CDs oder DVDs am besten zerbrochen werden, um das Lesen unmöglich zu machen. Mehr Informationen zum "richtigen Löschen" unter **http://www.bsi-fuer-buerger.de/daten/03_03.htm**.

Bundesnetzagentur nimmt Beschwerden entgegen

Meldung machen

Gute Nachrichten für alle Werbemüll-geplagten Internetnutzer: Wer mit elektronischem Werbemüll über Telefon, Fax, SMS oder E-Mail belästigt wird, kann sich an die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

http://www.bundesnetzagentur.de

wenden. Seit kurzem können Verbraucher die erhaltenen Faxe oder Werbemails mit einer kurzen Sachverhaltsdarstellung und der Bitte um Einschreiten der Bundesnetzagentur an die
Bundesnetzagentur Außenstelle Neustadt
Schütt 13
67433 Neustadt
Fax-Nummer 06321 / 934-111
oder die E-Mail-Adresse

Rufnummernspam@bnetza.de

schicken. Die Bundesnetzagentur schreitet allerdings nur dann ein, wenn es sich um die "gesicherte Kenntnis der rechtswidrigen Nutzung von Rufnummern" handelt. Der Betroffene dürfe zudem in keiner Geschäftsbeziehung zum Absender stehen und vorher auch keine Zustimmung erteilt haben, so die Bundesnetzagentur.

Newsletter des Bundesamt für Sicherheit in der Informationstechnik

„wie wichtig Sicherheitsmaßnahmen für das Überleben sind, erfuhren die Verantwortlichen der NASA bei der jüngsten Weltraummission der "Discovery", die kürzlich glücklich zu Ende ging. Lose Kacheln am Rumpf der "Columbia" hatten im Februar 2003 deren Sicherheitsschild unbrauchbar gemacht und zum Absturz des Shuttles geführt. Auch bei Computern und Mobiltelefonen sind es oft kleine Sicherheitslücken, durch die Angreifer Ihre Daten ausspähen oder Ihre Programme torpedieren können. "Phisher" sind noch immer sehr aktiv - und auch im Bereich der Mobiltelefonie erreichen uns immer häufiger Meldungen über Schädlinge. Bleiben Sie wachsam, damit Sie beim Wiedereintritt in die Online-Atmosphäre keine böse Überraschung erleben!“
mit diesem Text begrüßt das BSI im Internet.
Informationen zu aktuellen Sicherheitsrisiken im Internet und Tipps wie Sie sich schützen können, erhalten Sie im zweiwöchentlich erscheinenden Newsletter des BSI.
Bestellt werden kann dieser informative, nützliche und hilfreiche Newsletter unter:

http://www.bsi-fuer-buerger.de/newsletter/anmelden.htm

Die Inhalte des folgenden Artikels sind der Seite **www.bsi-fuer-buerger.de** entliehen:

„Aktive Inhalte“ beim Surfen

von: http://www.bsi-fuer-buerger.de/internet/index.htm

Wenn Sie die Grundeinstellung Ihres Browsers unverändert lassen, erlauben diese meist die Ausführung **nicht sichtbarer Funktionen**, welche in den besuchten Internetseiten verborgen sein können. Solche versteckten Programmteile oder Skripte werden als "Aktive Inhalte" bezeichnet. Die bekanntesten sind: Java-Applets, ActiveX-Controls, JavaScript und VBScript.

Da Sie nicht an der in Ihrem Browser angezeigten Seite erkennen können, welche Funktionen sich im einzelnen dahinter verbergen, haben Sie als Benutzer keinerlei Kontrolle darüber, wer auf Ihren Rechner zugreift und was die Aktiven Inhalte eigentlich alles auf Ihrem PC anstellen.

Auf diesem Weg können Spionageprogramme oder illegale Dialer über Aktive Inhalte auf Ihrem Rechnern installiert werden. Aber auch einmalige Aktionen können beim Besuch einer Webseite mit Aktiven Inhalten ausgeführt werden, die Ihre Daten im Zweifelsfall in Mitleidenschaft ziehen.

Deshalb empfiehlt das BSI Aktive Inhalte prinzipiell auszuschalten.

Im Kapitel Browser-Sicherheits-Check erfahren Sie, wie das genau funktioniert. Einziger Haken: Für Ihre Sicherheit büßen Sie einiges an Komfort ein. Denn viele Internetseiten sind so programmiert, dass sie nur dann richtig angezeigt werden, wenn Sie die Aktiven Inhalte zulassen. Die Entscheidung, was Ihnen wichtiger ist, liegt deshalb bei Ihnen.

Doch was verbirgt sich eigentlich technisch genau dahinter?

Java

Java ist eine universelle Programmiersprache, die sich auch für den Einsatz in Internetanwendungen eignet. Sie wurde von der Firma Sun Microsystems ursprünglich zur Steuerung von Haushaltsgeräten entwickelt, wurde aber schnell zu einer verbreiteten Programmiersprache für alle Arten von Anwendungen.

Aufgrund der Unabhängigkeit von der eingesetzten Hardware und vom eingesetzten Betriebssystem erfreute sich Java einer großen Beliebtheit und wurde von den Entwicklern auf immer neue Bedürfnisse angepasst. So bietet heute Java unter anderem die Möglichkeit, Webseiten mit Spezialeffekten (wie beispielsweise animierten Grafiken) auszustatten.

