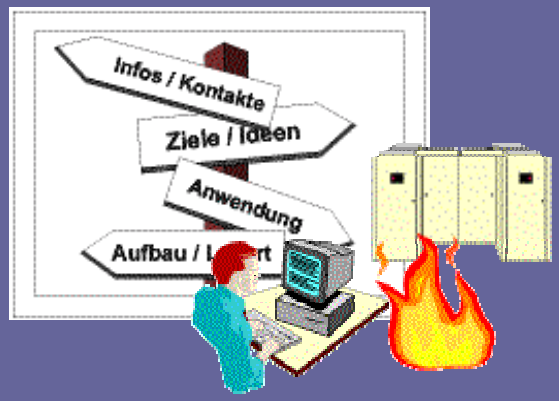
IT - Sicherheit

Ein Vortrag der dk-Computerschule



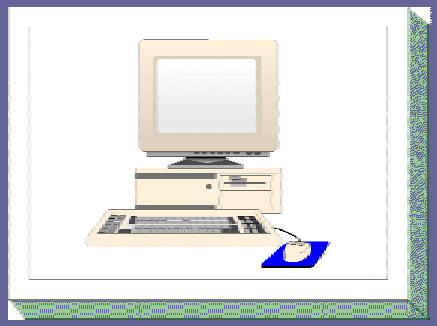
dk-Computerschule
Dillmann & Kriebs GbR

Bahnhofstr. 67
35390 Gießen

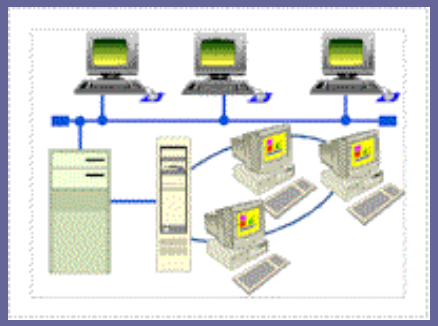
Tel.: 0641 / 971 921 0
Fax: 0641 / 971 921 1

Web: www.dk-services.de
e-Mail: mail@dk-services.de

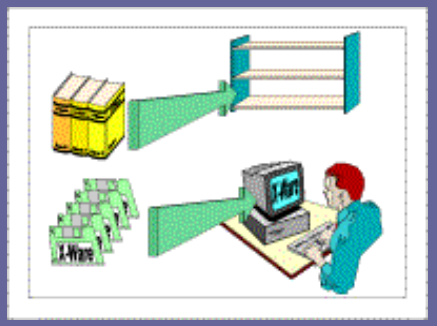
Was ist Informations-Technologie?



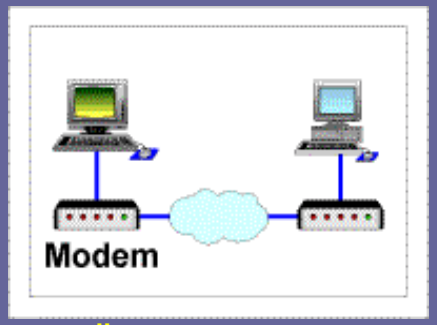
Einzel-PCs



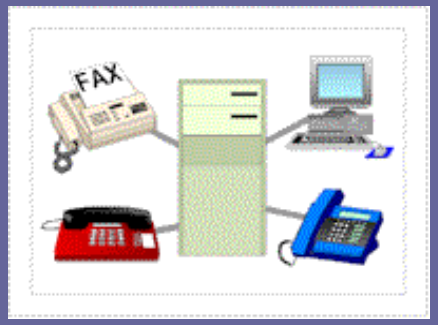
Computernetze



Software



DFÜ-Einrichtungen

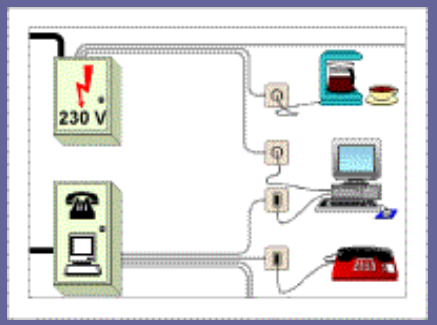


Telefonanlagen

Mobiltelefone

Anrufbeantworter, Fax

Heimarbeitsplätze



Infrastruktur, Verkabelung

dk-Computerschule – Gießen – Tel: 0641 / 971 921 0 – Fax: 971 921 1 – Mail: mail@dk-services.de – Internet: www.dk-services.de

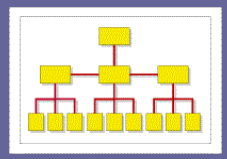
Warum IT-Sicherheit ?

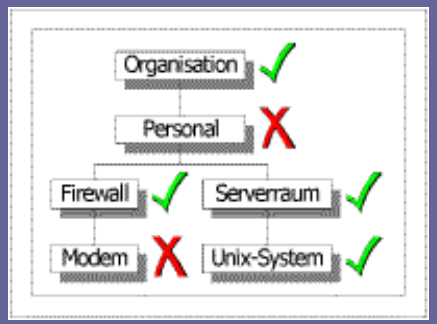
- Wir leben in einer **Informationsgesellschaft**.
- Das heutige Geschäftsleben ist in hohem Maße von einer funktionierenden **Informationstechnik** abhängig.
- Dieser Vortrag soll über **Risiken** und grundlegende **Maßnahmen** zu deren Vermeidung informieren.
- Der Schwerpunkt des Vortrags befasst sich mit dem **Computer** als IT-Gerät.
- Umfassende Informationen über das komplette Spektrum sind in der Literatur verfügbar. Eine umfassende, preiswerte Empfehlung finden Sie am Ende des Vortrags.

Wessen Angelegenheit ist **IT-Schutz** ?

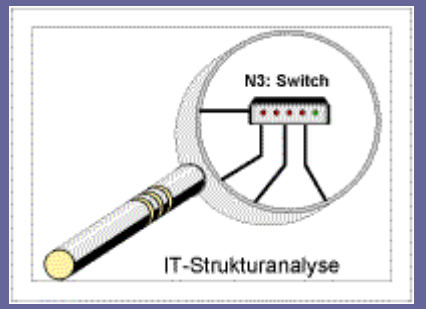
- IT Schutz ist ein umfassendes Konzept, welches sowohl
  - die Firma / Organisation,
  - IT-Spezialisten,
  - die IT-Technik sowie die
  - Mitarbeiter und
  - Private (Heimarbeit / Softwarenutzung)

  einbeziehen muss





Was beinhaltet IT-Schutz?



Analyse, Information und Massnahmen !

dk-Computerschule – Gießen – Tel: 0641 / 971 921 0 – Fax: 971 921 1 – Mail: mail@dk-services.de – Internet: www.dk-services.de

Was beinhaltet IT-Schutz?

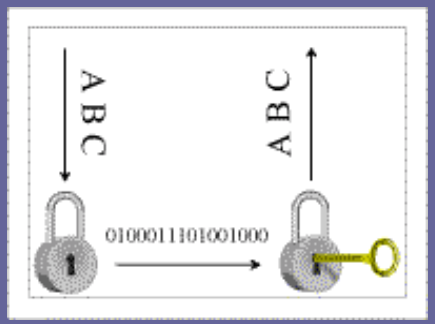
Sicherheitskonzepte

Vorsorge

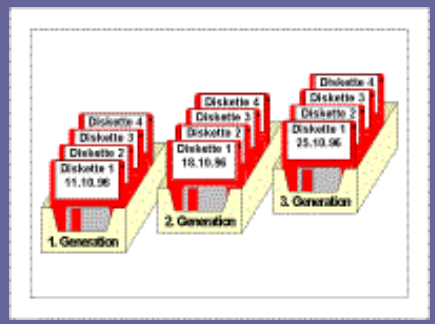
Abwehr

Information !

Schutz



Vertraulichkeit



Sicherung

dk-Computerschule – Gießen – Tel: 0641 / 971 921 0 – Fax: 971 921 1 – Mail: mail@dk-services.de – Internet: www.dk-services.de

Gebäude

Das Gebäude umgibt die aufgestellte Informationstechnik und gewährleistet somit einen äußeren Schutz. Weiterhin ermöglichen die Infrastruktur-Einrichtungen des Gebäudes erst den IT-Betrieb.

Für den **IT-Grundschutz eines Gebäudes** werden folgende **Typische Gefährdungen** angenommen

Höhere Gewalt:

- **Blitz, Feuer, Wasser**

Organisatorische Mängel:

- **Fehlende oder unzureichende Regelungen**
- **Unbefugter Zutritt zu schutzbedürftigen Räumen**

Technisches Versagen:

- **Ausfall der Stromversorgung**
- **Ausfall interner Versorgungsnetze**
- **Ausfall vorhandener Sicherungseinrichtungen**

Vorsätzliche Handlungen:

- **Unbefugtes Eindringen in ein Gebäude**
- **Diebstahl**
- **Vandalismus**

Büroraum

Für den **IT-Grundschutz eines Büroraums** werden folgende **Typische Gefährdungen** angenommen:

Organisatorische Mängel:

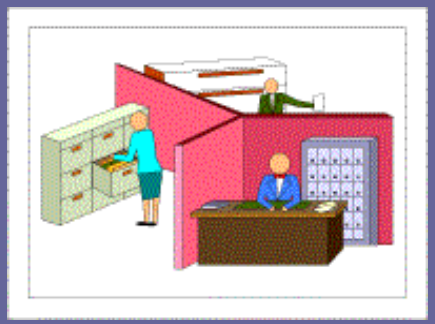
- Fehlende oder unzureichende Regelungen
- Unbefugter Zutritt zu schutzbedürftigen Räumen
- Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen

Menschliche Fehlhandlungen:

- Gefährdung durch Reinigungs- oder Fremdpersonal

Vorsätzliche Handlungen:

- Manipulation/Zerstörung von IT-Geräten oder Zubehör
- Manipulation an Daten oder Software
- Diebstahl
- Vandalismus



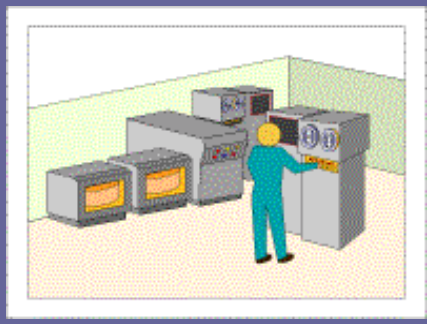
Server-Raum

- Der Serverraum dient in erster Linie zur Unterbringung eines Servers, z. B. eines LAN-Servers, eines Unix-Zentralrechners oder eines Servers für eine TK-Anlage.

