Sicher surfen im Internet

Eine persönliche Anleitung
(Stand 2004)

Vorwort des Autors

Ein grosser Teil der Bevölkerung verwendet heute regelmässig einen PC und das Internet. Aber nur wenige Anwender sind sich der Sicherheitsrisiken bewusst.

Mit diesem kleinen Werk möchte ich Hinweise und Tipps geben, um den Umgang mit dem Internet sicherer zu machen.

Aber vielleicht war Ihnen bisher gar nicht so recht bewusst, was alles möglich ist, wenn Sie sich im Internet anmelden? Würden Sie Ihre persönlichen Briefe und Dokumente jeder Person auf dieser Welt offen präsentieren? Nein? Wieso gibt es dann so viele Menschen, die dies gerade durch den eigenen PC via Internetanschluss tun?

Wenn Sie diese Tipps gelesen haben, dann werden Sie für viele Dinge sensibilisiert sein.

Das Internet bietet unglaublich viele Möglichkeiten. Es beinhaltet aber auch erhebliche Gefahren. Viele dieser Gefahren lassen sich mit einfachen Mitteln entschärfen oder gänzlich eliminieren.

Kommen Sie mit und machen auch Sie sich Gedanken zu Ihrer Sicherheit beim Umgang mit PC und Internet.

Inhaltsverzeichnis

1 Das Internet

Um es vorweg zu nehmen:

„Es gibt keine absolute Sicherheit im Internet.“ Dan D.

Aber es gibt einige Massnahmen, mit denen das Risiko minimiert werden kann. Dieses Dokument richtet sich nicht an Profis und Netzwerkbetreiber. Es ist für den Heimanwender gedacht.

Viele Tipps sind deshalb einfach gehalten, aber trotzdem sehr wirkungsvoll.

Wichtig ist, dass Sie sich immer im Klaren darüber sind, dass das Internet eine öffentliche Institution ist. Im Internet gibt es keine wirkliche Privatsphäre.

„Stellen Sie sich einfach vor, Sie stünden in einem grossen Saal auf der Bühne und alle würden via Beamer zusehen, wie Sie am Rechner arbeiten und alle würden sehen, was Sie gerade auf dem Rechner und im Internet machen.“ Zitat A. H.

Nur so surfen Sie, ohne dass es peinlich, gefährlich oder gar strafbar wird. Beherzigen Sie diesen Grundsatz. Irgend jemand sieht Ihnen dauernd über die Schultern!

Deshalb hier meine persönlichen Tipps (ohne Anspruch auf Vollständigkeit, absolute Korrektheit sowie mit vollständigem Rechts- und Haftungsausschluss):

2 Der Computer

Es gibt bezüglich Internet nur eine wirklich sichere Lösung:

Verwenden Sie für das Internet einen separaten Rechner.

Hiefür genügt ein alter/älterer Rechner vollkommen. Diese Rechner werden in vielen Firmen bei Umstellungen auf neue Systeme entsorgt. Auch über Kollegen oder Bekannte sind oft ältere PC in funktionstüchtigem Zustand zu einem kleinen Preis oder gratis erhältlich.

Natürlich könne Sie auch an einer Börse oder einer Auktion im Internet einen geeigneten PC erwerben. Ein weiterer guter Tipp sind die Alteisensammelstellen der Gemeinden. Hier werden oft PC's abgegeben die den gehobenen Anforderungen nicht mehr genügen, aber noch gut für das Internet zu gebrauchen sind. Ebenso werden solche PC's bei Händlern zurück gegeben, z.B. beim Kauf eines neuen Rechners. Auch dies ist eine Möglichkeit um an einen günstigen PC für's Internet zu kommen.

Wer etwas mehr ausgeben möchte, der kann einen einfachen PC verwenden. Für das Internet benötigen Sie weder einen CD-Brenner, noch ein DVD-Laufwerk. Auch ein Diskettenlaufwerk ist nicht erforderlich. Es genügt ein einfaches CD Laufwerk für die Installation des Betriebssystems oder allfälliger Programme. Auch bei den RAM oder der Rechnergeschwindigkeit genügen Auslaufmodelle noch Lange.

Zudem ist beim Surfen selten eine grosse Harddisk erforderlich. Es sei denn, Sie laden häufig Dateien vom Internet herunter. Dann kann eine etwas grössere Harddisk von Nutzen sein. Aber Speicherplatz kostet heute nicht mehr viel Geld.

Zwei PC's lassen sich übrigens mittels eines Umschalters über den gleichen Monitor, die gleiche Tastatur und die gleiche Maus bedienen. So können Sie an beiden PC's arbeiten oder im Internet etwas downloaden und gleichzeitig am Arbeitsrechner einen Brief schreiben.

Deshalb mein Tipp:

Ein separater Rechner ist eine der besten Lösungen für den Zugriff auf's Internet. Aber auch ein separater Rechner muss zusätzlich geschützt werden!

3 Das Betriebssystem

„Wenn Sie keinen zweiten Computer verwenden wollen, dann verwenden Sie am besten Knoppix zum surfen.“

Verwenden Sie allgemein möglichst Linux (oder Mac) anstelle von Windows um im Internet zu surfen.

Für Linux gibt es ganze Distributionen als Gratissoftware. Knoppix ist da nur ein Beispiel. Auch eine einfache, kommerzielle Distribution kann verwendet werden. Oft werden Distributionen auch zusammen mit einem Einführungsbuch (z.B. bei Knoppix) angeboten. Ebenso gibt es Angebote in Computerzeitschriften.

Die aktuelle Version von Knoppix kann vom Internet heruntergeladen werden (700 MB) oder kann zusammen mit einem Buch für ca. Fr. 25.-- (Preis 2004) im Laden gekauft werden. Die SUSE Heimanwenderdistribution ist für ca. Fr. 60.-- (Preis 2004) erhältlich und in Onlineauktionen werden etwas ältere Distributionen für ein paar Franken angeboten. Die SUSE Heimanwenderdistribution gibt es ebenfalls auf einer von CD startenden Version.

Knoppix hat übrigens einen sehr wesentlichen, grossen Vorteil. Es installiert sich nicht auf der Festplatte sondern startet direkt von der CD und ist trotzdem voll lauffähig. Es speichert auch keine Daten auf der Festplatte, ausser Sie genehmigen es ausdrücklich. Die persönlichen Einstellungen müssen allerdings separat gespeichert werden, ansonsten gehen diese verloren beim Herunterfahren von Knoppix. Trotzdem ist Knoppix eine sehr gute Alternative. Natürlich kann Knoppix auch auf dem PC installiert werden.

Auch von SUSE und Mandrake gibt es direkt ab CD lauffähige Versionen.

Ebenso ist Macintosh eine gute Alternative. Auch hier gibt es kaum Viren und so kann mit einem Mac problemlos im Internet gesurft werden.

Es bleibt aber zu vermuten, dass bei grösserer Verbreitung auch die Zahl der Viren für Linux und Mac zunehmen wird. Trotzdem sind beide Betriebssysteme eine echte Alternative zu Windows.

Beide Betriebssysteme (Linux wie Mac) haben noch einen weiteren Vorteil. Beide stellen weniger hohe Ansprüche an die Hardware und laufen deshalb auch auf „älteren“ PC’s gut und flüssig.

Wenn es unbedingt Windows sein muss, dann genügt eine ältere Version. Auch mit dieser lässt sich problemlos auf einem Zweitrechner im Internet surfen. Sie sollten darauf achten, dass beim Gebrauchtkauf eines älteren Rechners für das Internet das Betriebssystem enthalten ist und die Lizenz-CD zum PC mitgeliefert wird.

Passiert dann einmal etwas, so können Sie das Betriebssystem neu installieren. Auch Intern lässt sich ein System mit einem einfachen kleinen Trick zusätzlich schützen…

4 Das Internetuserprofil

Der kleine Trick besteht darin, einen Internetuser anzulegen. Jedes moderne Betriebssystem bietet die Möglichkeit eines Multiuserbetriebes.

Richten Sie deshalb einen Internetbenutzer mit eingeschränkten Rechten ein. Damit können Sie den Schaden bei einem Virenbefall zusätzlich vermindern.

Gleichzeitig erhöht dies die Sicherheit des ganzen Systems. Besonders dann, wenn Sie nicht so geübt im Umgang mit einem PC sind. Das eingeschränkte Userprofil vermindert die Möglichkeiten für betriebsgefährdende Aktionen erheblich bis gänzlich.

Mit dem Administrator sollten Sie sich auf dem System nur anmelden, wenn Sie auch wirklich eine Systemwartung durchführen und wissen, was Sie mit den jeweiligen Aktionen im System bewirken. In Windows müssen die zusätzlichen Benutzer eingerichtet werden. In Linux ist die Einrichtung des eigenen Users eine Pflicht. Dies ist mit ein Grund, weshalb Linuxsysteme weit weniger gefährdet sind.

Natürlich bleibt eine Firewall und ein Virusscanner trotzdem ein absolutes Muss.

5 Ohne Firewall kein Internet

Eigentlich sollten es alle längst gehört haben und wissen:

Eine Firewall gehört in jedem Fall auf den Internetrechner, unabhängig vom Betriebssystem.

In vielen Linuxdistributionen ist die Firewall bei der Installation schon standardmässig enthalten.

Für Windows gibt es genügend geeignete Firewalls. Teilweise dürfen diese durch Private gratis verwendet werden. Andere Firewalls sind zwar kostenpflichtig, bieten aber häufig auch einen grösseren Funktionsumfang.

Der Preis für eine Firewall ist zu verschmerzen und oft werden diese zusammen mit einem Virenscanner im Paket angeboten. Nur eine Firewall garantiert, dass weder von Aussen, noch von innen ein Programm unbefugt auf das Internet zugreift.

Dabei ist das Funktionsprinzip einer Firewall ganz einfach (grobe Kurzbeschreibung):

Eine Firewall kontrolliert die ein- und ausgehenden Datenströme.