Diese spezielle Art von Java-Programmen werden Java-Applets genannt. Sie sind dadurch gekennzeichnet, dass sie in eine Webseite integriert werden können. Durch Aufruf der Seite werden sie auf Ihren PC heruntergeladen, wo sie dann ausgeführt werden. Damit die Browser die Java-Applets verarbeiten, wurden sie um die für die Ausführung von Java-Programmen benötigte "Java Virtual Machine" erweitert.

Hierdurch laufen die Java-Applets wie ein lokal – also auf Ihrem Rechner direkt – installiertes Programm ab. Der einzige Unterschied: Der Funktionsumfang der Applets ist gegenüber normalen Java-Programmen begrenzt und Java-Applets können nicht ohne Ihre Erlaubnis auf Ihre lokalen Daten zugreifen. Wenn ein betrügerisch veranlagter Seitenersteller sich Ihre Erlaubnis jedoch erschleicht oder in der Implementierung der Java Virtual Machine Fehler enthalten sind, kann trotz allem der **uneingeschränkte Zugriff** auf Ihren Rechner und Ihre Daten möglich werden. Aber auch **Programmierfehler** im Applet selbst können zu einem Ärgernis werden. Im harmlosesten Fall stürzt nur der Browser ab. Bei so genannten **Endlos-Schleifen** hilft meist nur der Neustart des Rechners, da Programme mit Endlos-Schleifen sich immer wieder selbst aufrufen, bis der Prozessor des Computers vollkommen ausgelastet ist.

ActiveX-Controls

ActiveX ist von Microsoft als Konkurrenz zu Java entwickelt worden, wobei die Funktionen eng auf die Windows-Betriebssysteme zugeschnitten worden sind. Auch in den Internet Explorer wurde die Möglichkeit integriert, ActiveX-Elemente zu verarbeiten. Die ActiveX-Elemente, die als Aktiver Inhalt in Webseiten eingefügt werden können, werden ActiveX-Controls genannt. Der Funktionsumfang der ActiveX-Controls ist eben so groß wie das Risiko, das für den Anwender durch die Freischaltung dieser Controls entstehen kann.

Man kann z. B. Videos, Musik und alle erdenklichen Windowsgrafiken und -funktionen in Webseiten einbauen. Es werden aber auch häufig Schadprogramme und Dialer auf diesem Weg verbreitet Dies ist so einfach möglich, da es keine **richtigen Sicherheitsrichtlinien** gibt. Es gibt zwar signierte ActiveX-Controls, die versprechen aber nur einen Hauch von Sicherheit. Denn die Signatur bestätigt letztlich nur, von wem das ActiveX-Control stammt. Ob das Control schädigenden Code beinhaltet oder nicht, steht dabei jedoch in den Sternen. Läuft das ActiveX-Programm erst einmal, dann ist sein Funktionsumfang in keiner Weise eingeschränkt oder kontrollierbar.

Fazit: Das ActiveX-Programm läuft mit allen Rechten des angemeldeten Benutzers – ohne jede Einschränkung! Es ist demnach ein leichtes, private oder sicherheitsrelevante Daten auszulesen, zu löschen, zu manipulieren, den Rechner umzukonfigurieren, einen Virus oder ein Trojanisches Pferd zu installieren

JavaScript und JScript

JavaScript ist eine an Java angelehnte Skriptsprache. Skriptsprache heißt dabei, dass es sich um eine Programmiersprache handelt, die beim Anwender im Textformat vorliegt und durch ein eigens dafür vorgesehenes "Übersetzungsprogramm" (Interpreter) ausgeführt wird. JavaScript wurde speziell für den Einsatz als Aktiver Inhalt in Webseiten von der Firma Netscape entwickelt. JavaScript eignet sich beispielsweise zur Überprüfung von Formulareingaben innerhalb von Webseiten.

Wie die Java-Applets kommen auch die in JavaScript geschriebenen Aktiven Inhalte mehr oder weniger ungefragt auf Ihren Rechner. An der angezeigten Webseite ist nicht erkennbar, was sich so alles dahinter verbirgt. Hierdurch entsteht für den Anwender ein unüberschaubares Risiko. Schließlich sind auch bei JavaScript Fehler in der Implementierung nicht ausgeschlossen. Doch die Gefahr bei dem Einsatz von JavaScript ist noch größer als bei dem von Java-Applets.

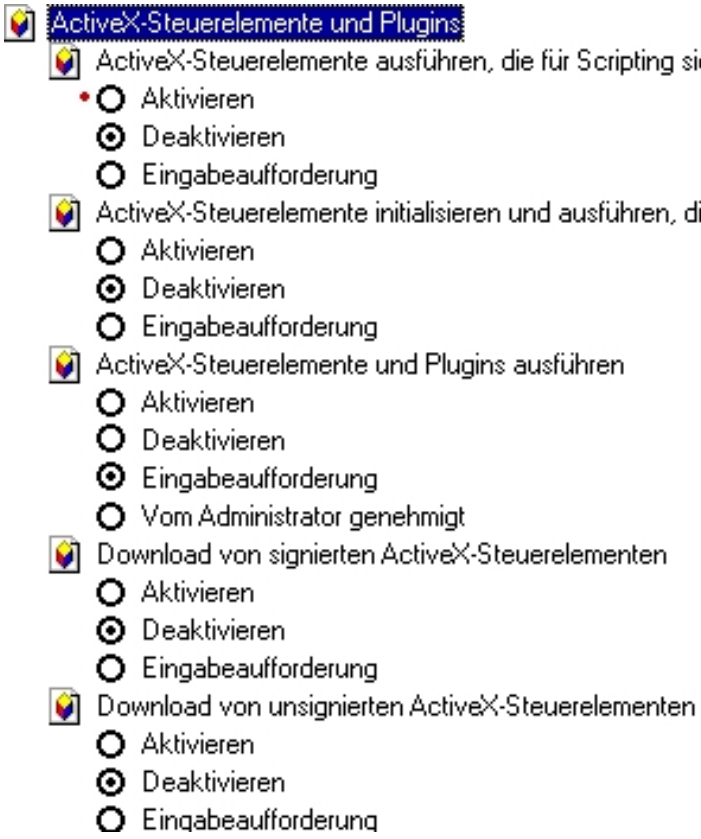
In der JScript genannten Variante von JavaScript, die Microsoft für den Internet Explorer entwickelt hat, gibt es Funktionen, die missbräuchlich eingesetzt einen großen Schaden auf dem Rechner des Anwenders verursachen können. So gibt es unter JScript beispielsweise die Möglichkeit, ActiveX-Controls anzusprechen, die einmal auf den Rechner geladen die gleichen Rechte wie ein lokal installiertes Programm besitzen.