- Darüber hinaus können dort serverspezifische Unterlagen, Datenträger in kleinem Umfang, weitere Hardware (Sternkoppler, Protokolldrucker, Klimatechnik) vorhanden sein.

- Im Serverraum ist oft kein ständig besetzter Arbeitsplatz eingerichtet; er wird nur sporadisch und zu kurzfristigen Arbeiten betreten.

- Zu beachten ist jedoch, daß im Serverraum aufgrund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als zum Beispiel in einem Büroraum.



Server-Raum

Für den **IT-Grundschutz eines Server-Raums** werden folgende **Typische Gefährdungen** angenommen :

Höhere Gewalt:

- **Feuer, Wasser**
- **Unzulässige Temperatur und Luftfeuchte**

Organisatorische Mängel:

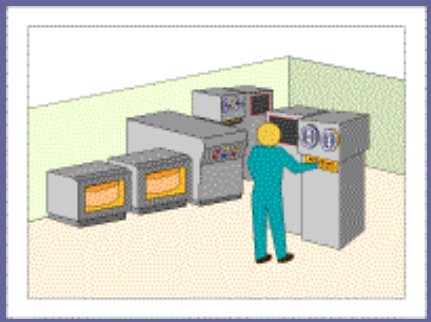
- **Fehlende oder unzureichende Regelungen**
- **Unbefugter Zutritt zu schutzbedürftigen Räumen**

Technisches Versagen:

- **Ausfall der Stromversorgung**
- **Ausfall interner Versorgungsnetze**
- **Spannungsschwankungen/überspannung/Unterspannung**

Vorsätzliche Handlungen:

- **Manipulation/Zerstörung von IT-Geräten oder Zubehör**
- **Manipulation an Daten oder Software**
- **Einbruch, Diebstahl**
- **Vandalismus**



Server-Raum

Maßnahmenempfehlungen

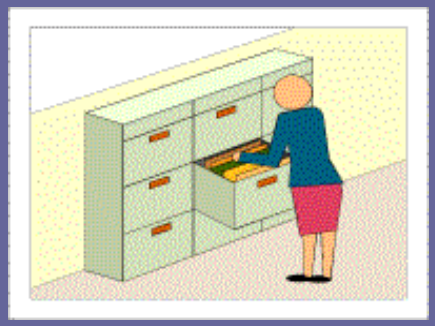
Infrastruktur:

- Angepaßte Aufteilung der Stromkreise
- Handfeuerlöscher
- Raumbelegung unter Berücksichtigung von Brandlasten
- Verwendung von Sicherheitstüren , geschlossene Fenster und Türen, abgeschlossene Türen
- Gefahrenmeldeanlage
- Vermeidung von wasserführenden Leitungen
- Überspannungsschutz
- Klimatisierung
- Lokale unterbrechungsfreie Stromversorgung
- Fernanzeige von Störungen

Organisation:

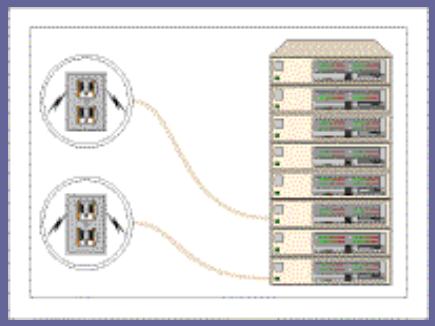
- Schlüsselverwaltung
- Beaufsichtigung oder Begleitung von Fremdpersonen
- Zutrittsregelung und –kontrolle
- Kontrollgänge
- Rauchverbot

Weitere vergleichbare Gefährdungen gelten für:



(Datenträger-) Archive

Sicherheits-Schränke



Technik-Räume

Heimarbeits-Plätze!

Allgemeine Gefährdungen eines PC-Systems

Unberechtigte Nutzung

- zuverlässige Kennwörter vergeben
- Kennwörter nicht weitergeben
- Nutzen Sie die Möglichkeiten professioneller Betriebssysteme und Softwareprodukte, Benutzer zu identifizieren und zu authentifizieren.
- Anhand der Identifikation lassen sich dann Zugriffsrechte regeln (nicht auf PCs unter den Betriebssystemen DOS, Windows 95/98/ME).
- Führen Sie Zugriffsprotokoll-Dateien und werten Sie diese auch aus.

Löschen von Daten

- Versehentliches Löschen/Überschreiben von Dateien richtet nach Meinung vieler Statistiken mehr Schaden an als Viren!
- Vorbeugung: Schulung der Mitarbeiter, Verwalten von Lösch- und Änderungsrechten durch den Systemverwalter, Datensicherung
- Arbeiten Sie mit Dokumentenvorlagen, anstatt „einen alten Brief“ als Vorlage zu benutzen. Allzu leicht vergißt man beim Speichern das Ändern des Dateinamens.

Allgemeine Gefährdungen eines PC-Systems

Manipulation von Daten

- Die Hauptgefahr ist hier neben dem Verlust der echten Daten die schwere Erkennbarkeit der Manipulation. Eventuell wird dann mit falschen Daten weiter gearbeitet.
- Auch manche Viren manipulieren Daten, statt „nur“ zu zerstören.
- Protokollieren Sie Zugriffe und Änderungen, wenn das System dies erlaubt.

Zerstörung von Daten

- Dies meint die böswillige Zerstörung von Datenbeständen, z.B. durch Viren, trojanische Pferde, Würmer, usw.
- Treffen Sie Maßnahmen zur Vorbeugung und Abwehr: Datensicherung, Firewalls, Virenscanner

Technisches Versagen

- Defekte Festplatten führen in der Regel zu einem kompletten Datenverlust!
- Bei defekten Platinen u.ä. können meist die Daten auf der Festplatte nach Reparatur oder Einbau in einen anderen Rechner noch gelesen werden.
- In jedem Fall ist eine regelmäßige Datensicherung als vorbeugende Maßnahme wichtig.

Vorsorge: Datenschutz

Kennwortschutz des lokalen PC´s

- Alle PCs, die den Zugang zu vertraulichen Daten ermöglichen, sind mit einem Kennwort zu schützen.
- Kennwörter können Sie auf der Ebene des PC´s (beim Start im BIOS) und auf der Ebene des Betriebssystems definieren.
  - Achtung: das BIOS-Kennwort kann in wenigen Minuten überwunden werden, wenn dem Angreifer das Öffnendes PC-Gehäuses möglich ist (Reset des BIOS auf Herstellerwerte).
- **Achtung:** DOS und Windows 95/98/Me haben ohne Unterstützung durch Spezialsoftware keinen lokalen Kennwortschutz, sondern identifizieren nur den Nutzer. Ein Schutz gegen unberechtigten lokalen Zugriff ist nicht möglich! Eine Anmeldung unter einem neuen Namen ist jederzeit möglich.

Kennwörter: Richtlinien

Folgende Regeln zum Kennwortgebrauch sollten beachtet werden:

- Das Paßwort darf nicht leicht zu erraten sein wie Namen, Kfz-Kennzeichen, Geburtsdatum.
- Innerhalb des Paßwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Das Paßwort sollte mindestens 6 Zeichen lang sein.
- Das Paßwort muß **geheimgehalten** werden und sollte nur dem Benutzer persönlich bekannt sein.
- Das Paßwort muß regelmäßig gewechselt werden, z. B. alle 90 Tage.
- Ein Paßwortwechsel ist durchzuführen, wenn das Paßwort unautorisierten Personen bekannt geworden ist.
- Voreingestellte Paßwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Paßwörter ersetzt werden.
- Paßwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.