Gleichzeitig wird auch geprüft, ob irgendjemand von aussen auf das System zugreifen will oder ob Programme von sich aus auf das Internet zugreifen wollen. Dabei erfolgt die Zustellung der Daten über sog. Ports. Genau diese Ports werden von der Firewall auf den gesamten ein- und ausgehenden Datenstrom überwacht. Auch kann die Firewall so eingestellt werden, dass die Daten nur von und an eine bestimmte Adresse über einen bestimmten Port übertragen werden können. Wenn Sie die Firewall installiert haben, dann kann es gut sein, dass Sie sehr überrascht sind, welche Programme alle von sich aus auf das Internet zugreifen wollen. Unterbinden Sie dies.

Es ist auch vernünftig, die Firewall „scharf“ einzustellen. Je besser und schärfer die Firewall eingestellt ist, desto sicherer ist das System. Natürlich kann eine Firewall auch so eingestellt werden, dass das Arbeiten mühsam oder gar unmöglich wird. Hier ist eine optimale Einstellung anzustreben. Wer sich mit der Materie nicht befassen will, der sollte die Grundeinstellungen verwenden. Viele Firewalls sind mit einer guten Grundeinstellung vorkonfiguriert.

Die Grundeinstellung darf in keinem Fall nicht nach unten verändert werden. Dies würde den Schutz verwässern oder gar aufheben. Die vorkonfigurierte Firewall bietet in vielen Fällen einen sinnvollen bzw. guten Schutz.

Sollten Sie einmal nicht sicher sein, ob Sie eine Aktion zulassen dürfen oder nicht, so sollten Sie immer das Blockieren wählen.

Zukünftig kann davon ausgegangen werden, dass ein Betriebssystem direkt eine Firewall integriert haben wird. Erste Ansätze sind bei Windows ja bereits vorhanden (Stand 2004).

Trotzdem, auch wenn Sie die Firewall installiert haben, dann ist ein Virenscanner ebenfalls weiterhin ein Muss.

6 Ein Virenscanner

Ein Viruserkennungsprogramm gehört auf jeden Internetrechner mit einem Windows Betriebssystem.

Bei Linux und Mac ist dies weit wesentlich weniger kritisch. Es gibt zwar auch ein paar Viren für Linux. Die Anzahl und Gefährlichkeit hält sich aber bisher in Grenzen (Stand 2004).

Bezüglich Mac verhält es sich gleich. Auch hier gibt es kaum Viren (Stand 2004).

Der Grund ist eigentlich ganz einfach. Viele Entwickler haben nicht sonderlich viel Freude daran, dass Microsoft eine derart grosse Monopolstellung am Markt hat. Auch hat Microsoft in den letzten Jahren mit immer neuen Betriebssystemen mehr Benutzer verärgert als hinzugewonnen. Dies rechtfertigt in keiner Weise das Schreiben und in Verkehr bringen von Viren. Es erklärt aber den Ärger vieler Anwender und insbesondere vieler Freaks und Programmierer.

Die Installation eines Virenscanners in Windows ist meist einfach und unkompliziert. Oft wird dieser auch gleich zusammen mit der Firewall installiert. Natürlich entspricht die installierte Version dem Stand der Produktion der CD. Deshalb ist es unbedingt notwendig, ein Update durchzuführen.

Nach der Installation des Virenscanners sollten Sie deshalb das System zuerst auf Viren scannen. Danach ist ein Update der Virensignatur notwendig. Schliesslich muss das gesamte System unbedingt nochmals auf Viren gescannt werden.

Ein automatisches Update der Virensignatur ist mindestens wöchentlich, besser täglich durchzuführen. Der Updatezyklus hängt von der Häufigkeit der Benutzung des Internets ab. Updaten Sie die Signatur immer dann sofort, wenn wieder einmal ein Virus viele Rechner befallen hat.

Die Virensignatur ist ein Verzeichnis der Viren und deren Erkennungsmuster. Da täglich neue Viren hinzukommen, wird dieses Verzeichnis regelmässig ergänzt. Und genau das machen Sie mit dem Update der Virensignatur auch auf Ihrem PC. Sie ergänzen das Verzeichnis mit den neuesten Angaben.

Es werden übrigens auch Online-Virusscanner angeboten mit denen das eigene System ab und zu gescannt werden kann. Dabei werden der Firma, welche die Daten scannt, natürlich auch persönliche Daten übermittelt. Seien Sie deshalb mit dieser Variante vorsichtig. Wenn Sie aber keinen Virenscanner haben und der Ansicht sind, dass Ihr System infiziert sein könnte, so kann dies ein Weg sein, die Infektion des Systems so schnell als möglich zu finden und zu bestimmen, welcher Virus es ist.

Es gibt aber auch noch weitere Möglichkeiten, ein System auf die Sicherheit zu prüfen…

7 Test des Systems auf Sicherheit

Die Sicherheit eines Systems zu testen ist ebenfalls möglich. Auf einigen Seiten von Firewall- und Virensoftwareanbietern kann das System auf Lücken getestet werden.

Am Schluss des Tests erhalten Sie einen Bericht. Diesen sollten sie genau studieren und allfällige Lücken schliessen.

Wenn Sie damit Schwierigkeiten haben, dann hilft Ihnen sicherlich ein Bekannter/eine Bekannte oder der/die Superuser/in bzw. IT-Verantwortliche ihrer Firma weiter.

Wichtig ist: Nehmen Sie Sicherheitslücken nicht auf die „leichte Schulter“. Das kann unangenehme Folgen haben. Schliessen Sie erkannte Sicherheitslücken.

Ein regelmässig gewartetes System ist Voraussetzung für das sichere Surfen im Internet.

Nun wollen wir uns den eigentlichen Anwendungen widmen.

8 Datentransfer zwischen den Computern

Wenn Sie meinen Rat beherzigt haben und zwei Computer verwenden, dann ist es immer wieder notwendig, dass Daten vom Internetrechner auf den normalen Arbeitsrechner verschoben werden müssen.

Vor einem Datentransfer vom Internetrechner auf den normalen Arbeitsrechner müssen die zu übertragenden Dateien deshalb IMMER auf Viren gescannt werden.

Verwenden Sie deshalb für den Datentransfer KEINE Direktverbindung mit dem Internetrechner wie z.B. Kabel, Bluetooth, Wireless-Lan usw.

Verwenden Sie einen Datenträger für den Transfer wie z.B. einen Speicherstift, eine Speicherkarte, evtl. eine CD oder besser eine CD-RW, evtl. Disketten, oder eine externe Harddisk.

Ich persönlich verwende hierfür einen Speicherstift. Diese sind heute günstig erhältlich und bieten eine beachtliche Speicherkapazität auf kleinem Raum. Auch sind diese für den Datentransfer auf andere Rechner geeignet.

Gehen Sie für den Datentransfer folgendermassen vor:

- Verschieben Sie alle zu übertragenden Daten auf den Datenträger (z.B. Speicherstift)
- Vergewissern Sie sich, ob der Virenscanner auf dem neuesten Update ist
- Scannen Sie den gesamten Datenträger (z.B. Speicherstift) auf Viren

Findet der Virenscanner keinen Virus, so können Sie die Daten vom Speicherstift auf den Arbeitsrechner verschieben.

Es gibt zwar auch mit dieser Methode keine 100%-ige Sicherheit. Aber bisher habe ich unter Einhaltung aller hier beschriebenen Sicherheitsmassnahmen noch nie einen Virus auf meinem Arbeitsrechner festgestellt.

Diese Methode hat übrigens noch einen weiteren Vorteil. Wenn versehentlich einmal ein Trojaner auf den Arbeitsrechner gelangt, so kann er zwar das System ausspionieren. Der Trojaner kann aber die gesammelten Daten nicht zurücksenden, da der Arbeitsrechner nicht mit dem Internet verbunden ist.

Zudem gilt bei Daten und Programmen von Freunden und Bekannten:

Vorsicht beim Übertragen oder Installieren von Daten und Programmen auf den Arbeitsrechner.

Wenn Sie einen Datenträger von einem Freund oder einem Bekannten erhalten, so scannen Sie diesen IMMER zuerst auf Viren! Übertragen Sie erst danach die Daten oder Programme auf den Internet- oder Arbeitsrechner.

Nun wollen wir uns noch dem eigentlichen Surfen im Internet zuwenden…

9 Das Surfprogramm

Natürlich benötigen Sie für das Surfen ein entsprechendes Programm. Aber welches?

Hier sollten Sie auf keinen Fall den Internet Explorer verwenden. Der Internet Explorer hat einfach noch zu viele Sicherheitslücken. Auch ist es schwierig, den Internet Explorer ohne Grundkenntnisse so zu konfigurieren, dass er einigermassen sicher ist und es sich gleichzeitig noch halbwegs komfortabel surfen lässt.

Es gibt genügend gute Alternativen wie Firefox, Mozilla, Netscape usw. Diese sind erst noch gratis und bieten teilweise wesentlich mehr Funktionsumfang.

Ich persönlich verwende Firefox. Das Programm ist klein, schnell und bietet eine Menge an Einstellmöglichkeiten die ich im Internet Explorer vergeblich suche. Auch sind viele Schutzfunktionen integriert. So ist ein Pop Up Blocker als Standard integriert und muss nicht mittels Update aufgespielt werden. Ebenso wie die Möglichkeit, die Chronik, die Formulardaten, die Passwörter, den Download Manager, das Cache und den Verlauf separat löschen zu können. Auch können die Cookies direkt und einfach verwaltet werden.

Es kann einzig sein, dass einige Funktionen im Internet nicht laufen. In einigen Fällen ist es deshalb notwendig, trotzdem den Internet-Explorer für bestimmte Seiten zu verwenden. Ich halte es persönlich allerdings anders. Wenn ein Anbieter es nicht fertig bringt, seine Internetseite so auf zu bauen, dass diese auf jedem gängigen Browser vernünftig angezeigt werden kann, dann kann ich auf diese Firma verzichten!

Ich halte mich deshalb an meine Regel: „Wenn die Seite im Firefox nicht richtig angezeigt wird, so lasse ich die Firma oder den Inhaber der Seite links liegen.“ Damit bin ich bisher gut gefahren.

Wenn da nicht diese lästige Werbung wäre…

10 Lästige Pop-Up's und Werbung

Pop-Up's und Werbung sind eine lästige Sache. Wenn die Firewall diese nicht blockiert und auch der Browser diese nicht filtert, so gibt es eine andere Hilfe.