VBScript

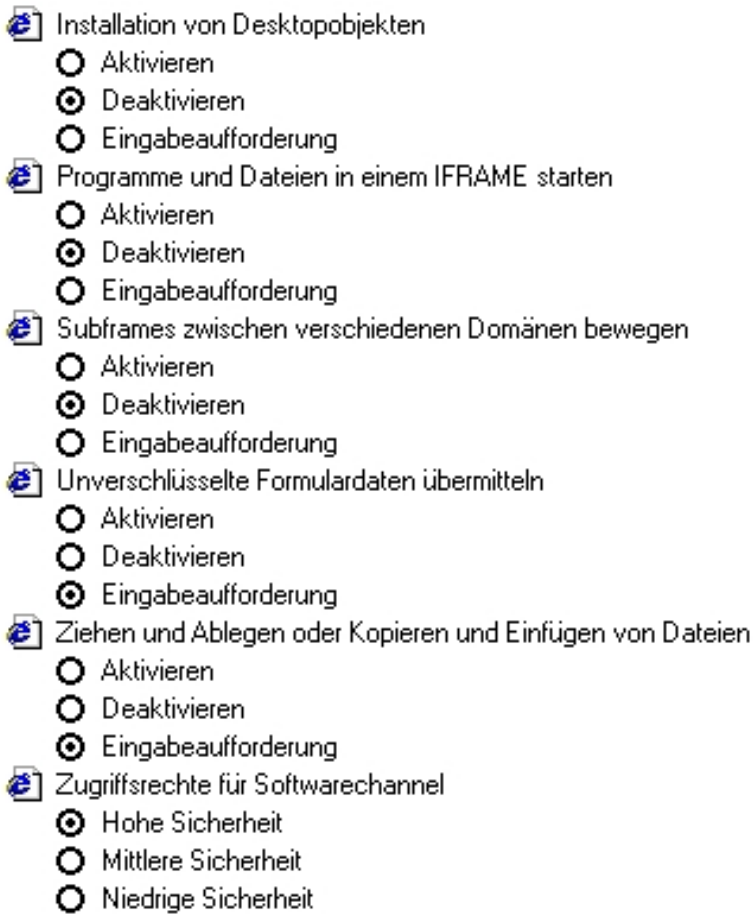
VBScript ist ebenfalls eine von Microsoft entwickelte Skriptsprache, die an die Programmiersprache Visual Basic angelehnt und wie diese eng an die Windows-Betriebssysteme gekoppelt ist. Auch mit VBScript können Webseiten um aktive Elemente erweitert werden. Allerdings ist der Internet Explorer der einzige Browser, der ohne zusätzliche Erweiterung VBScript in Webseiten ausführen kann.

Der Funktionsumfang von VBScript ist mit dem von JavaScript und JScript vergleichbar. Da VBScript eng mit dem Betriebssystem zusammenarbeitet, kommen noch Funktionen zur Bearbeitung von Daten und der Systemregistrierung (Registry) hinzu. Zusätzlich gibt es auch hier die Möglichkeit, ActiveX-Controls aufzurufen, die einmal auf den Rechner geladen die gleichen Rechte wie ein lokal installiertes Programm besitzen. Alle diese Funktionen stellen ein hohes Sicherheitsrisiko dar. Und dieses Risiko ist nicht gerade klein, da die Funktionen unbemerkt vom Anwender durchgeführt werden.