Kennwörter

Folgende Regeln zum Kennwortgebrauch sollten beachtet werden:

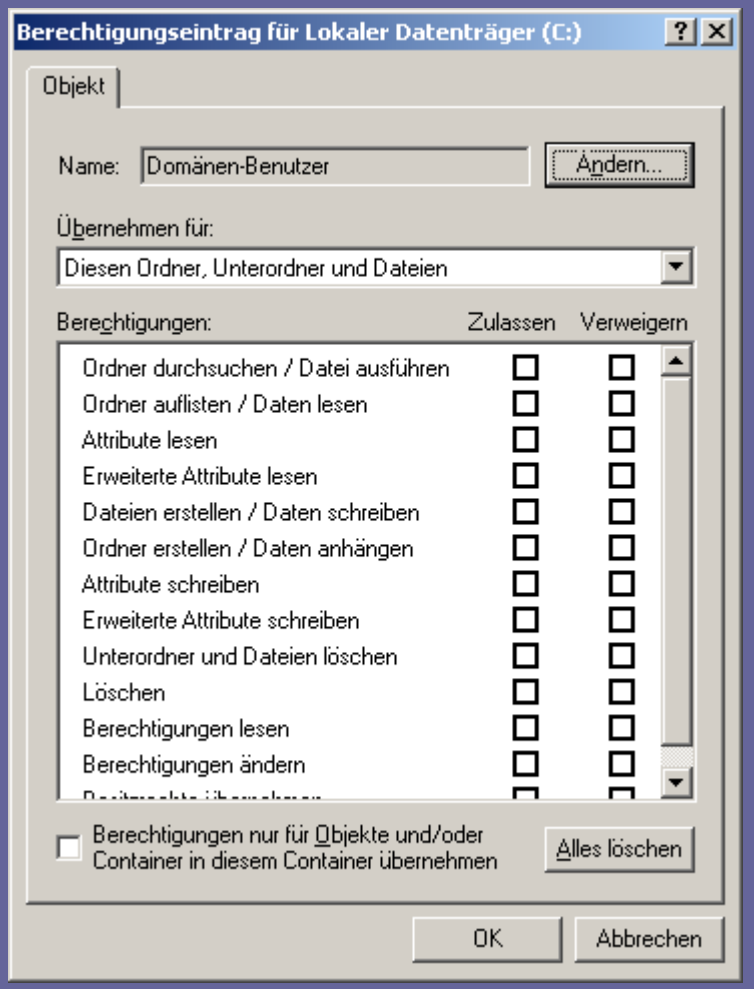
- Das Paßwort sollte nur für die Hinterlegung schriftlich fixiert werden, wobei es dann in einem verschlossenen Umschlag sicher aufbewahrt wird. Wird es darüber hinaus aufgeschrieben, ist das Paßwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren
- Alte Paßwörter sollten nach einem Paßwortwechsel nicht mehr gebraucht werden.
- Der Paßwortwechsel sollte vom System regelmäßig initiiert werden.
- Die Wiederholung alter Paßwörter beim Paßwortwechsel sollte vom IT-System verhindert werden (Paßwort-Historie).
- Die Eingabe des Paßwortes sollte unbeobachtet stattfinden.
- Die Wahl von Trivialpaßwörtern ("BBBBBB", "123456") sollte verhindert werden.

Kennwörter

- Jeder Benutzer muß sein eigenes Paßwort jederzeit ändern können.
- Für die Erstanmeldung neuer Benutzer sollten Einmalpaßwörter vergeben werden, also Paßwörter, die nach einmaligem Gebrauch gewechselt werden müssen. In Netzen, in denen Paßwörter unverschlüsselt übertragen werden, empfiehlt sich die dauerhafte Verwendung von Einmalpaßwörtern
- Nach dreifacher fehlerhafter Paßworteingabe sollte eine Sperrung erfolgen, die nur vom Systemadministrator aufgehoben werden kann.
- Bei der Authentisierung in vernetzten Systemen sollten Paßwörter nicht unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Paßwort nicht auf dem Bildschirm angezeigt werden.
- Die Paßwörter sollten im System zugriffssicher gespeichert werden, z. B. mittels Einwegverschlüsselung.

Datenschutz: Rechtevergabe

- Authentifizierung des Zuganges anhand von Kennwörtern
- Nach erfolgter Authentifizierung muss das System jedem Anwender die Rechte zum Erstellen, Ändern, und Lesen von Daten zuweisen, oder verweigern.
- Diese Rechte sind für alle Server, Laufwerke, Verzeichnisse, Dateien, und Datenbanken zu regeln
- Der Administrator profitiert hier von der Möglichkeit, Gruppenrechte, Rollen oder „Rechtevererbung“ von über- auf untergeordnete Ebenen zu nutzen.
- Dies ist im Umfang abhängig vom jeweiligen System, hier Windows 2000



Datenschutz: Verschlüsselung

- Vertrauliche Daten und/oder Datenträger sollten verschlüsselt werden, wenn die Gefahr besteht, daß diese in unbefugte Hände geraten (z.B. Diebstahl eines Laptops).
- Hierfür gibt es spezielle Software, wenn die benutzte Software dies nicht eigenständig macht, z.B. „PGP: Pretty Good Privacy“
- Ebenso sollte die Übertragung von Datenpaketen auch im lokalen Netzwerk verschlüsselt erfolgen.

Datensicherung

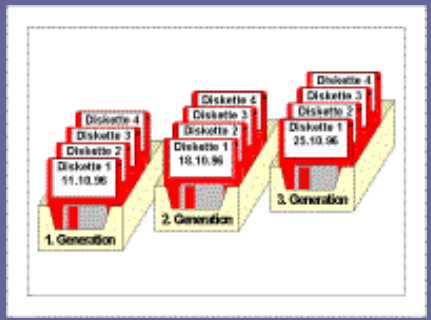
- Für den Fall eines eingetretenen Datenverlustes ist eine **Datensicherung** notwendig.
- Die Datensicherung ermöglicht die **Rekonstruktion** verlorener Datenbestände.
- Für die Sicherung von Daten sind **Administratoren wie auch Anwender verantwortlich.**

Administratoren:

- **regelmäßige Backups** der Datenbestände erstellen
- **Überprüfen** des Erfolges von Backups!

Anwender:

- Speichern aller wichtigen Daten auf Netzwerklaufwerken, damit sie beim Backup erfasst werden
- Daten auf lokalen PCs (Laptops!) werden in der Regel nicht beim Backup erfasst. Für deren Sicherung ist der PC-Benutzer verantwortlich.



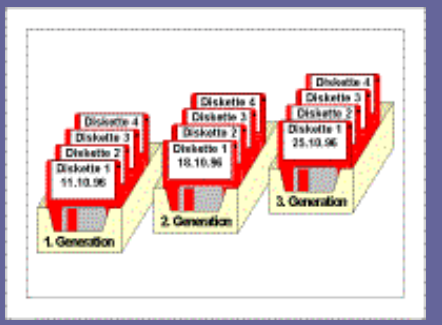
Datensicherung: wie?

Sicherung des Servers

- Diese erfolgt mit Hilfe **spezieller Datensicherungsgeräte**, in der Regel Magnetbandlaufwerke (Streamer).
- Weiterhin bieten Festplattenspiegelung, RAID-Systeme usw. erhöhten Datensicherheit.