Hier hilft der Web Washer.

Dieser ist für Privatanwender ohne Kosten nutzbar und filtert die lästige Werbung heraus. Gleichzeitig kann ein Blocker aktiviert werden, der die aufgehenden Werbefenster blockiert.

Falls eine Seite einmal nicht richtig angezeigt wird, so kann der Web-Washer einfach abgeschaltet werden und die Seite muss nur neu geladen werden. Einen Teil der Web-Washer Funktionen finden Sie auch im Firefoxbrowser als Standard.

Eine Besonderheit des Web-Washers ist das Herausfiltern von Werbung bzw. von Werbebannern. Auf jeder der Internetseite werden tatsächlich die Werbebanner nicht angezeigt. Das klappt fast immer ausgezeichnet.

Der Web-Washer wurde übrigens deshalb entwickelt, weilt das Laden der lästigen Werbebanner viel Zeit benötigte bei den früheren analogen Verbindungen via Telefonleitung. Auch möchte ich nicht die lästigen Werbungen lesen auf einer Seite, sondern die gesuchten Informationen. Ein lustige Spielerei des Web-Washers ist es auch, die Werbung durch ein anderes Bild zu ersetzen. Es ist immer wieder erstaunlich, wie viele Male das gleiche Bild auf einer Seite erscheinen kann. Alles nur Werbebanner.

Wichtig ist bei den Einstellungen des Web-Washers nur, dass Sie nur ein Häkchen bei Skripte beim schliessen ausführen machen. Wenn Sie ein Häkchen bei Skript beim Aufrufen einer Seite machen, so werden fast alle Seiten nicht richtig angezeigt. Ansonsten können Sie selber wählen, welche Optionen aktiviert werden sollen.

Noch einen grossen Vorteil hat der Web-Washer. Er läuft bei richtiger Konfiguration mit jedem Browser. Also, auch wenn Sie einmal auf den Internet Explorer wechseln, so arbeitet der Web-Washer noch immer genau gleich gut. Er sollte allerdings zusammen mit dem System automatisch gestartet werden.

11 E-Mail, Mailprogramm, Mailadressen

E-Mailverkehr ist heute schon fast ein Muss für jeden PC-Anwender. Leider ist der E-Mailverkehr aber auch das grosse Leck und der einfachste Ort für das Eindringen und Verbreiten von Viren, Trojanern und anderen Unannehmlichkeiten.

Aber auch hier lässt sicht einige machen. Wie auch beim Explorer (also dem Surfprogramm) ist das Programm von Microsoft alles andere wie sicherheitstechnisch unbedenklich. Deshalb empfehle ich eine alternative zu verwenden.

Es gibt gute Alternativen zu Outlook. Ich verwende hier für die allgemeine E-Mailadresse den Thunderbird von Mozilla.

Daneben verwende ich für meine persönliche private E-Mailadresse einen anderes E-Mailprogramm.

Dies hat den Vorteil, dass ich die allgemeine E-Mailadresse immer mit demselben Mailprogramm bearbeite und dieses auf genau die Erfordernisse der allgemeinen Internetadresse einstellen kann.

Bei den E-Mails kann natürlich viel „falsch“ gemacht werden. Ich empfehle nebst einem gesonderten E-Mailprogramm noch folgendes:

Sie sollten mindestens 2 E-Mailadressen verwenden, besser 3 E-Mailadressen.
Es sind dies:

- eine allgemeine E-Mailadresse für Anfragen, Umfragen (völlig öffentlich)
- eine halbprivate E-Mailadresse für Kollegen, persönliche Anfragen die Ihnen vertrauenswürdig erscheinen
- eine private E-Mailadresse für ganz persönliche Mails

Verwenden Sie die nichts aussagende, allgemeine E-Mailadresse für Anfragen, Umfragen oder wenn Sie eine Adresse im Internet hinterlassen müssen. Dabei sollte diese nur wenig auf den Namen hinweisen und mehr der Fantasie entspringen.

Verwenden Sie die **halbprivate E-Mailadresse** für vertrauenswürdige Personen und Firmen (z.B. Reisebüro, Bestellungen, Publikationen usw. usw.). Diese E-Mails können Sie, je nach Provider, auf die persönliche Mailadresse umleiten. So müssen Sie nur zwei Mailzugriffe verwalten.

Ein weiteres echtes Übel ist Spam. Dagegen gibt es zwei Möglichkeiten:

- Entweder Sie filtern die Mails
- oder der E-Mailanbieter filtert die Mails

Ich schlage Ihnen vor:
Wählen Sie für die allgemeine, öffentliche E-Mailadresse einen Anbieter mit einem Spamfilter.

Es ist einfacher, einen Anbieter zu wählen, bei welchem ein Spamfilter gleich eingeschlossen ist. Natürlich können Sie auch einen eigenen Spamfilter installieren auf dem PC und diesen Konfigurieren. Dies hat den Vorteil, dass Sie bestimmen, welche Mails gefiltert werden und welche nicht. Oftmals ist dies auch in den Kosten günstiger, da sich eine Anbieter diesen Service mit einer monatlichen Gebühr bezahlen lassen. Da ist schnell einmal

auf der Betrag für ein Spamprogramm angehäuft. Einige Firewalls oder Virenprogramme bieten zudem im Packet gleich noch ein Spamfilter an. Dies ist meist die kostengünstigste Variante.

Zum Abrufen der E-Mails sollten Sie unterscheiden zwischen allgemeiner Adresse und privater E-Mailadresse.

Verwenden Sie für den privaten E-Mailverkehr ausschliesslich eine verschlüsselte Verbindung und ein sicheres Passwort.

Dies verhindert zwar nicht, dass die E-Mails von unbefugten Personen oder von Geheimdiensten/Staatsstellen gelesen werden können. Aber Sie können so recht gut verhindern, dass jemand anderes direkt ihren E-Mailverkehr und das Postfach manipuliert.

Geben Sie die **persönliche Mailadresse nur an sehr gute Freunde und Bekannte** weiter und beharren Sie darauf, dass diese nicht weitergegeben wird. Geben Sie auch immer die allgemeine Mailadresse bekannt die weitergegeben werden darf.

Wenn Sie ein Mail auf Ihren Rechner heruntergeladen haben, dann müssen Sie folgendes beachten:

- **Öffnen Sie keine Mails und Mailanhänge von unbekannten Absendern bevor Sie diese nicht auf Viren gescannt haben**
- **Speichern Sie Mailanhänge auf dem PC und scannen Sie diese immer vor dem öffnen**
- **Versenden Sie keine persönlichen Daten via Mail**
- **Verraten Sie niemals persönliche Daten am Telefon (Passwort usw.)**
- **Verraten Sie niemals persönliche Daten auf eine Anfrage hin**
- **Folgen Sie niemals einem Link in einem Mail**
- **Bestätigen Sie niemals die Installation von irgendwelchen Programmen, Skripten oder anderen Anwendungen**

Bei E-Mail gibt es noch etwas, das vermutlich viele nicht wissen (!):

E-Mails sind nicht privat und können (theoretisch) von jedermann gelesen werden auf dem Weg vom Absender zum Empfänger.

E-Mails werden von Geheimdiensten auf bestimmte Begriffe gescannt und im Verdachtsfalle wird eine Kopie archiviert und näher durchleuchtet.

In Deutschland werden alle E-Mails über 2 Server geleitet und automatisch gescannt. Fällt ein E-Mail wegen eines bestimmten Inhaltes auf, so wird eine Kopie zurück gehalten und durch Mitarbeiter analysiert (gelesen).

Wer wirklich private Post per E-Mail zu versenden hat, der sollte seine Nachricht in ein Textdokument verpacken und dieses verschlüsseln. Hier gibt es heute sehr gute und teilweise kostenfreie Verschlüsselungssoftware.

Als Beispiel möchte ich PGP anführen. PGP ist in älteren Versionen frei verwendbar. Es gibt auch einen Freeware-Nachfolger von PGP. Dieses Programm ist eine sehr gute, frei verwendbare Software mit einem privaten und öffentlichen Schlüssel. Sie verursacht keine Kosten und gilt als extrem sicher.

Ansonsten verwenden Sie besser den Postweg oder das Telefon für wirklich vertrauliche und private Mitteilungen.

12 Dialer

Es gibt ein paar Sauereien im Internet. Eine der übelsten Abzocken sind Dialer. Einzig bei Verbindungen via Fernsehkabel sind diese Dialer kein sonderlich grosses Problem, da ja keine Internetverbindung via Telefon erfolgt. Beim Dialer handelt es sich um ein Programm, dass die Einwahlnummer des Modems ändert. Sie telefonieren plötzlich nicht mehr über eine Ortsnummer, sondern über eine teure 0190-er Nummer. Das kann locker Fr. 2.-- pro Minute kosten. Also Fr. 120.-- und mehr pro Stunde.

Aktivieren Sie in jedem Fall das 0190 Sperrset für Ihren Telefonanschluss.

Es ist auch sehr gut, zusätzlich einen 0190-Warner zu installieren. Nebst vielen Warnprogrammen bietet auch die Swisscom einen solchen zum Download auf der Swisscom-Homepage an.

Ich kann hier nur immer wieder das Beispiel eines Kollegen von mir aufführen. Er suchte nach einer Firma, die Visitenkarten herstellt (also nicht nach irgendwelchen Sexseiten!). Er wurde schliesslich nach einigem Suchen fündig. Gleichzeitig geriet er aber auch auf eine Seite, bei der er einen Dialer aktivierte. Und das bei der harmlosen Suche nach einem Anbieter, der Visitenkarten druckt!
Dieser veränderte die Zugangsnummer für das Internet auf eine kostenpflichtige Nummer und Ende Monat war die Überraschung mit einer Rechnung von über Fr. 450.-- für den Telefonanschluss perfekt.

Zwar ist dies nicht zulässig, aber ein nachfolgender Rechtsstreit kostet viel Geduld, Nerven, Zeit und Geld. Deshalb ist ein Dialerschutz ebenfalls ein Muss.