vom BSI empfohlene Sicherheitseinstellungen des Internet Explorer



- Benutzerauthentifizierung
  - Anmeldung
    - ○ Anonyme Anmeldung
    - ○ Automatische Anmeldung mit aktuellem Benutzernamen un
    - ○ Automatisches Anmelden nur in der Intranetzone
    - ◉ Nach Benutzername und Kennwort fragen
- Cookies
  - Cookies annehmen, die gespeichert sind
    - ○ Aktivieren
    - ◉ Deaktivieren
    - ○ Eingabeaufforderung
  - Cookies pro Sitzung annehmen (nicht gespeichert)
    - ○ Aktivieren
    - ○ Deaktivieren
    - ◉ Eingabeaufforderung
- Download
  - Dateidownload
    - ◉ Aktivieren
    - ○ Deaktivieren
  - Schriftartdownload
    - ◉ Aktivieren
    - ○ Deaktivieren
    - ○ Eingabeaufforderung
- Java
  - Java-Einstellungen
    - ○ Benutzerdefiniert
    - ◉ Hohe Sicherheit
    - ○ Java deaktivieren
    - ○ Mittlere Sicherheit
    - ○ Niedrige Sicherheit
- Scripting
  - Active Scripting
    - ○ Aktivieren
    - ◉ Deaktivieren
    - ○ Eingabeaufforderung
  - Einfügeoperationen über ein Skript zulassen
    - ○ Aktivieren
    - ◉ Deaktivieren
    - ○ Eingabeaufforderung
  - Scripting von Java-Applets
    - ○ Aktivieren
    - ◉ Deaktivieren
    - ○ Eingabeaufforderung
- Verschiedenes
  - Auf Datenquellen über Domänengrenzen hinweg zugreifen
    - ○ Aktivieren
    - ◉ Deaktivieren
    - ○ Eingabeaufforderung
  - Dauerhaftigkeit der Benutzerdaten
    - ○ Aktivieren
    - ◉ Deaktivieren



Die Inhalte des folgenden Artikels sind der Seite **www.bsi-fuer-buerger.de** entliehen:

Sicherheitsrisiko "Surf-Turbos"

In den letzten Monaten mehren sich die Angebote verschiedener Anbieter, die durch die Installation einer speziellen Zusatzsoftware auf dem PC des Kunden ein schnelleres Surfen im Internet versprechen. In der Regel handelt es sich dabei um unseriöse Marktforschungsunternehmen, die diese Software nach einer Registrierung kostenlos zum Download zur Verfügung stellen. Durch die Installation der Software wird der Datenverkehr beim Surfen im Internet über Proxy-Server des Anbieters geleitet - die Geschwindigkeitssteigerung soll dabei durch Komprimierung der Daten bei der Übertragung zwischen Anbieter und Kunde erzielt werden.

Die meisten Anwender sind sich bei der Nutzung eines solchen Angebots nicht bewusst, dass der Anbieter den gesamten Datenverkehr mitlesen, analysieren und mit den vom Anwender bei der Registrierung angegebenen persönlichen Daten verknüpfen kann. Eine besondere Bedrohung besteht darin, dass auch sensible Informationen - z. B. beim Internet-Banking übermittelte Daten wie Kontostand oder PINs und TANs - mitgelesen werden koennen. Auch vermeintlich durch eine SSL-Verbindung geschützte Daten sind bei der Nutzung von "Surf-Turbos" einiger Anbieter nicht vor unbefugtem Mitlesen sicher, da die verschlüsselte Verbindung auf dem Proxy-Server des Anbieters aufgebrochen wird. Es besteht dann keine direkte verschlüsselte Verbindung zwischen dem Browser des Anwenders und dem Server der besuchten Webseite, sondern der Datenstrom wird auf dem Proxy-Server entschlüsselt und anschliessend erneut verschlüsselt. Dies geschieht für den Anwender unbemerkt, da bei der Installation der Software ein zusätzliches Zertifikat des Anbieters installiert und automatisch in die Liste der vertrauenswürdigen Zertifikate aufgenommen wird. Der Internet-Browser zeigt dadurch keine Warnmeldung, dass die verschlüsselte Verbindung nicht zwischen dem PC des Anwenders und dem Server der besuchten Webseite (zum Beispiel einer Online-Bank), sondern lediglich bis zum Proxy-Server des Anbieters besteht.

Das BSI rät von der Nutzung von "Surf-Turbos" ab, wenn beim Surfen sensible Informationen wie Passwörter, PINs, TANs, vertrauliche oder personenbezogene Daten übermittelt werden.

Die Inhalte des folgenden Artikels sind der Seite **www.bsi-fuer-buerger.de** entliehen:

„Phishing“ oder „Passwort-Fischer

Sie können sich unter `http://www.bsi-fuer-buerger.de/abzocker/index.htm` zum Thema "Passwort-Fischer" oder auch neudeutsch "Phishing" genannt informieren.

In einigen Ländern haben sich viele Firmen bereits zur Anti-Phishing Working Group zusammengetan. Auf deren Internetseite (www.antiphishing.org) kann man Phishing-Mails melden und nachlesen welche schon bekannt sind.
In Deutschland hat sich eine neue interdisziplinäre Vereinigung aus Wissenschaftlern der Ruhr-Universität Bochum des Phishing-Problems angenommen. Die "Arbeitsgruppe Identitätsmissbrauch im Internet" (A-I3) stellt auf ihrem Online-Portal http://www.a-i3.org nicht nur aktuelle Informationen zu Themen der IT-Sicherheit bereit, sondern auch konkrete Hilfestellungen und Tools.

Allgemeine Schutzmaßnahmen

Die nachfolgenden Punkte werden auch als die "**10 Gebote zum Schutz vor Phishing**" bezeichnet. Um einen effektiven Schutz einzuhalten, muss rigoros die Reihenfolge der Regeln beachtet werden. Wichtig: Regel 1-4 müssen eingehalten werden, die restlichen Regeln können umgesetzt werden.

1. Pflegen Sie die Browser-Software regelmäßig mit aktuellen Sicherheits-Updates.
In den vergangenen Monaten haben Hersteller gängiger Browser maßgeblich ihre Produkte gegen Phishing-Angriffe resistenter gestaltet, und die browserspezifischen Funktionen, welche von Phishern gerne genutzt werden, eingeschränkt. Ein notwendiges Muss sind das Service Pack 2 (oder vergleichbare Updates anderer Browser), welches u.a. das deaktivieren des Statuszeile verbietet, und den Benutzer vertrauenswürdig über den Einsatz von SSL (Schlosssymbol in der Statuszeile) informiert. Der Gebrauch von SSL sollte immer vorausgetzt werden, wenn persönliche Informationen über das Internet übermittelt werden sollen, weil sie unter Umstände unverschlüsselt verschickt und als Folge manipuliert werden könnten.