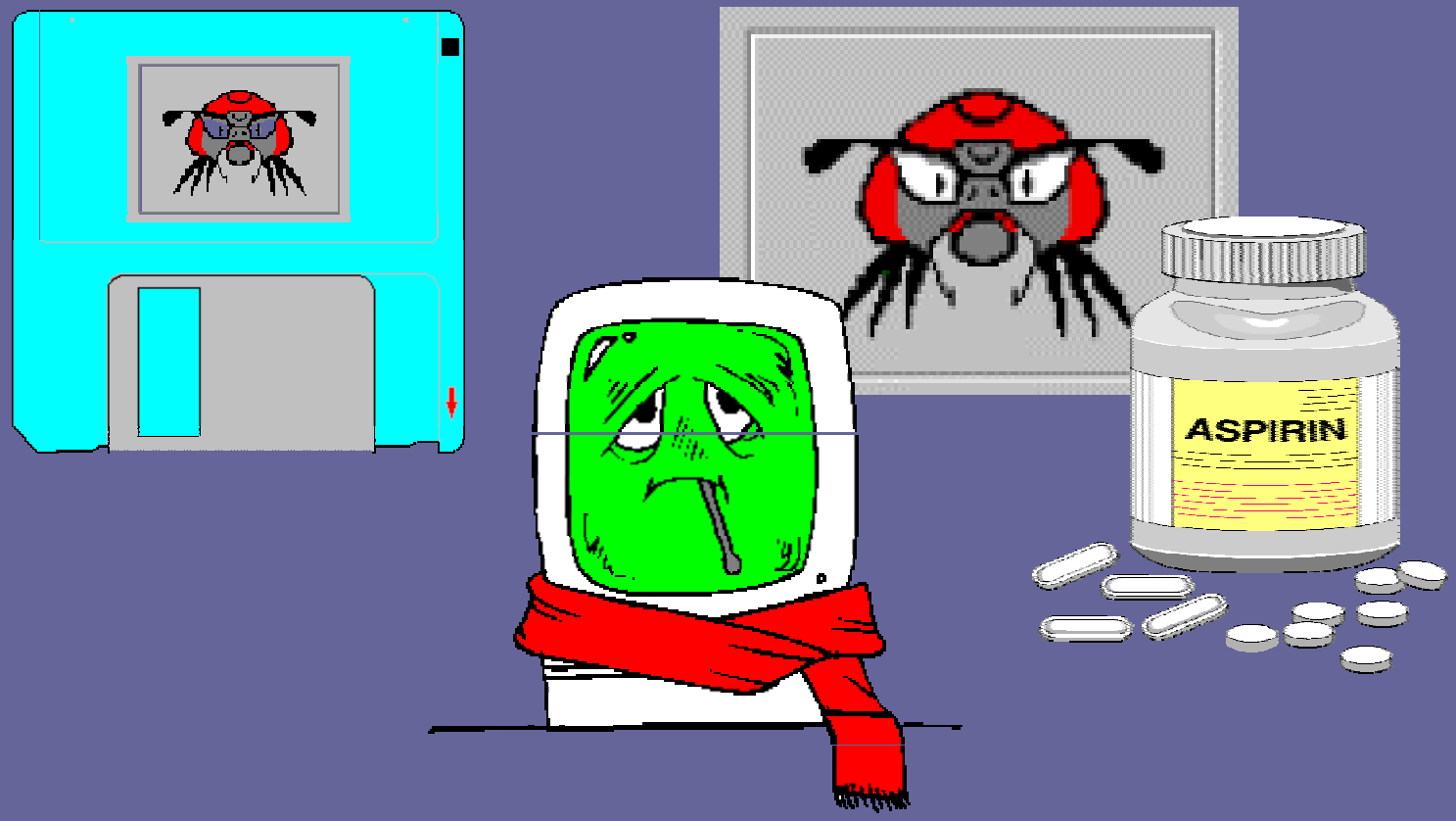
Sicherung von Workstations/Laptops

- Sichern Sie, wenn möglich, im Netzwerk
- **Wichtige lokale Daten müssen auf andere Datenträger kopiert werden**
- Je nach Umfang der Daten eignen sich insbesondere **Wechselmedien**, wie Disketten, ZIP-Disketten, oder das Brennen einer Daten-CD-ROM.
- Eine zweite Festplatte eignet sich nur bedingt, denn bei einem Virenangriff fällt auch die Sicherung dem Virus zum Opfer
- Eine Zweit-Kopie auf der gleichen Festplatte ist als Datensicherung völlig ungeeignet, da diese noch nicht einmal vor einem technischen Versagen schützt.
- Testen Sie, ob die Daten im Ernstfall rekonstruiert werden könnten! Schon oft waren Datenträger nicht lesbar oder leer!



Viren, Würmer, und Trojanische Pferde...

gibt es leider auch in der PC-Welt



Computer-Viren

Viren:

- Computer-Viren gehören zu den Programmen mit Schadensfunktionen. Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Daten oder Programmen sicherlich von größter Tragweite. Solche Funktionen von Programmen können sowohl unbeabsichtigt als auch bewußt gesteuert auftreten.
- Die Definition eines Computer-Virus bezieht sich nicht unmittelbar auf eine möglicherweise programmierte Schadensfunktion:
- *Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)*

Makro-Viren

- Mit dem Austausch von Dateien (z. B. per **E-Mail**) besteht die Gefahr, daß neben der eigentlichen Datei (Textdatei, Tabelle etc.) weitere, mit dem Dokument verbundene Makros übersandt werden.
- Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Winword, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert bzw. das Makro automatisch gestartet wird.
- Wird ein Dokument über einen WWW-Browser empfangen, der das Dokument automatisch öffnet, kann hierdurch ein (Auto-) Makro aktiviert werden.
- Da die Makrosprachen über einen sehr umfangreichen Befehlssatz verfügen, besteht auch die Gefahr, daß einem Dokument ein Makro beigefügt wird, das eine Schadfunktion enthält (z. B. einen Virus).
- In der Praxis hat diese Gefährdung insbesondere bei den Dateien der Programme Word für Windows, Excel und Outlook der Firma Microsoft weltweit beträchtlich zugenommen.
- **Die Word-Makro-Viren haben inzwischen die Spitzenstellung bei gemeldeten Infektionen eingenommen**.

Würmer

Würmer

- „kriechen“ durch Netzwerke, indem sie z.B. nach dem Öffnen eines E-Mails sich selbst weiter per Mail versenden, ohne daß der Anwender dies merkt.
- Der neue Empfänger wird ebenfalls geschädigt, und versendet seinerseits unbemerkt den Wurm an Dritte
- Kürzlich hat der Wurm „I LOVE YOU“ auf diese Weise Tausende vonRechnern befallen.
- Neben seiner reinen Verbreitung, welche alleine bereits Netzwerke stilllegen kann, können weitere Schädigungen auftreten(z.B. Datenverluste).

Trojanische Pferde

- Ein **Trojanisches Pferd** ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Der Benutzer kann daher auf die Ausführung dieser Funktion keinen Einfluss nehmen, insoweit besteht eine gewisse Verwandtschaft mit Computer-Viren. Es ist jedoch keine Selbstreproduktion vorhanden. Als Träger für Trojanische Pferde lassen sich alle möglichen Anwenderprogramme benutzen.
- Diese „Schädlinge“ **täuschen vor**, ein **nützliches Programm**, ein interessanter Bildschirmschoner oder ein Spiel zu sein.
- **Damit wird das Interesse des Anwenders geweckt**. Ist das vordergründige Programm gestartet, dann kann der in diesem Programm zusätzlich eingeschleuste Trojaner im Verborgenen sein Unwesen treiben.
- Solche Trojaner können z.B. Kennwörter oder sogar Kreditkartennummern protokollieren und bei nächster Gelegenheit per E-Mail an die „Hacker“ senden.

Trojanische Pferde

"Ein Kinderspiel" - Realschüler knackten Computer der Telekom
Sicherheitslücke bei größtem Online-Anbieter aufgedeckt

BM/dpa Hamburg *- "Sicher wie die Bank von England" - Mit flotten Sprüchen wirbt der Telekom-Dienst "T-Online" für die Sicherheit seines Systems. Doch für zwei 16 Jahre alte Schüler war es nur "ein Kinderspiel", den Zugang zum größten Online-Dienst zu knacken. Mit einem kleinen manipulierten Windows-Programm, einem sogenannten "Trojanischen Pferd", brachten sie die Zugangsdaten von über 600 T-Online-Kunden in ihren Besitz, mit denen sie Rechnungen von insgesamt mehreren 10 000 Mark hätten verursachen können.*

Die spektakuläre Aktion der beiden pfiffigen Realschüler deckt grundsätzliche Schwachstellen des T-Online-Systems auf. Die Programmierer der Telekom arbeiten nun fieberhaft an einer neuen Version der Zugangssoftware, die Hacker-Angriffen besser widerstehen soll.

Die Hacker-Attacke der beiden Realschüler wird von Experten als besonders gravierend eingeschätzt. T-Online wird nämlich von vielen Kunden zum Homebanking sowie dem kostenpflichtigen Abruf von Angeboten wie Datenbanken oder Auskunftsdiensten - aber auch Sex-Seiten - genutzt.

Hoax

Ein Hoax (englisch für Streich, Trick, falscher Alarm) ist eine Nachricht, die eine Warnung vor neuen spektakulären Computer-Viren oder anderen IT-Problemen enthält und Panik verbreitet, aber nicht auf realen technischen Fakten basiert.

Meist werden solche Nachrichten über E-Mails verbreitet. Beispielsweise wird dabei vor Computer-Viren gewarnt, die Hardware-Schäden verursachen können oder durch das bloße Öffnen einer E-Mail (nicht eines Attachments) zu Infektionen und Schäden führen können und die durch keine Antiviren-Software erkannt werden.

Neben dieser Warnung wird darum gebeten, die Warnmeldung an Freunde und Bekannte weiterzuleiten. Noch wirksamer wird ein solcher Hoax, wenn als Absender eine gefälschte Adresse angegeben wird, wie zum Beispiel die eines namhaften Herstellers.

Ein solcher Hoax ist nicht zu verwechseln mit einem Computer-Virus, der tatsächlich Manipulationen am IT-System vornehmen kann. Vielmehr handelt es sich um eine irreführende Nachricht, die ohne Schaden gelöscht werden kann und sollte.

Die einzigen Schäden, die ein Hoax herbeiführt, sind die Verunsicherung und Irritation der Empfänger und ggf. die Kosten an Zeit und Geld für den Weiterversand des Hoax.

Im Bereich des Mobilfunks gab es eine ganze Reihe solcher Hoax-Nachrichten, bei denen davor gewarnt wurde, dass an Mobiltelefonen die Eingabe bestimmter Tastenkombinationen oder die Wahl bestimmter Rufnummern dazu führen könnten, Gespräche abzuhören oder auf Kosten anderer zu telefonieren. Durch die Nennung bestimmter Mobiltelefon-Marken und einiger technischer Ausdrücke wird der Anschein von Seriosität erweckt. Solche Gerüchte halten sich hartnäckig und verunsichern die Benutzer.

Beispiel:

Im Frühjahr 2000 kursierte folgende Falschmeldung per E-Mail (und teilweise sogar per Brief):

"Wenn sie eine Nachricht auf Ihr Handy erhalten, dass sie unter der Nummer 0141-455xxx zurückrufen sollen, antworten sie auf keinen Fall darauf. Ihre Rechnung steigt sonst ins Unermessliche.

Diese Information wurde von der "Zentralstelle zur Unterdrückung von betrügerischen Machenschaften" (Office Central de Repression du Banditisme) herausgegeben. ..."