13 Passwörter

Es ist schon ein echtes Übel. Passwörter werden langsam aber sicher zu einer echten Anforderung. An vielen Orten müssen wir uns mit einem Passwort identifizieren. Sei dies im Geschäft (meist gleich mehrmals), am Bancomaten, mit der Benzinkarte, am heimischen PC, beim Zugriff auf das E-Mailkonto, bei der Anmeldung am heimischen PC usw. Dabei werden die meisten Benutzer darauf hingewiesen, dass die geschäftlich genutzten Passwörter nicht privat verwendet werden dürfen. Dies ist absolut korrekt und muss auch unbedingt eingehalten werden, auch wenn der Arbeitgeber dies nicht unbedingt fordert.

Der Ärger ist nun, dass für die vielen Anwendungen auf keinen Fall das gleiche private Passwort verwendet werden sollte. Auch sollte dieses regelmässig geändert werden. Denn nebst guten Passwörtern gibt es leider auch Hackprogramme für Passwörter. Diese Hackprogramme sind ziemlich erfolgreich und können einfache Passwörter relativ schnell und mühelos herausfinden. Es ist deshalb notwendig, für die Anwendungen **verschiedene und sichere Passwörter** zu verwenden.

Verwenden Sie deshalb nur sichere Passwörter. Speichern Sie diese nicht auf dem Internetrechner.

Nur was ist ein sicheres Passwort?

Hierfür gibt es Anleitungen im Internet. Grundsätzlich besteht ein sicheres Passwort aus mindestens 6 Zeichen. Es sollten immer Grossbuchstaben, Zahlen, Sonderzeichen und Kleinbuchstaben enthalten sein. Dabei soll das Passwort keinen bekannten Begriff darstellen. Hier ein paar einfache Beispiele: Kp4G+t I?qCp8 U9eY%G usw. usw. usw.

Nun dürften solche Passworte nur schwerlich zu merken sein. Deshalb empfiehlt es sich, einen Passwortsafe zu verwenden. In einem solchen Programm können die Passwörter mit den entsprechenden Angaben abgelegt werden. Gleichzeitig mit der Speicherung werden die Daten verschlüsselt auf der Festplatte gespeichert. Danach muss ich mir nur noch ein Passwort merken, nämlich dasjenige für das Passwortsafe. Dass der Passwortsafe nur auf dem Arbeitsrechner installiert werden darf, dürfte sich von selbst verstehen.

Wer bereit ist, Fr. 30.-- bis Fr. 50.-- aus zu legen, der kann auch eine Verschlüsselungssoftware erwerben. Für Linux gibt es solche Programme gratis. Diese erzeugt ein verschlüsseltes Laufwerk auf dem Harddisk. Dieses kann dann nur mit einem Passwort geöffnet werden. Diese Methode hat den grossen Vorteil, dass nicht nur die Passwörter sicher abgelegt werden können. Auch alle sehr persönlichen Dokumente und Dateien können hier abgelegt werden. Damit hat kein anderer als Sie selbst Zugriff auf die Dateien und Passwörter. Die Passwörter können Sie dann einfach in einem Word- Excel- oder Textdokument auf dem verschlüsselten Laufwerk speichern.

Dieses System hat natürlich auch Nachteile. Denn wer unterwegs auf seine Passwörter zugreifen muss, der hat diese natürlich nicht dabei. Kommen Sie nun auf **keinen Fall** auf die Idee, die Passwörter auf zu schreiben! Hierfür gibt es heute bessere Möglichkeiten.

Eine weitere, gute Möglichkeit ist ein Verschlüsselungsprogramm, mit welchem ein portabler Safe hergestellt werden kann. Darin können dann die Passwörter abgelegt werden. Auch kann der Passwortsafe auf einem Speicherstick installiert werden. Auch damit lässt sich unterwegs darauf zugreifen. Diese Funktion eines portablen Safes für die Daten ist in einigen Laufwerkverschlüsselungsprogrammen inbegriffen (z.B. in Steganos).

Nur, wer hat schon immer einen Laptop dabei?

Aber heute gibt es ja diese topmodernen Organizer. Ausser den extrem billigen Modellen haben diese Organizer jeweils einen passwortgeschützten Bereich. In diesem lassen sich die Passwörter problemlos ablegen. Bei einigen Modellen kann auch das Passwortsafeprogamm installiert werden.

Für die Verwaltung der Termine und der Passwörter benötigen Sie aber kein Topmodell. Ein einfacher Organizer tut es auch. Wenn Sie nur die Passwörter und z.B. einige ganz persönliche Telefonnummern speichern wollen, so genügt ein einfachster Organizer mit passwortgeschütztem Bereich. Diese sind nicht nur klein und handlich, sondern auch einfach zu handhaben.

Auf die Idee der Speicherung im Mobiltelefon sollten sie besser verzichten. Mobiltelefone haben normalerweise keinen verschlüsselten und passwortgeschützten Bereich für besondere Daten. Deshalb ist diese Möglichkeit ungeeignet. Wenn Ihnen das Mobiltelefon gestohlen wird oder verloren geht, dann kann diese schwere Folgen haben!

Auch bei den Organizern müssen Sie unbedingt darauf achten, dass die Daten vernünftig geschützt sind und die Daten nicht mit Zusatzprogrammen von jedem PC aus ausgelesen werden können.

Wichtig ist in jedem Fall:
Wenn Ihnen der Organizer oder der PC/Laptop evtl. das Mobiltelefon abhanden kommt, so müssen Sie sofort alle Kreditkarten sperren, die Bankkonten sperren und alle Passwörter für alle Anwendungen und E-Mailkonten sowie für alle anderen Dienste so schnell als möglich ändern und den Verlust allen Betreibern sofort melden!

Auch den Kreditkartenfirmen und Banken sollten Sie den Verlust nicht nur sofort per Telefon melden. Eine zusätzliche schriftliche, eingeschriebene Meldung empfehle ich unbedingt.

Es gibt genügend Beispiele für reichhaltigen Ärger nach dem Verlust eines Organizers, eines PC's, eines Laptops, eines Handys, von Kreditkarten, Bankkarten, Kundenkarten usw. usw. usw. Sorgen Sie deshalb rechtzeitig vor, bevor es zu spät ist!

Wenn Sie nun so am Surfen sind, so beachten Sie bitte, dass es besser ist, das Login und das Passwort jedes mal neu einzugeben, als dieses im Browser zu speichern. Schliesslich sind nicht alle Browser in der Lage, ein Passwort verschlüsselt zu speichern.

Heute gibt es übrigens auch frei nutzbare Passwortsafeprogramme oder günstige Passwortsafeprogramme zu kaufen. Für die Erstellung von sicheren Passwörtern gibt es zudem frei nutzbare Programme oder Internetseiten.

Auf die Problematik, dass nicht alle Verschlüsselungsalgorhythmen wirklich sicher sind, soll hier nicht weiter eingegangen werden. Denn, um eine verschlüsselte Datei zu knacken benötigt es schon einiges an Fachwissen, weshalb im Allgemeinen eine reine Verschlüsselung genügt. Weiter benötigt der Hacker auch einige Zeit für das Knacken, so dass Sie hoffentlich vorher die Passwörter geändert und alle Meldungen erledigt haben.

Auch wenn Sie die Passwörter in einem Safe, einem verschlüsselten Laufwerk oder in einem passwortgeschützten Bereich aufbewahren, so ist es immer Notwendig bei einem Verlust sofort alles Sperren zu lassen.

Wenn Sie dies alles beherzigen, so können Sie sich viel nachträglichen Ärger und einiges an Kosten ersparen.

14 Einkauf im Internet / Kreditkarten

Es ist so einfach in der neuen digitalen Welt. Nur auf Bestellung drücken, die Kreditkartennummer eingeben, die Lieferadresse ausfüllen und fertig ist der Einkauf via Internet. Aber ist das auch wirklich sicher?

Ich weiss, ich bin altmodisch und viel zu vorsichtig. Nur, es gibt einige Personen, die durch solche Unvorsicht einen erheblichen Verlust erlitten haben. Darum:

Kreditkartennummern, Kreditkartendaten und andere persönliche Daten gehören nicht auf den Internetrechner.

Wenn überhaupt, dann müssen diese unbedingt verschlüsselt auf der Harddisk gespeichert werden. Natürlich darf das Laufwerk während der Verbindung mit dem Internet nicht geöffnet sein.

Aber nochmals zum Kauf via Kreditkarte im Internet:

Ich persönlich rate vom Kauf via Kreditkarte im Internet ab.

Der Kauf via Kreditkarte ist zwar kein Problem im Internet und meist geht es auch gut. Leider gibt es auch hier schwarze Schafe. Die Problematik liegt ganz einfach in der Beweisbarkeit. Beim normalen Einkauf mit der Kreditkarte in einem Geschäft ist die Unterschrift das Kriterium.
Beim Internet ist es nur die Kreditkartennummer, eine hoffentlich verschlüsselte Verbindung und ein „Enter“.

Das ist nach meiner Ansicht einfach viel zu wenig. Es gibt zwar seit einiger Zeit ein System, bei welchem sich die Person mittels einer Autorisierungskarte identifiziert.
Diese spezielle Karte beinhaltet besondere Sicherheitsmerkmale und muss durch eine Amtsstelle ausgestellt werden. Aktuell wird dieses Verfahren für die digitale Unterschrift verwendet.
Möglicherweise ist dies die Zukunft einer sicheren Zahlung via Internet. Spuren hinterlässt allerdings beides. Und was ist, wenn die Indentifikations- / Autorisierungskarte verloren geht oder gestohlen wird? Ich bin noch nicht gänzlich überzeugt vom neuen System, auch wenn die Ansätze in eine gute Richtung gehen.

Irgendwann wird sich bestimmt ein sicheres System durchsetzen. Das wäre dann vermutlich auch etwas für mich.

Daneben gibt es aber auch noch einiges, was interessant ist. Denn generell gilt:

Kreditkarten/Banocmatkarten/EC-Karten usw. verleiten zu vermehrten Ausgaben. Wer seine Finanzen im Griff haben will, der verzichtet im täglichen Leben auf eine Kreditkarte/EC-Karte und kauft ohne Ausnahme mit Bargeld ein.

Weiter sollte die Bezugsmöglichkeit mit der Bancomatkarte auf eine monatliche Limite begrenzt werden.