2. Überprüfen sie das Aussteller-Zertifikat
Ein Doppelklick auf das Schlosssymbol in der Statuszeile öffnet ein neues Fenster, das Informationen über den Aussteller der Webseite anzeigt (ähnlich einem Personalausweis). Um sicherzustellen, dass sie auch tatsächlich auf der richtigen Seite ihre privaten Informationen übermitteln, müssen sie prüfen, ob

- der angezeigte Domain Name des Ausstellers auch der ihnen bekannte ist und auch mit dem Namen in der Adresszeile übereinstimmt,
- das Zertifikat von einer vertrauenswürdigen Partei (Certificate Authority) ausgestellt wurde (wenn dem Browser das Zertifikat unvertraut ist, erscheint eine Fehlermeldung).
- das Zertifikat gültig ist.

Ist einer der Punkte nicht erfüllt, sollten sie davon absehen, persönliche Informationen an die Seite weiterzugeben, sie könnte gefälscht sein.

Bemerkung: Die Regel kann nur wirkunsvoll eingesetzt werden, wenn Regel 1 erfüllt ist!

3. Überprüfen Sie, ob die Website gesichert ist, bevor kritische Daten eingegeben werden: Die URL sollte mit "https://" und nicht nur mit "http://" starten.
Bemerkung: Beachten sie, dass Phisher die Adresszeile fälschen könnten, so dass sie unter Umständen eine gefälschte URL sehen könnten. Einen stärkeren Schutz erhalten sie durch Regel 2.

4. Gehen Sie niemals über einen angebotenen Link zu der gewünschten Website, geben Sie stattdessen immer die entsprechende URL in den Browser ein.
Bemerkung: Diese Regel hiflt nicht gegen Pharming. Nutzen sie Regel 1-3 um Pharming-Angriffe aufzudecken.

5. Deaktivieren Sie Javascript im Browser, um Cross-Site-Scripting zu vermeiden, und den Windows Skripting Hosts (WSH), um die Ausführung von ungewollten Skripten zu unterdrücken.
Bemerkung: Es ist nicht nachgewiesen, dass es Phishing-Angriffe gibt, die ohne den Einsatz von Javascript auskommen. Fakt ist, dass sie den Spielraum der möglichen Täuschungsangriffe eingrenzen. Nachteilig ist, dass moderne Webseiten selten ohne den Gebrauch von Javascirpt dargestellt werden können.

6. Öffnen Sie möglichst keine Mails von unbekannten Absendern und wenn doch, klicken Sie auf keinen darin enthaltenen Link und bestätigen Sie niemals Kontonummern, Passwörter oder andere geheime Daten nach einer Mail-Aufforderung – entsprechende Institute oder Firmen würden ein solches Vorgehen aus Sicherheitsgründen nie wählen.

7. Verifizieren Sie auffällige Mails von vertrauten Adressaten (wie zum Beispiel der eigenen Bank) mit einem kurzen Anruf.

8. Schließen Sie den Browser, falls die gewünschte Website in der Regel eine Authentifizierung verlangt und plötzlich ohne eine solche auszukommen scheint.

9. Installieren Sie Webfilter, die ihren Sperrkatalog ständig um gefälschte Web-Seiten erweitern.
10. Setzen Sie aktuelle Anti-Virenprogramme und Firewalls ein. Verwenden Sie die neusten Signaturen.
Bemerkung: Der Schritt sollte selbstverständlich sein, wenn sie das Internet zur Weitergabe persönlicher Daten nutzen.

Die Inhalte des folgenden Artikels sind der Seite **www.bsi-fuer-buerger.de** entliehen:

Personalsierung beim IE6

Eine Personalisierung des User Interfaces hilft, Visual Spoofing Angriffe aufzudecken.

Weil ein Angreifer keine Veränderungen an der Oberfläche des Web Browsers ermitteln kann, sind personalisierte Web Browser ein vielversprechendes Mittel, um sich vor Täuschungsangriffen zu schützen.

Der Angreifer setzt eine Standardoberfläche des Browsers voraus. Er verfügt nicht über die technischen Möglichkeiten persönliche Einstellungen auszulesen. Das erste Konzept gründet auf der Idee, das Browser Interface zu individualisieren. In erste Linie müssen die ***Browser Spezifischen Sicherheitsindikatoren*** authentifiziert werden. Dies wird durch die Auswahl eines frei wählbaren Hintergrundbildes (Menü- und Adressleiste) und -textes (Titel- und Statusleiste) erreicht. Der Kerngedanke des Konzepts ist, dass das Bild persönlich ist, so dass es stets im Interesse des Benutzers steht. Im Gegensatz zu einem vorgegebenen Motiv des Web-Browser Herstellers oder der Firma kann der Benutzer mit dem persönlichen Bild sich identifizieren. Für die Wahl des Statustextes gilt eine analoge Argumentation. Fehlen beim Betreten einer (neuen) Web-Seite die in Abbildung 1 eingekreisten persönlichen Veränderungen, so wie sie in Abbildung 2 fehlen, dann ist dies eindeutig ein Indiz, das auf einen Visual Spoofing Angriff deutet. Folglich muss der Benutzer sich auf einer gefälschten Seite befinden.