Virenschutz

Organisation:

Erstellung eines Computer-Virenschutzkonzepts

Identifikation potentiell von Computer-Viren betroffener IT-Systeme

Auswahl eines geeigneten Computer-Viren-Suchprogramms

Meldung von Computer-Virusinfektionen

Aktualisierung der eingesetzten Computer-Viren-Suchprogramme

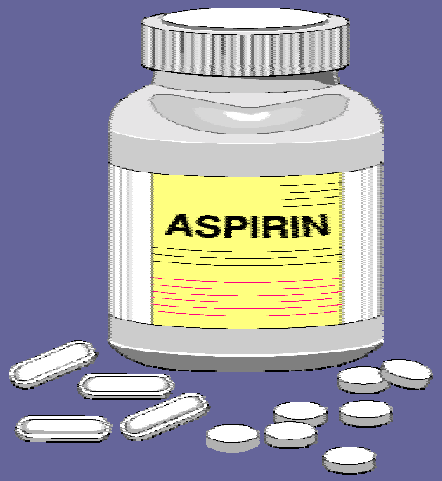
Regelungen zum Computer-Virenschutz

Nutzungsverbot nicht freigegebener Software

Überprüfung des Software-Bestandes

Dokumentation der Veränderungen an einem bestehenden System

Informationsbeschaffung über Sicherheitslücken des Systems



Virenschutz

Personal:

Schulung zu IT-Sicherheitsmaßnahmen

Hardware/Software:

Regelmäßiger Einsatz eines Viren-Suchprogramms

Einsatz eines Viren-Suchprogrammes bei Datenträgeraustausch und Datenübertragung

Prüfung eingehender Dateien auf Makro-Viren

Nutzung der BIOS-Sicherheitsmechanismen

Notfallvorsorge:

Verhaltensregeln bei Auftreten eines Computer-Virus

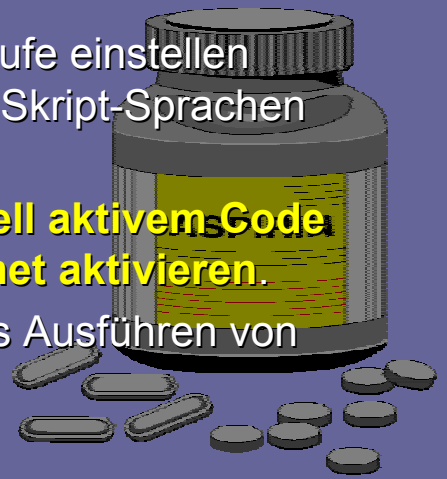
Erstellen einer PC-Notfalldiskette

Regelmäßige Datensicherung

Virenschutz: Anwender

Einstellungen am Rechner

- Bereits durch das Aktivieren verfügbarer Sicherheitsfunktionen wird das Eindringen von Computer-Viren erheblich erschwert.
- **Alle vorhandenen Sicherheitsfunktionen des Rechners aktivieren** (Passwort-Schutz, Bildschirmschoner mit Passwort, etc.), damit während der Abwesenheit des berechtigten Benutzers Unbefugte keine Möglichkeit haben, durch unbedachte oder gewollte Handlungen den Rechner zu gefährden.
- **Aktuelles Viren-Schutzprogramm mit aktuellen Signatur-Dateien** einsetzen, das im Hintergrund läuft (resident) und bei bekannten Computer-Viren Alarm schlägt.
- Im Microsoft Explorer sollte die **Anzeige aller Dateitypen** aktiviert sein.
- **Makro-Virenschutz von Anwendungsprogrammen** (WinWord, Excel, Powerpoint, etc.) aktivieren und Warnmeldungen beachten.
- **Sicherheitseinstellungen von Internet-Browsern** auf höchste Stufe einstellen (Deaktivieren von aktiven Inhalten (ActiveX, Java, JavaScript) und Skript-Sprachen (z.B. Visual Basic Script, VBS), etc.).
- **Keine Applikationsverknüpfung für Anwendungen mit potentiell aktivem Code (MS-Office) im Browser nutzen oder Anwendungen über Internet aktivieren.**
- Sicherheitseinstellungen (ECL) bei Lotus Notes bearbeiten und das Ausführen von "gespeicherten Masken" per Datenbank unterbinden.

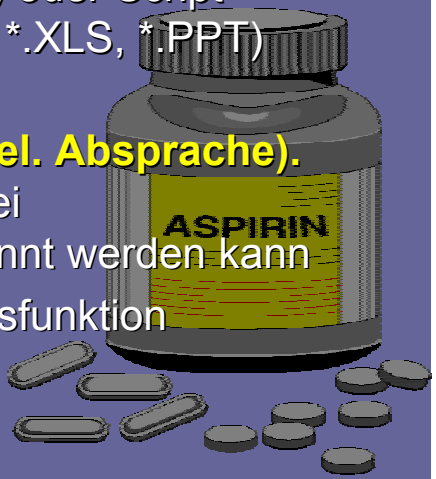


Virenschutz: Anwender

Verhalten bei eingehender E-Mail

Eingehende E-Mail ist das größte Einfalltor für Computer-Viren. Bei sicherheitsbewusstem Verhalten lassen sich hierbei schon die meisten Viren herausfiltern.

- Offensichtlich nicht sinnvolle E-Mails von unbekannten Absendern sofort ungeöffnet löschen (?).
- **Bei E-Mail auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern prüfen, ob der Text der Nachricht auch zum Absender passt** (englischer Text von deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde.
- **Vorsicht bei mehreren E-Mails mit gleichlautendem Betreff.**
- **Kein "Doppelklick"** bei ausführbaren Programmen (*.COM, *.EXE) oder Script-Sprachen (*.VBS, *.BAT), Vorsicht auch bei Office-Dateien (*.DOC, *.XLS, *.PPT) sowie Bildschirmschonern (*.SCR).
- **Nur vertrauenswürdige E-Mail-Attachments öffnen (z. B. nach tel. Absprache).** Es ist zu beachten, dass die Art des Datei-Anhangs (Attachment) bei Sabotageangriffen oft getarnt ist und über ein Icon nicht sicher erkannt werden kann
- Auch eine E-Mail im HTML-Format kann aktive Inhalte mit Schadensfunktion enthalten.



Virenschutz: Anwender

Ausgehende E-Mail

Durch Beachtung der folgenden Maßnahmen kann die Gefahr reduziert werden, dass ein Endanwender unabsichtlich Computer-Viren verteilt.

- **E-Mails nicht im HTML-Format versenden**, auch wenn es vom eingesetzten Mail-Programm her möglich wäre; ebenso sind aktive Inhalte in E-Mails zu vermeiden.
- **WinWord-Dokumente im RTF-Format versenden** (Damit wird auch die Weiterleitung von ggf. vertraulichen Informationen im nicht direkt sichtbaren Verwaltungsteil der DOC-Datei verhindert.)
- **Keine unnötigen E-Mails mit Scherz-Programmen und ähnlichem versenden**, da diese evtl. einen Computer-Virus oder Trojaner enthalten können.
- **Gelegentlich prüfen, ob E-Mails im Ausgangs-Postkorb stehen, die nicht vom Benutzer selbst verfasst wurden.**
  Dies ist ein Hinweis z.B. auf Trojaner!
- Keinen Aufforderungen zur Weiterleitung von Warnungen, Mails oder Anhängen an Freunde, Bekannten oder Kollegen folgen, sondern direkt nur an den IT-Sicherheitsbeauftragten senden. Es handelt sich nämlich meist um irritierende und belästigende Mails mit Falschmeldungen (Hoax oder "elektronische Ente", Kettenbrief).

Virenschutz: Anwender

Verhalten bei Downloads aus dem Internet

Daten und Programme, die aus dem Internet abgerufen werden, stellen einen Hauptverbreitungsweg für Computer-Viren und Trojanische Pferde dar, um Benutzerdaten auszuspähen, weiterzuleiten, zu verändern oder zu löschen.

- Programme sollten nur von vertrauenswürdigen Seiten geladen werden, also insbesondere von den Originalseiten des Erstellers. Private Homepages, die bei anonymen Webspace-Providern eingerichtet werden, stellen hierbei eine besondere Gefahr dar.
- **Die Angabe der Größe von Dateien, sowie einer evtl. auch angegebenen Prüfsumme, sollte nach einem Download immer überprüft werden.**
  Bei Abweichungen von der vorgegebenen Größe oder Prüfsumme ist zu vermuten, dass unzulässige Veränderungen, meist durch Viren, vorgenommen worden sind. Daher sollten solche Dateien sofort gelöscht werden.
- Mit einem **aktuellen Viren-Schutzprogramm** sollten vor der Installation die Dateien immer überprüft werden.
- **Gepackte (komprimierte) Dateien** sollten erst entpackt und auf Viren überprüft werden. Installierte Entpackungsprogramme sollten so konfiguriert sein, dass zu entpackende Dateien nicht automatisch gestartet werden.
- Es muß darauf hingewiesen werden, dass auch **Office-Dokumente** (Text-, Tabellen- und Präsentations-Dateien) Makro-Viren enthalten können.

Virenschutz: Administratoren

Zentrale Schutzmaßnahmen

- **Viren-Schutzprogramme zur zentralen Überprüfung des E-Mail-Verkehrs sind auf Mail-Servern und Gateways zu installieren und regelmäßig zu aktualisieren.**
- **Einsatz von Viren-Schutzprogrammen mit regelmäßiger automatisierter Aktualisierung** (Update), da ein veraltetes Schutzprogramm nur für ein falsches Sicherheitsgefühl sorgt. Die Programme sollten sowohl zentral bei der Überwachung der E-Mail eingesetzt werden (File- bzw. Mail-Server), als auch lokal beim Endanwender (Client), damit dieser auch bei verschlüsselter Kommunikation geschützt ist.
- **Die Konfiguration der E-Mail-Clients sollte so eingestellt sein, dass Attachments nicht automatisch geöffnet werden.**
- Außerdem sollten als E-Mail-Editor keine Programme mit der Funktionalität von Makro-Sprachen (z.B. WinWord) oder Scripts eingesetzt werden. Aus Sicherheitsgründen sollte ebenfalls das HTML-Format nicht verwendet werden.
- Für Probleme ist ein zentraler Ansprechpartner (E-Mail-Adresse, Telefon- und Fax-Nummer) zu benennen.