Wer in den Ferien eine Kreditkarte verwendet sollte sich eine klare Limite setzen und diese auch einhalten.

Leider sind die Codes der Kreditkarten auch nicht das Sicherste, was es gibt. Dies hat Tron eindrücklich bewiesen. Möglicherweise starb er auch genau deshalb. Zwar wurde der Schutz durch ein neues System bei Bancomaten verbessert. Geknackt werden können diese aber noch immer. Ein weiteres System ist dasjenige des Aufsatzes auf den Bancomaten. Dabei wird ein Lesekopf auf den Bancomaten aufgesetzt dieser zeichnet die Daten der Kreditkarte auf. Zusammen mit dem ausgespähten Code lässt sich ein Klon der Kreditkarte erstellen. Der Rest findet sich auf dem Kontoauszug.

Wer mehr erfahren möchte findet dies auf der Homepage des Chaos Computer Clubs und auf den von diesem herausgegebenen CD's.

Zwar ist Barzahlung auch nicht alles. Aber Barzahlung hat einige Vorteile. So z.B., dass die nachfolgenden Kunden und Kundinnen nicht so lange an der Kasse warten müssen. Und wenn die Verarbeitung der Kreditkartenbezüge mal wieder überlastet ist (wie z.B. vor Weihnachten) dann kann es schon mal sein, dass Sie die Ware wieder zurück ins Gestell legen müssen. Mit Bargeld wäre Ihnen das nicht passiert.

Bargeld bedeutet aber auch eine erhöht Wachsamkeit über das Portemonnaie!

Wofür Sie sich auch immer entscheiden, alles hat Vor- und Nachteile. Ich bin allerdings der Ansicht, dass die Barzahlung am meisten Vorteile und am wenigsten Nachteile hat. Entscheiden Sie selbst.

15 Anonym im Internet

Ich habe es schon ganz am Anfang erwähnt. Das Internet ist nicht Anonym. Dies gilt für alles, was Sie im Internet tun.

Bleiben Sie deshalb bei meinem Tipp. Stellen Sie sich weiterhin vor, Sie stünden in einem grossen Saal auf der Bühne und alle würden via Beamer zusehen, wie Sie am Rechner arbeiten und alle würden sehen, was Sie gerade auf dem Rechner und im Internet machen.

Na ja, nicht gerade angenehm. Ein wenig privater geht es schon.

Sie können einen Anonymusdienst während des Surfens verwenden.

Die Spuren im Internet können insofern vermieden werden, als dass nicht zurückverfolgt werden kann, welches Ihre IP-Nummer (ID im Internet) ist und wo Sie sich verbunden haben.

Dies ist besonders bei ISDN, ADSL und Surfen via Kabelnetz wichtig. Bei der Telefonverbindung wird normalerweise jedes Mal eine neue IP zugeteilt. Damit ergibt sich jedes Mal eine neue ID bei einer Telefonverbindung. Bei ISDN, ADSL und Kabelnetz ist dies nicht immer der Fall.

Ich verwende für das anonyme Surfen JAP von der Uni Dresden. Diese Software läuft auf Windows und/oder Linux. Es verhindert, dass der Surfer eindeutig identifiziert werden kann. Leider hat das aber auch einen Nachteil. Die Surfgeschwindigkeit nicht ab. Dies deshalb, weil alle Daten zuerst über den Server der Uni Dresden laufen müssen.

Wer also nicht unbedingt auf ein anonymes Surfen angewiesen ist, kommt ohne Anonymisierung schneller voran im Internet.

16 Surfspuren

Auch wenn nicht jeder im Internet die Spuren ihres Surfens verfolgen kann, so hinterlässt das Surfen immer irgendwelche Spuren. Besonders auf dem eigenen PC. Nur, was dagegen tun?

Surfspuren lassen sich mit einfachen Programmen oder einigen Einstellungen im jeweiligen Browser beseitigen. Allerdings sollten Sie die Beseitigung der Spuren regelmässig durchführen, am Besten nach jedem Surfen im Internet.

Bei Firefox können die wichtigsten Spuren (Chronik, Formulardaten, Passwörter, Cookies und Cache) getrennt verwaltet und getrennt oder gesamthaft manuell gelöscht werden.

Beim Internet Explorer ist dies teilweise unter Extras/Einstellungen möglich. Leider können nur die Cookies und der Verlauf gelöscht werden. Dies ist ärgerlich. Der Rest muss direkt im Profil des jeweiligen Users gelöscht werden. Insbesondere für den Internet Explorer gibt es kommerzielle Programme die die Spuren auf dem PC mit einem Klick löschen.

Auch löschen diese Programme üblicherweise auch die temporären Dateien und die temporären Verknüpfungen im Ordner Start/Dokumente.

Noch einen Vorteil hat das regelmässige Löschen. Das System bleibt sauber, stabil und schnell. Denn je mehr solcher Daten auf dem System verbleiben, desto mehr Rechenleistung werden gebunden, zumindest im Prinzip. Das ist am Anfang nicht viel, kann sich aber mit der Zeit zusammenzählen und das System langsamer machen.

Wer sicher gehen will, der verwendet am Besten ein kommerzielles Programm für die Vernichtung der Surfspuren. Bei einem guten Anonymizer ist ein Spurenvernichter oftmals bereits enthalten.

Wen es nicht stört, der kann auch nur gelegentlich die Dateien manuell löschen. Mir persönlich genügt die manuelle Löschung.

17 Laptop und Notebook

Laptop oder Notebooks sind eine feine Sache. Mit Ihnen lässt es sich fast überall arbeiten. Leider verbirgt sich hinter einem tragbaren Computer auch ein nicht unerhebliches Sicherheitsrisiko.

Denn, wer mit einem Laptop unterwegs ist, der hat oft vergessen, diesen genügend zu sichern. Deshalb gilt:

Sie sollten besonders vorsichtig sein, wenn Sie einen Laptop / ein Notebook ausserhalb von Zuhause verwenden.

Nebst einer gesunden Vorsicht ist ein Schutz eines Laptops notwendig. Einige kleine Massnahmen können hier schon viel eindämmen oder verhindern. Natürlich lassen sich auch hier die meisten Sicherheitseinstellungen umgehen. Dafür ist aber meist ein ziemlich grosser Zeitaufwand notwendig! Deshalb sind die hier beschriebenen Massnahmen im allgemeinen genügend.

Folgende Massnahmen empfehle ich Ihnen:

Schützen Sie den Laptop durch ein sicheres Bios-Passwort. Dieses müssen Sie zwar bei jeder Anmeldung eingeben, dafür ist der PC einigermassen gut geschützt, und dies schon beim Aufstarten. Ohne einen Hardwareeingriff kann normalerweise das Bios-Passwort nicht entfernt werden.

Legen Sie ein mobiles Profil an. Insbesondere ausserhalb von Zuhause sollten Sie nur mit einem mobilen Profil arbeiten. Dieses muss nicht nur eingeschränkt sein bezüglich der Rechte. Es müssen unbedingt alle kabellosen Verbindungen (Bluetooth, W-Lan) deaktiviert werden. Damit kann sich niemand unbemerkt mit Ihrem Laptop verbinden.

Für die Zeit, in welcher Sie den Laptop nicht benützen sollten Sie unbedingt das Bildschirmpasswort aktivieren. Damit ist sichergestellt, dass zufällig vorbeigehende Personen nicht einfach im Laptop schnüffeln können. Schalten Sie den Bildschirmschoner ein und aktivieren Sie die Passworteingabe bei Reaktivierung. Stellen Sie die Zeit auf das Minimum von einer Minute ein.

Arbeiten Sie unterwegs zudem NIE mit dem Administratorprofil. Schützen Sie alle anderen Profile durch geeignete Passwörter. Natürlich müssen Sie auch dem mobilen Profil ein Passwort vergeben.

Wenn Sie das CD-Laufwerk / Diskettenlaufwerk / Modem usw. nicht benötigen, dann melden Sie beide in diesem Benutzerprofil für unterwegs ab. Ebenso können Sie andere Schnittstellen abmelden (Serielle, Parallele, USB usw.) in diesem Benutzerprofil.

Verschlüsseln Sie unbedingt alle persönlichen Daten auf dem Laptop. Hierfür gibt es gute und günstige Programme (z.B. Steganos Safe). Verwenden Sie für die Verschlüsselung ein besonders sicheres Passwort.

In einigen Ländern ist es zudem notwendig, den Laptop beim Verlassen des Hotelzimmers mechanisch zu sichern. Auch daran sollten Sie denken und ein Schloss mit Stahlkabel mitführen.

Lassen Sie keine CD, Disketten, Speichersticks usw. mit sensiblen Daten in der Laptoptasche zurück. Gleiches gilt für Programminstallationen. Das Beste ist, Sie führen diese Datenträger schon gar nicht mit.

Wenn Sie bestimmte Treiber oder Installationen regelmässig benötigen und genügend Speicherplatz auf der Festplatte haben, dann können Sie die CD auch auf die Festplatte kopieren. Einige Programme lassen sich so auch installieren. In jedem Fall läuft das Ganze mit einem virtuellen Laufwerkprogramm. Das Mitführen von Installationen ist deshalb nicht notwendig.

ACHTUNG:
In einigen Ländern ist das Einführen von Verschlüsselungsprogrammen unter Androhung von Strafe bis hin zur Todesstrafe verboten (z.B. in China gilt auf die Einfuhr von Verschlüsselungsprogrammen die Todesstrafe).

Hier in Europa darf – meines Wissens (ohne Haftung) - jeder seine Daten verschlüsseln, wie er will. Dies ist besonders wichtig für portable Computer.

18 Updates

Es geht heute so einfach. Bei der Installation von Windows und anderen Programmen ist das automatische Update eingeschaltet. Jedes Mal, wenn der PC gestartet wird verbindet sich dieser automatisch mit dem Internet und holt die neuen Updates ab.

Nur, sind Sie sicher, das er nur Updates abholt und keine persönlichen Daten versendet? Ich nicht. Deshalb empfehle ich:

Erlauben Sie keine automatischen Updates.

Entscheiden Sie selbst, wann Sie ein Update vornehmen wollen und von wem und für welches Programm.