Abbildung 1

Diese Konzept wurde prototypisch für den **Internet Explorer 6** als Browser Helper Object implementiert. Es ist aber auch kompatibel zu der Version 5 und 5.5 des Internet Explorers.

Download:
http://www.nds.rub.de/forschung/gebiete/UI/VS/Download/Visual%20Spoofing%20Toolbar.exe

Kurzanleitung:
http://www.nds.rub.de/forschung/gebiete/UI/VS/Download/Dokumentation.pdf

Abbildung 2

Wer mit mozilla firefox arbeitet, kann über folgenden Link http://trustbar.mozdev.org/installation.html einen Schutz gegen Phishing downloaden

Die Inhalte des folgenden Artikels sind der Seite **www.bsi-fuer-buerger.de** entliehen:

Sorglosigkeit im Umgang mit Passwörtern

Echte Hürde?

Passwörter können ihre Funktion nur erfüllen, wenn sie geheim gehalten werden. Die Hälfte der Computernutzer in Unternehmen schreiben dennoch Passwörter auf - das ergab die Studie eines Sicherheitsunternehmens. Bei der großen Masse von Zugangsdaten, die sich ein Computernutzer heute merken muss, ist dies auch nicht verwunderlich. 47 Prozent der Befragten müssen schließlich zwischen fünf und zehn Passwörter im Kopf behalten - und das allein für die Unternehmensanwendungen. Über ein Drittel der 2700 Studienteilnehmer aus den USA, Deutschland, Frankreich und Großbritannien tauschen darüber hinaus die Passwörter auch untereinander aus. Hinweise zum sicheren Umgang mit Passwörtern finden Sie auf den Webseiten von BSI-FUER-BUERGER [**http://www.bsi-fuer-buerger.de/schuetzen/07_02.htm**].

Gesundheitsrisiken durch vermehrte Notebook-Nutzung

Notebooks werden bei allen Gruppen von Computeranwendern immer beliebter. Günstigere Preise bei steigenden Leistungswerten ließen die Nachfrage nach den mobilen Rechnern stetig steigen und mittlerweile haben die Notebooks die klassischen stationären PCs bei den Absatzzahlen überholt. Doch es gibt auch kritische Stimmen zur zunehmenden Nutzung von Notebooks. Insbesondere Ergonomie-Spezialisten warnen vor möglichen Gesundheits-gefahren.

Über die ergonomischen Aspekte bei der Nutzung von Notebooks (Laptops) gibt es bislang nur wenige Untersuchungen und Studien. Dies ist vor allem darauf zurückzuführen, dass die mobilen Rechner nur von den wenigsten Anwendern ununterbrochen über längere Zeiträume genutzt wurden. Üblicherweise beschränkte sich die Arbeit am Notebook auf einige Minuten am Stück, und auch die eifrigsten Außendienstler arbeiteten kaum mehr als zwei bis drei Stunden pro Tag ohne Unterbrechung am mobilen Rechner.

Doch mittlerweile ändert sich das Einsatzgebiet für die Notebooks. So verzichten schon viele Firmen auf die obligatorische Ausstattung bestimmter Arbeitsplätze mit einem Desktop-Rechner und stellen den Arbeitnehmern ausschließlich einen tragbaren Rechner zur Verfügung. Wird ein Notebook jedoch als **Ersatz für den stationären PC** und damit täglich über längere Zeiträume genutzt, zeigen sich schnell die Schwächen dieses Gerätekonzepts, das vor allem in ergonomischer Hinsicht einiges zu wünschen lässt.

Insbesondere die fehlende Trennungsmöglichkeit von Tastatur und Bildschirm macht eine ergonomische Gestaltung des Bildschirmarbeitsplatzes ohne die Nutzung zusätzlicher Geräte unmöglich. Ein einfaches Notebook genügt damit nicht den **Anforderungen der Bildschirmarbeitsplatzverordnung von 1996**, die sowohl einen leicht drehbaren und neigbaren Bildschirm als auch eine vom Bildschirm trennbare und neigbare Tastatur vorschreibt. Will man diesen Vorgaben entsprechen, müssen also sowohl ein externer Monitor als auch eine externe Tastatur sowie Maus am Notebook angeschlossen werden. Zur einfachen Anbindung dieser Geräte empfiehlt sich eine **Dockingstation**, mit der sich der Verkabelungsaufwand erheblich reduzieren lässt.

Ohne derartige Maßnahmen drohen Nutzern von Notebooks bei permanenter, längerer Arbeit mit dem mobilen Rechner **gesundheitliche Probleme** etwa im Bereich der Handgelenke oder der Halswirbel bzw. im Nackenbereich. Auf die zunehmende Gefährdung der Gesundheit von Notebook-Anwendern wies jetzt der Ergonomie-Experte Alan Hodges, Leiter des renommierten **Ergonomie-Labors** an der amerikanischen Cornell Universität, hin (**http://ergo.human.cornell.edu/**).

Dabei verwies er auf die steigende Zahl der Krankmeldungen von Arbeitnehmern an Bildschirm-arbeitsplätzen hin. Zwar gebe es noch keine detaillierten Zahlen zu den Notebook-Nutzern in dieser Gruppe, generell sei jedoch ein stetig steigender Anteil dieser Benutzergruppe zu verzeichnen.