Virenschutz: Administratoren

Zentrale Schutzmaßnahmen

- **Filterregeln an Gateways oder Firewalls, sowie die Nutzung von "Policies" sind zur Erhöhung der Sicherheit gut geeignet.** Derartige Maßnahmen erfordern oft keine teuren Zusatzprodukte. Dabei können Datei-Typen (z.B. *.VBS, *.WSH, *.BAT, *.EXE), die im täglichen Arbeitsablauf nicht als Anhänge von E-Mails vorkommen, gleich zentral abgeblockt werden.
- **Es sollten nur vertrauenswürdige E-Mail-Programme zugelassen sein**, die auch über entsprechende Sicherheitsfunktionen verfügen. "Private" Insel-Lösungen auf einzelnen Arbeitsplatz-Rechnern dürfen nicht zugelassen werden, um die Sicherheit des Gesamtsystems nicht zu gefährden.
- **Rechner, auf denen für die Organisation, Firma oder Behörde kritische Anwendungen laufen, müssen ohne E-Mail und Internet-Zugang betrieben werden**.
- **Rechner mit ungeschützter externer Kommunikationsverbindung (z.B. Modem ohne Anschluss über gesicherte Gateways und Firewalls) dürfen nicht gleichzeitig mit dem Firmen- oder Behörden-Netz verbunden sein.**
- **Und nicht zu vergessen – Datensicherung!**
  Bei Datenverlust ist das die einzige Maßnahme, die einen Weiterbetrieb der Firma, Organisation oder Behörde ermöglicht.

Datenträger-Austausch

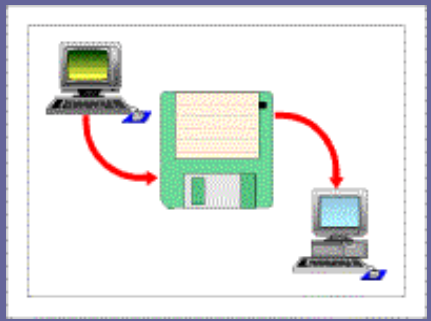
Gemeint ist der Austausch von Datenträgern zur Datenübertragung zwischen nicht vernetzten IT-Systemen.

Zu berücksichtigende Datenträger sind z.B. **Disketten**, **Wechselplatten** (magnetisch, magneto-optisch), **CDs**, **Magnetbänder** und **Kassetten**.

Grundsätzlich gelten die **gleichen Gefährdungen** und **Schutzmaßnahmen** wie beim Austausch von Dateien über E-Mail oder Internet.

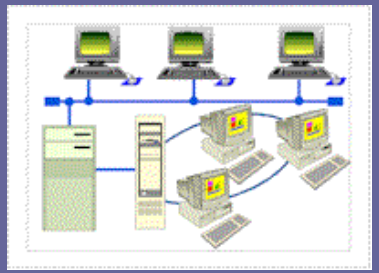
Zusätzlich ist zu beachten, daß die Datenträger während des Transports in unbefugte Hände gelangen können.

Dies erfordert unter Umständen Datenschutz durch Verschlüsselung.



„Hacker“ im Netzwerk / Internet

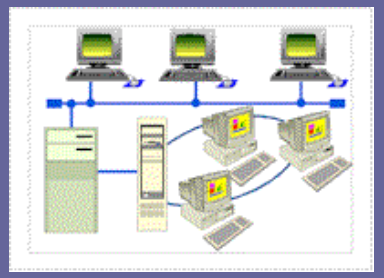
- Grundsätzlich besteht die Gefahr, daß Daten auf Ihrem PC durch Hacker „belauscht“ werden, wenn Ihr PC in ein Netzwerk eingebunden ist, oder über einen Internet-Anschluß verfügt.
- Die Gefahren, die innerhalb eines Firmennetzwerks bestehen, werden von vielen unterschätzt. Firmeninterne Informationen sind für Hacker oft viel interessanter als irgendwelche Daten fremder Firmen.
- Tatsache ist, daß eventuelle Täter es innerhalb der Firma viel leichter haben, Daten zu belauschen, als ein Angreifer aus dem Internet.
- Ihnen gelingt der Zugriff auf den PC oder auf Netzwerk-Laufwerke viel leichter, denn sie sind bereits selbst im Firmennetz und müssen nicht erst die Sicherheitsmechanismen überwinden, welche die Firma in Form einer Firewall nach außen aufbaut.



„Hacker“ im Netzwerk / Internet

- Geben Sie also niemals Ihr Kennwort an Kollegen weiter. Diese könnten damit später unbefugt andere Daten abrufen, an die Sie heute gar nicht denken.
- Speichern Sie niemals z.B. PIN / TAN-Nummern auf Ihrem PC, auch wenn Ihr Homebanking dadurch unbequemer wird. Wer Zugang zum PC erlangt, kann dann auch auf Ihr Konto zugreifen.
- Melden Sie sich von Ihrem PC ab, wenn Sie das Büro verlassen
- Benutzen Sie Bildschirmschoner mit Kennwortschutz.

SICHERHEIT IST LEIDER UNBEQUEM !



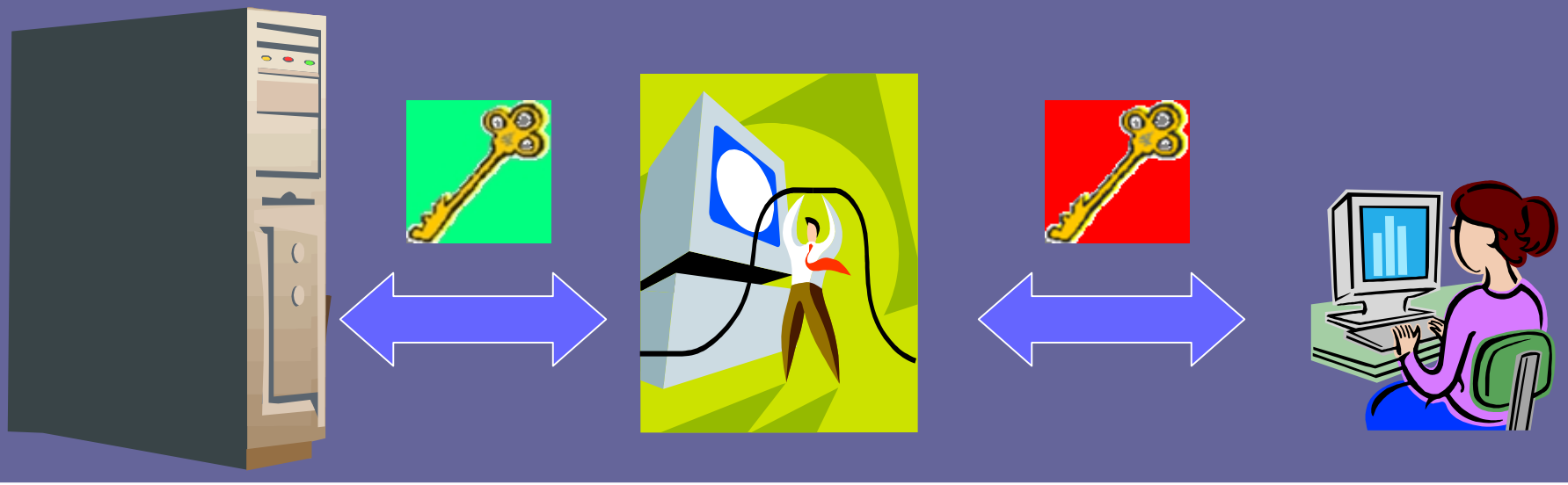
Risiko TCP / IP

- **Internet-Verbindungen werden über das TCP/IP – Protokoll abgewickelt.**
- Jeder Rechner im Internet oder lokalen Netz verfügt über eine eindeutige IP-Adresse, welche ihn identifiziert, z.B. 192.198.0.178
- Zwei Rechner kommunizieren anhand dieser Adressen über sogenannte „Ports“, welche quasi Leitungen für bestimmte Dienste darstellen.
- TCP/IP verfügt über Dutzende von Ports, von denen meist nur wenige für Dienste genutzt werden.
- Leider bleiben auf vielen Rechnern in Standard-Konfiguration die restlichen Ports geöffnet
- **Offene TCP/IP-Ports stellen ein leichtes Einfallstor für Hacker dar.**
- **Es gibt spezielle „Port-Scanner“-Software, mit welcher Hacker systematisch und automatisch nach offenen Ports suchen können**
- Natürlich sollten auch Administratoren solche Port-Scanner einsetzen, um Schwachstellen des Systems zu erkennen.
- Auch viele Trojanischen Pferde öffnen dem Hacker zuvor geschlossene TCP/IP-Ports!