Ausser beim Virusscanner sollten Sie alle automatischen Updates erlauben. Dies ist vernünftig, weil der Virenschutz nur dann etwas nützt, wenn er regelmässig auf dem neuesten Stand gehalten wird. Deshalb ist dies auch das einzige Programm, bei welchem ich ein automatisches Update erlaube.

Insbesondere sollten Sie via Firewall alle Zugriffe von Programmen auf das Internet unterbinden.

Danach können Sie einzeln auswählen, ob ein Programm einen Update oder eine Registrierung vornehmen darf oder nicht. Dabei sollten Sie den Zugriff immer nur einmalig erlauben. Sie werden staunen, wie viele Programme auf das Internet zugreifen wollen.

Übrigens wollen nicht nur Programme ihre persönlichen Daten an die Softwarefirma senden. Besonders Windows steht hier in vorderster Reihe.

19 Windows phone Home

Windows hat die leidige Angewohnheit bestimmte Daten an Microsoft senden zu wollen. Zudem ist bis heute nicht klar kommuniziert worden, welche Daten in welchen Fällen an Microsoft gesandt werden.

Einzig bei der Registrierung hat Microsoft einige Angaben bekannt gegeben. Ob diese Meldungen tatsächlich der Wahrheit entsprechen ist aber weiterhin nicht bekannt. Alle anderen Updates, Aktivierungen und Verbindungen mit dem Softwareherstellern können zum übertragen von Informationen führen. Besonders dem Betriebssystem Windows sollten Sie dies abklemmen.

Verwenden Sie deshalb das Programm Anti-Spy und deaktivieren Sie die entsprechenden Einstellungen in Windows.

Das Programm ist Freeware und erlaubt viele Einstellungen von Windows einfach durch einen Mausklick zu ändern bzw. die Kontaktaufnahme und das Senden von Daten zu unterbinden. Auch andere Sicherheitseinstellungen können damit entsprechend angepasst werden.

Damit sind Sie wenigstens bezüglich Datenmeldungen einigermassen auf der sicheren Seite. Zudem stoppt eine richtig eingestellte Firewall allfällige nicht explizit gesperrte Meldungen, vor allem aber die Meldungen anderer Programme.

20 Datenvernichtung in Windows

Sicher haben Sie schon einmal Daten gelöscht und waren der Ansicht, dass diese dauerhaft gelöscht sind. Löschen ist in Windows nicht einfach löschen. Die Daten werden dabei nicht wirklich gelöscht. Es wird nur der Verzeichniseintrag in den Papierkorb verschoben. Von dort aus kann dieser wieder hergestellt werden.

Auch wenn im Papierkorb diese Eintrag gelöscht wird, dann ist die Datei noch immer nicht endgültig gelöscht. Vielmehr wird der Speicherplatz für neue Daten frei gegeben. Wann dieser Speicherplatz überschrieben wird, ist nicht vorhersagbar. Dies deshalb nicht, weil Windows ein dynamisches Speichersystem besitzt. Das bedeutet, dass dort gespeichert wird, wo es gerade Platz und/oder wo die Lese- und Schreibköpfe der Harddisk schnell zugreifen können.

Löschen Sie sensible Daten deshalb dauerhaft durch eine Mehrfachüberschreibung.

Um eine Datei dauerhaft zu löschen muss der Speicherplatz auf der Harddisk mehrmals überschrieben werden. Denn auch einmal überschriebene Dateien können wieder hergestellt werden.

Auch hierfür gibt es entsprechende Programme. Dabei sollte dieses Mehrfachüberschreibsystem nur für sehr sensible Daten verwendet werden. Die Prozedur ist - je nach Anzahl der Überschreibungen - sehr zeitaufwendig. Bei einigen Programmen ist ein solches Tool in der Verschlüsselungssoftware/Datensafe inbegriffen (z.B. bei Steganos).

Nach Anwendung eines solchen Tools können keine gelöschten Dateien auf der Harddisk mehr wiederhergestellt werden. Es gibt meist auch die Möglichkeit, direkt beim Löschen diese Dateien mittels des Programms zu überschreiben und so nicht den ganzen freien Speicherplatz überschreiben zu müssen. Das spart viel Zeit und Mühe.

Schliesslich gibt es noch eine ganz einfach Methode. Wer seine Daten in einem Datensafe ablegt, der kann diese dort problemlos löschen. Denn auch die Wiederherstellung des Dateinamens vermag die Datei nicht wieder herzustellen, denn diese befindet sich ja im verschlüsselten Laufwerk und damit ist diese unerreichbar (zumindest wenn das Laufwerk geschlossen ist). Wenn nun das verschlüsselte Laufwerk gelöscht wird, dann kann auch keine einzelne Datei mehr wiederhergestellt werden. Denn es kann nur das ganze Laufwerk wiederhergestellt werden. Und nach der Wiederherstellung sind die Daten noch immer verschlüsselt. Denn Wiederherstellung bedeutet nur, dass die Daten auf den letzten Stand (das verschlüsselte Laufwerk) zurück gestellt werden.

So einfach kann Datensicherheit sein.

21 Freie Programme (Freeware)

Zum Abschluss noch etwas zu der freien Software.

Darunter verstehe ich Freeware und GNU/GPL Programme.

Ich persönlich rate allen Personen, wenn immer möglich nur Freeware oder GNU/GPL Programme zu verwenden. Von diesen Programmen gibt es heute eine grosse Anzahl auf dem Markt. Für fast alle Anwendungsbereiche.

Oftmals werden auch kommerzielle Programme für Heimanwender frei gegeben, d.h. Privat dürfen gewissen Programme frei verwendet werden ohne eine Lizenz zu erwerben (z.B. Web Washer). Nur wer diese kommerziell einsetzt muss eine Lizenz erwerben. Auch dies ist eine gute Möglichkeit, Software frei zu nutzen.

In jedem Fall rate ich dazu, keine Software ohne Lizenz auf dem PC ein zu setzen. Es gibt wirklich genügende und gute Alternativen.

Wenn Sie diesem Clinch generell entgehen wollen, dann sollten Sie Linux verwenden. Ich verwende übrigens eine SUSE Distribution und bin damit sehr zufrieden. Linux bietet für viele Anwendungen eine geeignete Lösung, oftmals mehrere Lösungen. Hinzu kommt, dass der Quellcode zugänglich ist und damit auch Anpassungen der Programme vorgenommen werden können.

Diese Art der Software ist in jedem Fall besser als die Verwendung von „Raubkopien“. Nebst der Tatsache, dass Sie sich mit Freeware nicht strafbar machen kommen Sie erst noch viel billiger oder fast gratis zur Software. Heute gibt es schliesslich schon ganze Officelösungen als GNU/GPL im Sinne einer Freeware.

Auch sind diese Programme fast immer mit den Programmen von Microsoft kompatibel, zumindest was die Datenhaltung angeht.

Wer eine Textverarbeitung zum Briefe schreiben benötigt, einen Notizblock, eine Tabellenkalkulation, einen Internetzugriff und eine Bilderverwaltung mit Bildbearbeitung, der ist mit Linux genau so gut bedient wie mit Microsoft. Zudem ist die heutige Benutzeroberfläche z.B. des KDE von Linux sehr gut und einfach zu bedienen.

Nicht immer gibt es jedes Programm auch in einer Linux-Version. Doch fast immer gibt es eine ähnliche Lösung mit einer Linux-Anwendung. Für die wenigen Fälle, in denen dies nicht möglich ist, können Sie immer noch ein Windows auf dem Rechner belassen. Wenn dieses aber nicht geschützt ist, dann verwenden Sie unbedingt nur Linux zum Arbeiten und Surfen.

Ansonsten sollten Sie diese Tipps beherzigen und Ihr System sicherer oder gar sicher machen.

22 Der Computer am Arbeitsplatz

Ein paar Worte möchte ich noch über den Computer am Arbeitsplatz verlieren.

Heute arbeiten viele Menschen mit einem Computer, viele auch den ganzen Tag. Da drängt sich immer wieder die Frage nach Datensicherheit, PC-Verwendung oder Spionage auf.

Hierzu gibt es einige wissenswerte Tatsachen:

Der PC am Arbeitsplatz ist grundsätzlich für die Erledigung der täglichen Arbeit gedacht und wird hierfür auch vom Arbeitgeber zur Verfügung gestellt.

Jegliche private Verwendung müsste eigentlich durch den Arbeitgeber ausdrücklich genehmigt oder verboten werden. Die Situation in der Realität sieht oftmals anders aus. Viele Arbeitgeber und Angestellte sind hier mit einer Grauzone einverstanden. Das bedeutet, dass viele Arbeitgeber die Verwendung des PC's für private Zwecke (z.B. um einen Brief zu schreiben) in einem beschränkten Umfang erlauben.

Beim E-Mail und beim Internet ist die Situation ein wenig anders. E-Mail ist heute sehr weit verbreitet. Dabei ist E-Mail alles andere als eine sichere Möglichkeit der Kommunikation. Auch für E-Mail gilt im Prinzip dasselbe wie für den PC allgemein. Es muss vereinbart werden. Allerdings gibt es beim E-Mail einige Tricks. Es lassen sich alle E-Mails zum Systemverantwortlichen umleiten. Noch schlimmer, von jedem E-Mail kann im System eingegeben werden, dass eine Kopie an eine bestimmte Person geht (z.B. an den Chef, den EDV-Verantwortlichen) OHNE dass Sie etwas davon merken!

Das System erstellt im Hintergrund eine Kopie des E-Mails und sendet das Original an Sie und die Kopie an die entsprechende Person. Auch das Lesen Ihrer E-Mails ausserhalb der Geschäftszeit ist nur ein paar Mausklicks entfernt. Ob ein Betrieb hier die E-Mails der angestellten Personen liest oder nicht, können Sie anhand des Systems bzw. Ihres E-Mailordners nicht feststellen. Und nicht in allen Betrieben erhalten Sie auf die Frage nach der E-Mailüberwachung auch eine ehrliche Antwort.