Praxis-Tipp:

Wenn das Notebook auch als Desktop-Ersatz genutzt werden soll, empfiehlt sich in jedem Fall die Nutzung von externen Peripheriegeräten, die am einfachsten über eine Docking-Station angeschlossen werden können. Soll kein zusätzliches Display genutzt werden, kann durch einen höhenverstellbaren Notebook-Ständer eine ergonomische Positionierung des Notebook-Bildschirms erreicht werden. Ähnliche Lösungen sind auch auf der Website **http://www.ergoindemand.com/laptop-workstation-ergonomics.htm** zu finden. Als ergonomisch wird eine Positionierung angesehen, bei der die oberste Zeile des Bildschirms knapp unterhalb der Augenhöhe liegt und die Tastatur sich ungefähr auf Höhe der Ellenbogen befindet. Weitere Angaben zur Gestaltung eines ergonomischen Bildschirmarbeitsplatzes finden Sie auf der Website der **Bundesanstalt für Arbeitsschutz und Arbeitssicherheit** (**http://www.baua.de/prax/buero/bildtast.htm**).

Kostenlose Alternativen: F R E E W A R E

Man muss nicht unbedingt auf Unix/Linux umsteigen, um vom Microsoft- und anderen Kartellen loszukommen: Für viele, recht teuere Microsoft- und andere Programme gibt es kostenlose Alternativen: **FREEWARE**
Zugegebenermaßen sind einige Programme vom Umfang eingeschränkt und evtl. etwas „gewöhnungsbedürftig", sie erfüllen aber auf alle Fälle die durchschnittlichen Erwartungen an ein Programm und ...
... entsprechen einer meiner tiefen Überzeugungen:

Entwickle ich etwas, formuliere ich etwas, stelle ich zu einem Thema ein Dossier zusammen

- während meiner Arbeitszeit, so wurde ich dafür von meinem Arbeitgeber entlohnt.
- während meiner Freizeit, so war es mein freier Wille und hat mir Freude und Spaß gemacht (sonst hätte ich es nicht gemacht).

Warum also soll ich dafür von meinen Mitmenschen für die Nutzung und den Gebrauch noch zusätzlich Geld verlangen?

Wolfgang Lenssen (Geschäftsführer)

openoffice: Die Alternative zum OFFICE (mit PowerPoint, Excell, Word)
http://de.openoffice.org/

irvanview
ist einer der wenigen deutschsprachigen Freeware-Bildbetrachter. Dank der flotten Miniatur-Vorschau beim Öffnen einer Datei blättern Sie durch Ihre Grafik-Verzeichnisse und haben alle Bilder im Überblick. Das kostenlose Programm Irfanview leistet auch gute Dienste bei der Fotobearbeitung und stellt die wichtigsten Funktionen wie „Größe verändern", „Ausschnitt bestimmen" und sogar einige Effekte zur Verfügung.
http://www.irfanview.de/

active slide
ist eine Präsentationssoftware, mit der Sie interaktive, animierte Präsentationen erstellen. Bei der Standard Edition handelt es sich um eine kostenlose, voll funktionsfähige Version, die zeitlich unbegrenzt genutzt werden kann.
http://www.activeslide.com/de/download.php (17,9 MB)
(Leider lief die install.exe bei mir nach dem Download nicht - das Öffnen der Datei und die Installation online hat funktioniert.

hot potatoes
Ein Programm für den Unterricht, die Gruppenarbeit etc. mit den Möglichkeiten, Lückentexte, Kreuzworträtsel, Multible Choice usw. zu erstellen.
http://web.uvic.ca/hrd/halfbaked/index.htm#downloads
danach muss man sich registrieren lassen, sonst steht nur eine eingeschränkte Programmversion zur Verfügung

notepad
Ein einfach zu bedienendes Programm zum Notenschreiben. Der besondere Gag bei diesem Programm ist die Möglichkeit, sich die Melodie anschließend vorspielen zu lassen.
http://www.klemm-music.de/coda/

firefox
neben Opera der alternative Browser für das Internet:
http://www.firefox-browser.de/

Software für Mp3- Player: Freerip MP3
wandelt die Songs ihrer Musik-CD´s in Mp3-files um:
http://www.mgshareware.com/frmmain.shtml
Dasselbe leistet **Powerlame** (deutsch):
http://www.powerlame.de

PGP Mail für nicht-kommerzielle Nutzung
Der PGP Corporation (www.pgp.com) stellt ab sofort die deutsche Version von PGP Freeware 9.0 für Windows zur Verfügung.
http://www.pgp.com/products/de/freeware.html

Linux Knoppix Version 4.0.1
http://www.knopper.net/knoppix/

Quellen

Einige Artikel sind aus dem kostenlosen Newsletter des Bundesamtes für Sicherheit in der Informationstechnik, **www.bsi.bund.de**. Sie wollen den Newsletter abonnieren? Dafür senden Sie bitte eine E-Mail an **newsletter_anmelden@bsi-fuer-buerger.de**

Portal Telearbeit:
http://www.aus-innovativ.de/themen/6844.htm

Die Inhalte des folgenden Artikels sind der Seite **www.bsi-fuer-buerger.de** entliehen:

Kinderschutz

Kinder gehören zu den aktivsten Nutzern der neuen Technologien.