Szenario eines Hacker-Angriffs: die „Man-in-the-Middle-Attack“

- Durch einen Trojaner gelingt es dem Hacker, ein simuliertes Sicherheitszertifikat auf einem PC einzuschleusen.
- Gleichzeitig leitet er alle Anfragen an die „Sparkasse Nirgendwo“ über seinen eigenen PC um.
- Der Anwender vertraut der verschlüsselten Verbindung mit der Bank
- In Wirklichkeit wird jedoch der falsche Schlüssel des Hackers verwendet, er kann mitlesen.
- Damit er nicht auffällt, leitet sein PC anschließend Ihre Anfragen mit dem echten Schlüssel an die Bank weiter, die diesen Angriff daher auch nicht bemerkt.
- Umgekehrt empfängt er Datenpakete der Bank, und leitet diese mit seinem falschen Schlüssel an den Kunden weiter.
- Der Hacker gelangt in den Besitz aller Konto-Informationen

Szenario eines Hacker-Angriffs: die „Man-in-the-Middle-Attack“



Sparkasse Irgendwo	Daten mit echtem Schlüssel	PC des Hackers	Daten mit falschem Schlüssel	Kunde

Sicherheitszertifikate

- Ganz schutzlos sind Sie diesem Angriff nicht ausgeliefert, da die Sicherheits-Zertifikate üblicherweise zertifiziert sind.
- Ihr Browser zeigt die Zertifikate und deren Einstufung an.
- Fälschungen fallen auf, wenn Sie aufmerksam lesen.
- Allerdings: längst nicht alle bemängelten Zertifikate stammen von Hackern!
- Oft ist dem Browser nur die Zertifizierungsstelle unbekannt.
- Sie können auch bemängelten Zertifikaten vertrauen, wenn Ihnen die Herkunft sicher bekannt ist.
- Zum Beispiel: Ihre Bank hat Ihnen für Ihr Online-Banking ein Zertifikat in Form einer Diskette oder Chip-Karte persönlcih ausgehändigt. Dies ist im Online – Banking per HSCB-Verfahren weit verbreitet.

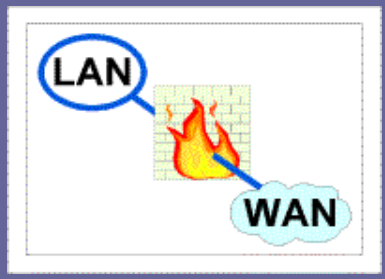
- Ein Beispiel für ein Zertifikat sehen Sie auf der nächsten Seite:

Sicherheitszertifikate

- Dieses Zertifikat wird von einem Netscape-Browser bemängelt.
- Es stammt von einer regulären Bank, doch ist offensichtlich das Rechenzentrum der Bank dem Browser unbekannt.
- Sie können nun das Zertifikat ablehnen, oder ihm einmalig oder dauerhaft vertrauen.

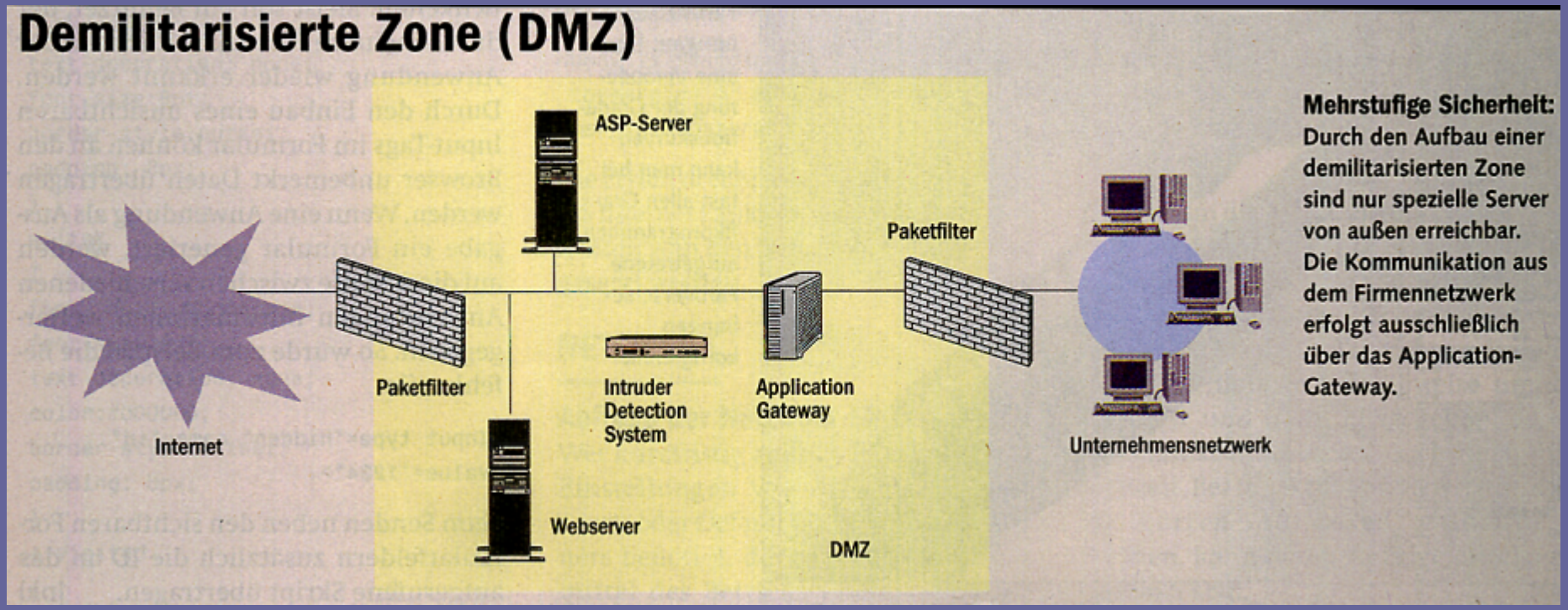
Schutz vor Fremden: die Firewall

- Zum Verbinden eines Büronetzes mit dem Internet wird auf einem speziellen Rechner eine „Firewall“ installiert.
- Dies ist eine spezielle Software, welche alle ein- und ausgehenden Datenpakete nach verschiedenen Mechanismen kontrolliert. Datenpakete, welche die Prüfung nicht bestehen, werden abgewiesen.
  - z.B. kann eine Firewall den Zugriff nur auf „erlaubte“ Internet-Seiten regeln
  - z.B. lässt eine Firewall nur eingehende Datenpakete passieren, die zuvor auch explizit angefordert wurden.
  - z.B. schließt eine Firewall unnötige offene TCP/IP-Ports



Demilitarisierte Zonen

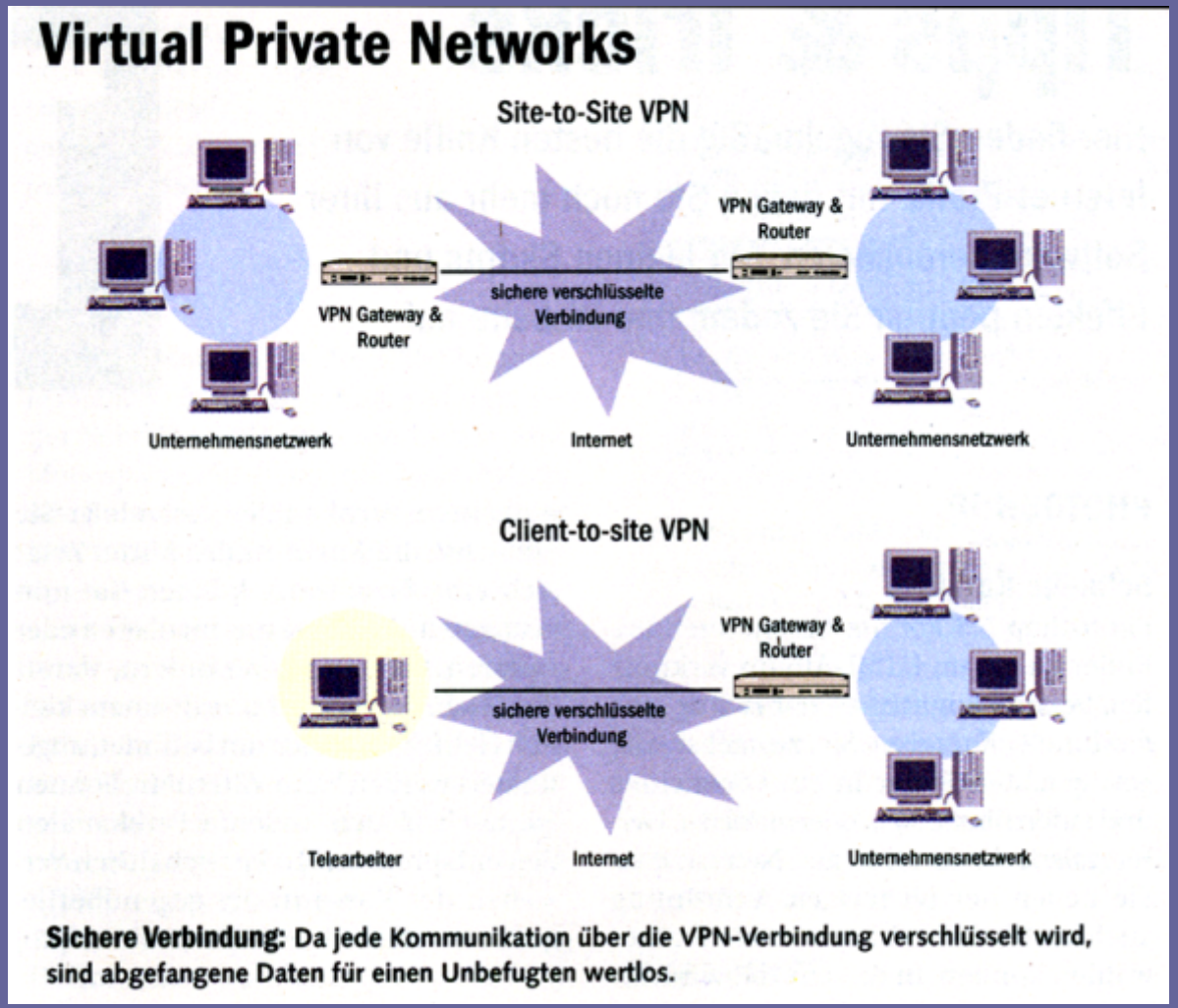
Wenn Sie öffentlichen Zugang zu Ihren Rechern benötigen (eigener Webserver), bietet sich eine Demilitarisierte Zone an. Dies ist quasi eine doppelte Firewall, innerhalb derer sich keine PCs mit gefährdeten Daten befinden.