Allerdings ist es auch für den Arbeitgeber nicht ganz so einfach. Denn wer die E-Mails der Angestellten ohne deren Wissen überwacht, der greift in die Privatsphäre jedes einzelnen Angestellten ein. Dies wiederum stellt einen klaren Verstoss gegen den Grundsatz des Verbotes einer dauernden Überwachung dar. Der Arbeitgeber kann zwar allenfalls die Informationen gegen Sie verwenden, allerdings muss er bei einer Klage meist auch einstecken.

Beim Internet ist die Sache noch etwas komplizierter. Denn wer während der Arbeitszeit surft, schädigt im Prinzip den Arbeitgeber. Dies in der Form, als dass er während der Surfzeit keine Arbeit erledigt. Dies ist üblicherweise so lange kein Problem wie die Person in der Lage ist, trotz surfen, die Arbeit fristgerecht, korrekt und qualitativ gut auszuführen.

Natürlich könnte der Arbeitgeber nun argumentieren, dass ohne Surfen die angestellte Person mehr Arbeit erledigen könnte. Und dies ist bei einer Einzeltätigkeit auch ein echtes Beweisproblem. Wenn hingegen eine Person die gleiche Arbeit wie viele andere Personen im gleichen Betrieb macht und insgesamt die gleiche Arbeitsleistung wie eine Person erbringt, die nicht im Internet surft, so dürfte dies keine grösseren Schwierigkeiten geben. Voraussetzung ist natürlich, dass beide etwa gleich viel Lohn haben.

In diesem Fall können Sie sich darauf berufen, dass Sie trotz surfen die gleiche Arbeitsmenge in gleich guter Qualität erledigen, wie die langsamer arbeitende Person in gleicher Funktion und demzufolge dem Arbeitgeber keine Mehrkosten entstehen. Denn der

anderen Person in gleicher Funktion muss der Arbeitgeber für die gleiche Arbeit (inkl. Surfen) den gleichen Lohn zahlen.

Wenn Sie allerdings mehr verdienen oder die einzige Person sind, die diese Aufgabe erfüllt, dann haben sie Pech gehabt. In diesem Fall gibt es weder eine Vergleichszahl, noch können Sie sich auf den Lohn berufen. Vielmehr kann der Arbeitgeber in diesem Fall darauf hinweisen, dass er für mehr Lohn auch mehr Leistung erwarten darf. Abgesehen vom Alter.

Zudem hat das Internet noch andere Gefahren. Wenn Sie im Internet surfen und einen Virus, Trojaner oder eine andere Software auf den Rechner laden, dann kann dies ernsthafte Folgen haben. Dies kann bis hin zu Schadensersatzforderungen gehen. Sie sollten deshalb in jedem Fall vorsichtig sein beim Surfen im Geschäft. Klicken Sie keine Seiten mit zweifelhaften Inhalten an. Laden Sie nichts auf den PC herunter und geben Sie keine Angaben über Sie oder die Firma bekannt.

Zudem wird üblicherweise aufgezeichnet, welche Internetseiten eine Person anwählt. Damit lässt sich genau verfolgen, wann Sie welche Seite aufgerufen haben und wie lange Sie dort verweilt sind.

Hier ist die Problematik der Überwachung etwas komplizierter. Denn, der Arbeitgeber darf grundsätzlich die Aktivitäten des Internets (im Prinzip auch des E-Mail, PC's, Telefons, Fax usw.) aufzeichnen. Dabei muss er allerdings die Stichproben, ob eine Person verbotenes im Internet gemacht hat, Stichprobenweise analysieren. Diese Analyse muss z udem anonym sein.

Findet der Arbeitgeber nun solche Informationen, so darf er nachsehen, welche Person diese Zugriffe verursacht hat. Daraufhin dürfen zwar die Daten nicht gegen Sie verwendet werden. Aber der Arbeitgeber kann Sie auffordern, die Aktivitäten zu unterlassen. Ebenso kann er eine Überwachung ankündigen.

Wenn ein Arbeitgeber eine Überwachung ankündigt, so muss er genau angeben, was überwacht wird, bei wem und wie lange. Eine generelle Überwachung und Aufzeichnung ist nicht zulässig. Gemäss Art. 11 des Datenschutzgesetzes DSG sind dauernde Überwachungen durch Privatpersonen oder Firmen, ohne dass die betroffene Person davon Kenntnis hat, dem Datenschutzbeauftragten zu melden, sofern es sich nicht um eine gesetzliche Pflicht zur Datenerhebung und Speicherung handelt.

Daraus ist auch ersichtlich, dass Spionageprogramme generell nicht erlaubt sind! Die Privatsphäre am Arbeitsplatz wird sowohl arbeitsrechtlich als auch durch das verfassungsmässige Fernmeldegeheimnis (BGE 126 I 50) geschützt.

Hinzu kommt, dass der Arbeitgeber nur Daten speichern darf, die der Einhaltung des Zweckbindungs- und Verhältnismässigkeitsprinzips entsprechen (Art. 26 Ar GV 3 DSG und Art. 328 und 328b OR).

Es ist deshalb mehr als sinnvoll, wenn ein Arbeitgeber klar bekannt gibt, wie und unter welchen Voraussetzungen die einzelnen Kommunikationsmittel verwendet werden dürfen. Insbesondere für E-Mail und Internet wäre eine klare Regelung ein Muss für jeden Betrieb.

Das hindert allerdings viele Arbeitgeber nicht daran, E-Mails zu lesen, Computereingaben aufzuzeichnen, das Internet zu überwachen und die Telefonlisten zu kontrollieren. Ich spreche aus eigener Erfahrung, wenn ich sage, dass die Installation von Spionageprogrammen auf dem PC der angestellten Personen keine Seltenheit sind. Das kann in Einzelfällen auch bis hin zur Überwachung mit Videokameras gehen.

Heute sind übrigens Videokameras so klein, dass ein stecknadelgrosses Loch irgendwo in der Decke oder der Wand genügt, um klare und verwertbare Aufnahmen zu erhalten und das bei guter Installation sogar mit Ton.

Abschliessen kann ich nur darauf hinweisen, dass die Überwachung am Arbeitsplatz gerne verschwiegen wird. Auch werden mehr Kontrollen gemacht, als häufig angenommen wird. Gleichzeitig gibt es aber auch Firmen, die sich überhaupt nicht darum kümmern. In jedem Fall ist es mehr als unangenehm für die Betroffenen und deshalb sollten Sie immer wieder nachfrage, ob solche Kontrollen statt finden. Falls ja, dann sollten Sie eine Einsicht in die Dokumente verlangen.

Gleichzeitig ist es wichtig, dass der Arbeitgeber klare Richtlinien erlässt.

Trotzdem. Auf den Geschäftsrechner gehören keine privaten bzw. sehr persönliche E-Mails. Dafür ist das Geschäft nicht der richtige Ort. Auch heikler Briefverkehr gehört nicht auf den Geschäfts-PC.

Noch schlimmer ist das Ganze bei einem Laptop. Dort ist es zwar einfacher, eigene Daten zu speichern. Jedoch sollten Sie bedenken, dass diese bei der Rückgabe wirklich gelöscht werden müssen. Zudem muss der Laptop richtig gesichert sein damit die geschäftlichen Daten auch wirklich sicher sind. Dies sollten Sie auf keinen Fall vernachlässigen.

Je vorsichtiger Sie mit dem Geschäfts-PC umgehen, desto weniger Ärger kann entstehen.

Aber auch hier gelten alle obigen Bemerkungen bezüglich Sicherheit im Internet sinngemäss.

23 Schlussbemerkungen

Ist so viel Sicherheit nicht krankhaft?

Nein. Ich bin nicht paranoid. Ich habe nur ein ausgeprägtes Sicherheitsbewusstsein aufgebaut aufgrund meiner früheren Tätigkeit als EDV-Verantwortlicher. In dieser Funktion habe ich gesehen, wie Systeme überwacht und ausspioniert werden können. Ebenso sah ich aber auch, wie schnell sich ein Virus ausbreiten kann, wenn ein System nicht genügend geschützt ist.

Egal wie gut ein System auch immer gesichert ist und egal wie ausgefeilt Firewall und Virenscanner arbeiten. Ein Befall des Rechners kann nie ganz ausgeschlossen werden. Aber mit den hier vorliegenden, persönlichen Ratschlägen werden viele kritische oder gefährliche Situationen abgeblockt.

Seit gut einem Jahr verwende ich persönlich eine SUSE Linux Distribution mit Firewall. Seither habe ich mir noch nie einen Virus eingefangen, trotz fehlendem Virenscanner.

Zuvor habe ich mit Windows 98 und XP gesurft. Hier habe ich mir ein mal einen Virus eingefangen als ich versehentlich die Firewall ausgeschaltet habe. So etwas kann auch mir passieren. Mit dem Virenscanner von Symantec/Norton konnte ich den Virus aber innert kürzester Zeit wieder vom System eliminieren. Ansonsten hatte ich beim geschützten Windows-System nie irgendwelchen Ärger mit Viren.

Geraten Sie deshalb nicht in Panik, wenn Sie einen Virus auf dem System haben.

Versuchen Sie diesen mit dem Virenscanner zu beseitigen und/oder ersuchen Sie Freunde/Bekannte um Hilfe. Wenn Sie einen separaten Internetrechner verwenden, dann ist das Schlimmste was passieren kann, dass Sie das System neu installieren müssen.

Vergessen Sie in keinem Fall - nach jeder Arbeit auf dem Arbeitsrechner - die Daten extern zu sichern! Mischen Sie diese Daten nie mit den Daten des Internetrechners.

So kann auch das Betriebssystem abstürzen und es gehen keine Daten verloren.

Nun wünsche ich Ihnen

Viel Erfolg!

24 Allgemeine Geschäftsbedingungen Fa. Kirja / Daniel Dürr

Anmerkung des Autors: Es ist sehr bedauerlich, dass dieser Hinweis überhaupt notwendig ist...

Ich weise hier noch auf meine allgemeinen Geschäftsbedingungen hin. Diese gelten für dieses Dokument wie auch für alle anderen Dokumente und den gesamten Inhalt der Internetseiten und/oder der CD's und/oder den gesamten Geschäftsverkehr mit der Firma Kirja / Daniel Dürr und/oder der Versandfirma bzw. dem beauftragten Rechtsvertreter.