Der Umgang mit dem Medium Internet ist für viele von ihnen bereits selbstverständlich. Mit einem PC und Internetzugang können Kinder mit Freunden chatten, neue Leute kennen lernen, Spiele spielen. Sie können Filmausschnitte gucken, Musik hören, Videospiele ausprobieren oder herunterladen, Fremdsprachen erlernen und neue Interessen entwickeln. Kurz gesagt: **Das Internet bietet Kindern ungeahnte Möglichkeiten und es gibt keinen Zweifel daran, dass die meisten davon sinnvoll sin**d. Bevor Sie Ihr Kind jedoch auf die Datenautobahn schicken, sollten Sie ihm sozusagen einen "Sicherheitsgurt" anlegen. **Welche Gefahren gibt es?** Zahlreiche Internetseiten sind für jüngere Menschen nicht geeignet. Besonders Seiten über Sex, Rassismus und Gewalt stellen eine Bedrohung dar. Weil das Internet jedoch global und dezentralisiert ist, können die Inhalte nur schwer kontrolliert werden. Zusätzlich versucht täglich eine große Anzahl Pädophiler über das Internet Kontakt zu Kindern und Jugendlichen aufzubauen. So genannte Selbstmordforen, die Möglichkeit über das Internet an Drogen zu gelangen oder durch Unachtsamkeit beim Internetsurfen einen 0190-Dialer auf dem PC zu installieren, sind nur drei von vielen weiteren Gefahren, die Ihrem Kind im Internet begegnen können. Darüber hinaus ist das Internet ein persönlich ansprechendes Medium, das Experten zufolge Kinder in einen "Schwebezustand" versetzen kann, der sie für Werbung sehr empfänglich macht. Es sind subtilere Marketingmethoden möglich, die Kinder zum Kaufen animieren können. Von den 100 am häufigsten aufgerufenen Seiten für Kinder und Jugendliche sind nur rund zehn Prozent nicht kommerzieller Natur. Um Ihr Kind vor diesen Gefahren zu schützen, können Sie den **Internetzugang Ihres Kindes entweder unterbinden, filtern** beziehungsweise zensieren, **oder Sie protokollieren alles**, was sich Ihr Kind im Internet ansieht.

Weitere Ausführungen zu diesen Maßnahmen finden sich auf den Seiten http://www.bsi-fuer-buerger.de

Checkliste als Grundlage für ein Gespräch zwischen Eltern / Betreuungspersonen und Kindern

- Glaube nicht einfach, was du im Internet liest!
- Sprich mit deinen Eltern drüber, wenn dir etwas komisch vorkommt!
- Gib niemals jemandem über das Internet deinen Namen, deine Adresse, deine Telefonnummer bekannt!
  Wenn du meinst, dass es wirklich einmal sein muss, dann besprich das vorher mit deinen Eltern oder anderen Vertrauenspersonen.
- Pass auf, wenn du über das Internet Dateien herunterlädst!
  Oft kommen dabei auch gleich bösartige Programme wie Viren oder Würmer mit, die auf deinem Computer Schaden anrichten können! Frage vor dem Herunterladen deine Eltern oder andere Erwachsene, ob dein Computer davor geschützt ist! Manchmal entstehen beim Herunterladen auch hohe Kosten – auch daran muss man denken!
- Sei vorsichtig beim Herunterladen von Klingeltönen oder anderen Programmen für dein Handy!
  Dabei kannst du sehr schnell auch schädliche Software auf dein Telefon laden - und es kann auch sehr teuer werden! Lies dir daher vorher gemeinsam mit deinen Eltern oder anderen Vertrauenspersonen die Betriebsanleitung oder die Internetseiten der Herstellerfirmen durch. Dort bekommst du Informationen darüber, ob dein Handy vor Viren und Würmern geschützt ist!
- Öffne keine Dateien in E-Mails oder Internet Messenger- Nachrichten, wenn du nicht weißt, wer sie geschickt hat!
  Du kannst dadurch nämlich leicht Viren, Würmer und andere bösartige Programme auf deinen Computer laden.
- Pass auf beim Herunterladen von Musik und Filmen aus dem Internet!
  Im Internet gibt es dafür viele kostenlose Angebote. Oft haben die Anbieter gar nicht das Recht dazu, sie auf ihre Webseite zu stellen. Und deshalb kannst dich auch du strafbar machen, wenn du sie herunterlädst! Sprich also vorher lieber mit deinen Eltern oder anderen Vertrauenspersonen.
- Sprich mit deinen Eltern oder anderen Vertrauenspersonen, bevor du dich mit Internetbekanntschaften triffst.
  In Chatrooms kann man schnell Leute kennen lernen. Und manchmal wollen die sich auch wirklich mit dir treffen. Bevor du aber ein solches Treffen ausmachst, sprich mit deinen Eltern oder anderen Personen, denen du vertraust darüber. Denn leider versuchen auch Menschen mit bösen Absichten, auf diese Weise mit dir in Kontakt zu kommen.

Literaturtipps

Die empfehlenswerte Broschüre **"Ein Netz für Kinder - Surfen ohne Risiko?"** des Bundesministeriums für Familie, Senioren, Frauen und Jugend ist im Jahr 2005 aktualisiert und überarbeitet worden.
www.jugendschutz.net/materialien/netz_fuer_kinder.html

"Klicks-Momente – So unterstützen Sie Ihr Kind in der Medienkompetenz" ist eine Broschüre der Polizei. Sie kann kostenfrei aus dem Internet geladen werden:
www.polizei-beratung.de/mediathek/kommunikationsmittel/index/content_socket/medien/display/8

Wichtige Tipps für Kinder und Jugendliche rund um das Thema Chatten.
www.dlz-kids.de/tipps.html