VPN: Das virtuelle private Netzwerk

Wenn sich Außendienst-Mitarbeiter oder Heim-arbeiter ins Firmennetz einwählen müssen, z.B. per ISDN, dann bietet sich eine VPN-Lösung an.

Diese gewährleistet eine sichere verschlüsselte Point-To-Point-Verbindung zweier Rechner unter Nutzung der preiswerten öffentlichen Internet-Leitungen.



Entsorgung von Altgeräten und alten Datenträgern

- Betriebsmittel oder Sachmittel, die schützenswerte Daten enthalten (Druckerpapier, Disketten, Streamertapes, Magnetbänder, Festplatten, aber auch spezielle Tonerkassetten, Kohlepapier oder Carbonbänder) und nicht mehr gebraucht werden oder aufgrund eines Defektes ausgesondert werden sollen, sind so zu entsorgen, daß keine Rückschlüsse auf vorher gespeicherte Daten möglich sind.

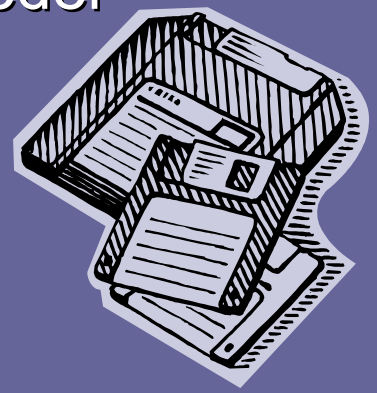
- **Bei funktionstüchtigen Datenträgern sollten die Daten physikalisch gelöscht werden**.
  - Es genügt nicht, eine Datei zu löschen oder eine Festplatte zu formatieren.
  - Dabei werden die Daten nicht wirklich gelöscht, sondern nur aus dem Inhaltsverzeichnis gelöscht. Mit speziellen Programmen kann man die Daten wieder herstellen.
  - Um Daten zuverlässig zu löschen, müssen die Dateien mit anderen Daten überschrieben werden.

- **Nicht funktionierende oder nur einmal beschreibbare Datenträger wie CD-ROMs müssen mechanisch zerstört werden**

Wie löscht man Disketten, Festplatten,... zuverlässig?

Disketten

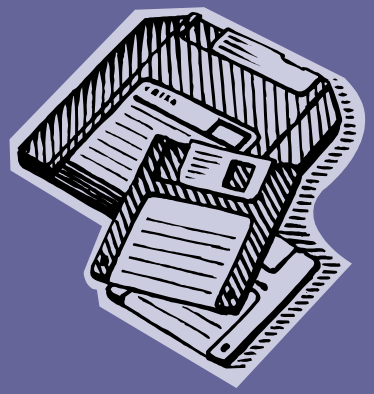
- Für mittlere Sicherheitsansprüche überschreiben Sie die Diskette mehrfach mit unterschiedlichen, nicht sicherheitsrelevanten Inhalten.
- oder nutzen Sie ein spezielles Programm.
- Die Funktionen „löschen“ oder „formatieren“ des Betriebssystems sind für vertrauliche Daten nicht zuverlässig genug. Man kann die Daten, z.T. sogar mit „Bordmitteln“ des Betriebssystems, wieder herstellen.
- Im Zweifelsfall zerstören Sie die Diskette.



Wie löscht man Disketten, Festplatten,... zuverlässig?

Festplatten

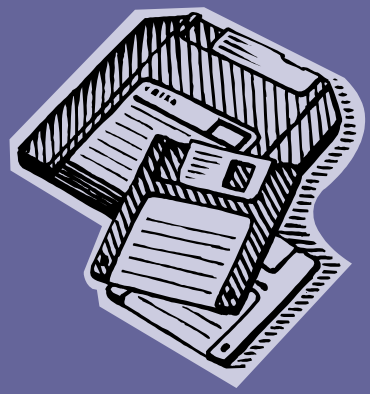
- Das „Formatieren“ einer Festplatte ist nicht ausreichend, um Daten komplett zu löschen. Die Formatierung kann mit speziellen Programmen wieder hergestellt werden.
- Nutzen Sie mindestens den „fdisk“-Befehl des Betriebssystems, um die Platte „low-level“ zu formatieren.
- Formatieren Sie die Platte anschließend und überschreiben Sie die Platte mit belanglosen Daten.



Wie löscht man Disketten, Festplatten,... zuverlässig?

Der beste Schutz

- Spezialisierte Programme zum Löschen von Daten nutzen
- Spezielle Löschgeräte benutzen, welche die Datenträger mit magnetischen Wechselfeldern durchfluten
- Achtung: Datenträger mit einer magnetischen Servospur, z.B. ZIP-Disketten, sind danach völlig unbrauchbar.
- Die mechanische Zerstörung ist der zuverlässigste Schutz, und bei nicht löschbaren Datenträgern (CD-ROMs) auch die einzige Möglichkeit.



Software-Empfehlungen für den privaten Gebrauch

- Für Firmennetzwerke gibt es eine Vielzahl von Produkten, die auf der Ebene der Hard- oder Software die Integrität der Daten und der Zugriffsrechte sicherstellen. Welche Produkte die geeigneten sind, wird man erst nach einer gründlichen Analyse der IT-Struktur feststellen und entscheiden können.

- Doch auch der Einzelplatz – PC oder der PC zu Hause kann leicht und preiswert geschützt werden.
- Einige bewährte und in der Branche allgemein als zuverlässig bekannte Produkte möchten wir Ihnen hier nennen, ohne Anspruch auf Vollständigkeit.

Software-Empfehlungen für den privaten Gebrauch

Gute Virenscanner

sind schon bei Preisen bis ca. 100,- DM erhältlich, z.B.

- Norton Antivirus (bei vielen PC-Händlern)
- McAfee Antivirus (bei vielen PC-Händlern, als kostenlose Testversion auf vielen Shareware-CD-ROMS)
- Neue Virensignaturen (den Impfstoff gegen neue Viren) laden diese Produkte regelmäßig aus dem Internet nach.

Software-Empfehlungen für den privaten Gebrauch

Auch eine einfache Firewall,

welche in der Lage ist, den Zugriff aus dem Internet auf Ihren PC, oder die Übermittlung von beispielsweise Kontodaten durch erfolgreich eingedrungene Trojaner ins Internet hinaus zu verhindern, können Sie installieren.

Nennen möchten wir hier:

- ZONEALARM (Internet: www.zonelabs.com, auf vielen Freeware-CD-ROMS, für den privaten Gebrauch kostenlos)
- NORTON PERSONAL FIREWALL (Internet: www.symantec.de, bei vielen PC-Händlern, ca. 100 DM).
- PGP Pretty Good Privacy, siehe nächste Seite

Software-Empfehlungen für den privaten Gebrauch

Datenschutz durch Verschlüsselung

gewährleistet

- **PGP Freeware**
  (Pretty Good Privacy, auf vielen Freeware-CD-ROMS, für privaten Gebrauch kostenlos).

In der aktuellen (9/2001) Version 7.0.3 leistet PGP:

- Generieren und Verteilen **asymmetrischer RSA-Schlüssel**. Bei ausreichender Schlüssellänge können diese gegenwärtig auch mit Großrechnern (Suoercomputer) nicht geknackt werden.
- **Schützt komplette Datenträger** wie Festplatten oder Disketten gegen unbefugten Zugriff (Laptops!)
- **Verschlüsselt E-Mails**, so daß nur der berechtigte Empfänger das Mail lesen kann.
- **Elektronisches Unterschreiben von E-Mails und Dokumenten** (Echtheit wird gewährleistet)
- **PGP integriert sich dafür in die gängigen Mail-Anwendungen** (Outlook, Netscape usw.), was eine bequeme Handhabung möglich macht.

Software-Empfehlungen für den privaten Gebrauch

PGP 7.03 leistet weiterhin:

- Sicheres Löschen von Dateien durch mehrfaches Überschreiben
- Firewall-Funktionalität
- Intrusion Detection System: Erkennung und Abblocken von Hackern, welche die Firewall überwunden haben
- VPN: Unterstützung von virtuellen privaten Netzwerken für sichere Point-to-Point-Verbindungen über das öffentliche Internet

Umfassende Informationen

Bundesamt für Sicherheit in der Informationstechnik

Online im Internet: **http://www.bsi.de** Hier finden Sie aktuelle Informationen direkt im Internet.

Offline: Das BSI verteilt kostenlos CD-ROMs zum IT-Grundschutz. Hier finden sich neben der aktuellen deutschen Version des **IT-Grundschutzhandbuchs** auch die englische Übersetzung, die HTML-Version des Handbuchs sowie weitere Informationen des BSI.

Diese BSI-CD-ROMs können gegen Einsendung eines ausreichend frankierten Rückumschlags (Format C5, 3,- DM) an das BSI, IT-GSHB, Postfach 20 03 63, 53133 Bonn bezogen werden.

Aktuelle Informationen

IT-Grundschutzhandbuch

Dieses wird als Loseblatt-Sammlung vom Bundesanzeiger-Verlag vertrieben.

ISBN 3-88784-915-9

Bestelladresse:

Bundesanzeiger-Verlag
Postfach 100534
50455 Köln
Tel.: (0221) 97668-200
Fax: (0221) 97668-278
E-Mail: bestellungen@bundesanzeiger.de