Leider gibt es immer weniger ehrliche Menschen auf dieser Welt. Es ist deshalb notwendig, einige rechtliche Aspekte zu regeln. Hier nun die Geschäftsbedingungen der Fa. Kirja / Daniel Dürr:

Urheberrecht

Alle Schriftstücke, sind urheberrechtlich geschützt. Jede Verbreitung, Kopie, Vervielfältigung, Veröffentlichung, ob auszugsweise oder gesamthaft, bedürfen der schriftlichen Zustimmung des Autors.

Jede/r Erwerber/in hat das Recht, allen rechtmässig erworbenen Schriftstücken alle Informationen zu entnehmen und/oder diese für den persönlichen, privaten Gebrauch auszudrucken. Die Verwendung der in den Schriftstücken enthaltenen Angaben für den persönlichen, privaten Gebrauch ist ausdrücklich gestattet. Jede/r Erwerber/in hat das Recht, sich eine Kopie der CD oder der Datei anzufertigen für die Datensicherung und/oder den persönlichen, privaten Gebrauch.

Sämtliche anderweitigen, nicht dem persönlichen, privaten Gebrauch dienenden Verwendungen bedürfen der schriftlichen Zustimmung des Autors. Insbesondere bedarf jegliches Kopieren der CD oder der darauf enthaltenen Dateien sowie jeder Druck, Auszug, Nachdruck oder jede anderweitige Verwendung, Vervielfältigung, Weitergabe usw. der CD bzw. des/der Schriftstücke/s - auch in gedruckter Form - der schriftlichen Zustimmung des Autors. Nebst diesen Bestimmungen gilt das allgemeine Urheberrecht.

Haftung

Für sämtliche Inhalte und jegliche Links sowie alles Anderweitige wird jede Haftung abgelehnt. Ebenso jede Haftung für Fehler, Irrtümer, den Inhalt und allfällige Folgen von Inhalten, Irrtümern und Fehlern.

Alle Haftungsansprüche wegen Schäden jeglicher (materieller oder immaterieller) Art, sind/werden soweit gesetzlich zulässig, vollständig ausgeschlossen. Jede Verwendung, Benutzung, Nachahmung, Weiterverwendung, Nachbau sowie sämtliche andern Möglichkeiten erfolgen vollständig auf eigenes Risiko und unterliegen keiner Haftung.

Personenkreis/Bestellung/Format/Verwendung

Alle zum Zeitpunkt der Bestellung mit dem/der Käufer/in im gleichen Haushalt lebenden Personen (Wohnsitz) dürfen das/die Schriftstück/e entsprechend den obigen Bedingungen ebenfalls nutzen.

Sämtliche Schriftstücke können nur schriftlich bestellt werden. Dies unter Angabe des Namens, Vornamens und der vollständigen Adresse sowie der E-Mailadresse und/oder der Telefonnummer (für Rückfragen).

Nach der Bestellung erhält der Kunde/die Kundin eine CD-Rom zusammen mit einer Rechnung und einem Einzahlungsschein.

Auf der CD-Rom befindet sich jeweils das/die entsprechende/n, bestellte/n Schriftstück/e in einem Exemplar. Üblicherweise erfolgt die Auslieferung im PDF Format. Anderweitige E-Bookformate können zur Anwendung gelangen. Das Leseprogramm wird üblicherweise ebenfalls auf der CD-Rom ausgeliefert. Es besteht kein Anspruch auf ein bestimmtes Format des/der Schriftstückes/e. Die Firma Kirja / Daniel Dürr legt das Format und die Bedingungen für den Lesezugriff sowie das Leseprogramm (PDF, E-Book oder andere) frei fest.

Bestellt der Kunde/die Kundin mehr als ein Werk- bzw. Schriftstück, so entscheidet die Firma Kirja / Daniel Dürr ob die Auslieferung aller Schriftstücke auf einer CD-Rom erfolgt oder ob jedes Schriftstück jeweils auf einer separaten CD-Rom ausgeliefert wird. Dabei wird, nach Möglichkeit, auf die Wünsche der bestellenden Person Rücksicht genommen. Ein Anspruch auf eine bestimmte Auslieferungsform besteht nicht.

Durch die Bestellung der/des Schriftstücke/s verpflichtet sich der Käufer zur Zahlung des Rechnungsbetrages, ohne jeden Abzug, innerhalb von 30 Tagen. Die Zustellung erfolgt innerhalb der Schweiz mit normaler Postsendung (B-Post) sowie ins Ausland üblicherweise mit eingeschriebener Sendung.

In besonderen Fällen behält sich der Autor/die Versandfirma vor, die CD/'s oder das/die Schriftstück/e mittels eines Codes/Passwortes zu sperren. Nach Einzahlung des vollständigen Rechnungsbetrages erhält der Kunde/die Kundin den persönlichen Lese- Druckzugangsscode/Passwort für das/die Schriftstück/e oder die CD/'s per Post oder EMail. Ein ausschliesslicher Anspruch auf eine Postzustellung des Codes besteht nicht.

Alle Schriftstücke können gelesen und gedruckt werden. Der generelle Code für jegliche Bearbeitung und Veränderung des/der Dokumente/s/Schriftstücke/s oder/und der CD wird nicht ausgeliefert. Es besteht mit dem Erwerb des Schriftstückes auch keinerlei Anspruch auf den generellen Bearbeitungscode bzw. das generelle Passwort.

Mit dem persönlichen Benutzercode kann der Kunde/die Kundin das Schriftstück lesen und ausdrucken. Über dies hinaus gehende Verwendungen sind gesperrt und nicht erlaubt. Ausgenommen bleiben die oben erwähnten *persönlichen, privaten*

Verwendungen. Jede Umgehung dieser Schutzvorkehren/Sperrfunktionen (Knacken des Codes usw. sowie alle anderen über das Lesen und Drucken hinaus gehenden Anwendungen) stellt eine strafbare Handlung im Sinne des Gesetzes dar und kann in jedem Einzelfall geahndet werden.

Das Schriftstück und der Datenträger bleiben Eigentum der Firma Kirja / Daniel Dürr. Mit dem Kaufpreis erwirbt der Käufer/die Käuferin das Recht, das Schriftstück (inkl. CD) auf unbestimmte Zeit gemäss den allgemeinen Geschäftsbedingungen zu nutzen. Ein Rückkauf durch die Fa. Kirja ist jederzeit, ohne Vorankündigung, möglich. Der Rückkaufspreis entspricht dem Durchschnittspreis für einen gleichen oder einen ähnlichen, leeren Datenträger, höchstens aber 10% des Verkaufspreises.

Verweigerung der Lieferung

Die Auslieferung der CD bzw. auch des persönlichen Benutzercodes erfolgt üblicherweise innerhalb von wenigen Arbeitstagen, längstens innerhalb von 30 Tagen nach Bestellungseingang. Der Autor/die Versandfirma behält sich in besonderen Fällen vor, ohne Angabe von Gründen, die Auslieferung zu verweigern. Dies wird dem Kunden üblicherweise schriftlich, innerhalb von 30 Tagen, angezeigt. Es besteht jedoch kein Anspruch auf eine schriftliche oder mündliche Benachrichtigung.

Verlust/Nachbestellung erworbener Schriftstücke und CD's/Rückgabe

Im Falle eines Nichterhaltes oder Verlustes durch die Post kann ein einziges, neues Exemplar schriftlich, innerhalb von 10 Tagen nach der Versandbestätigung, angefordert werden. Bei einem nochmaligen Verlust wird dem Kunden/der Kundin pro CD ein Betrag von 20% des Kaufpreises, mindestens jedoch Fr. 10.-- pro CD zusätzlich in Rechnung gestellt. Die spätere Nachbestellung einer CD, eines oder mehrerer Dokumente, ist unter Angabe des Namens, Vornamens und der vollständigen Adresse inkl. E-Mail und Telefonnummer möglich. Die Kosten betragen in diesem Fall 50% des aktuellen Verkaufspreises.

Ein Rückgaberecht der CD oder der/des Dokumente/s (z.B. wegen Nichtgefallens) und eine Rückerstattung des Kaufpreises besteht nicht.

Im Kaufpreis enthalten ist/sind

Im Rechnungsbetrag/Kaufpreis (ohne Abzug) enthalten ist/sind

- das Schriftstück/die Schriftstücke auf einer oder mehreren CD-Rom's
- das Porto für die Zustellung des/der Schriftstücke/s auf einer CD-Rom inkl. Rechnungsstellung und Einzahlungsschein innerhalb der Schweiz
- das Porto für die allfällige, eingeschriebene Zustellung des/der Schriftstücke/s auf einer CD-Rom inkl. Rechnungsstellung und Einzahlungsschein ausserhalb der Schweiz
- in besonderen Fällen: das Porto für die Zustellung des persönlichen Codes oder die Zustellung des Codes per E-Mail
- die allfällige MWST der Schweiz

Im Kaufpreis nicht enthalten ist/sind

Im Rechnungsbetrag/Kaufpreis (ohne Abzug) nicht enthalten ist/sind

- sämtliche Gebühren ab der Schweizer Grenze
- sämtliche Gebühren ausserhalb der Schweiz
- sämtliche Gebühren, welche oben nicht ausdrücklich genannt sind

Haftungsausschluss/Akzeptanz der allg. Geschäftsbedingungen/Besonderes

Es besteht ein vollständiger Rechts- und Haftungsausschluss für den gesamten Inhalt, alle Links sowie alle in diesem Werk angegebenen Daten, Fakten und alle weiteren Angaben, Hinweise, Tipps usw.

Mit der Bestellung (und/oder dem Download) erklärt sich der Käufer/die Käuferin (der Verwender/die Verwenderin) ausdrücklich mit diesen allgemeinen Geschäftsbedingungen der Firma Kirja / Daniel Dürr einverstanden. Der Gerichtsstand für alle Streitigkeiten ist der Wohnort des Autors (allenfalls der Versandfirma oder dem Rechtsvertreter der Fa. Kirja / Daniel Dürr).

Alle Zitate/Tipps dürfen unter Angabe des Autors und ohne Veränderung wiedergegeben und weitergegeben werden.

Wohnort des Autors, 03.03.2007

Der Autor

Firma Kirja

Daniel Dürr