Schützen Sie Ihre Daten

10 Tipps zur Datensicherheit

Elektronische Datenverarbeitung ist heute ein selbstverständlicher Teil unseres täglichen Lebens. Nicht ganz so selbstverständlich sind aber die dabei zu treffenden Sicherheitsvorkehrungen zum Schutz der Daten. Die nachfolgenden Hinweise sollen die Notwendigkeiten und Möglichkeiten zur Datensicherheit erläutern und einen bewussten Umgang mit der Technik fördern. Sie befassen sich mit folgenden Fragestellungen:

Regelmäßige Datensicherung

Es ist geschafft. Mit viel Mühe haben Sie Ihre persönlichen Dokumente, Ihren Schriftverkehr oder Ihre Fotosammlung auf dem PC sorgfältig gespeichert. Alle Daten sind auf der Festplatte gesichert und der PC kann beruhigt ausgeschaltet werden.

Doch Vorsicht! Elektronische Speichermedien wie beispielsweise Festplatten haben heute zwar lange Lebenszeiten, doch ist dies keine Garantie für fehlerfreies Funktionieren. Tritt ein Plattenfehler auf oder kann die Systemsoftware nur durch erneutes Einspielen restauriert werden, können Ihre persönlichen Daten unwiederbringlich verloren gehen. Besitzen Sie keine aktuellen Kopien Ihrer Schreiben, Ausarbeitungen oder Fotos können für Sie große Probleme entstehen, weil Sie z.B. Termine nicht einhalten können, Arbeiten ein zweites Mal durchführen müssen oder Sie Inhalte wichtiger Schreiben nicht mehr belegen können.

Und so sollten Sie Ihre Daten sichern:

Speichern Sie Ihre Daten in persönlichen Ordnern, so dass sie zusammenhängend gesichert werden können. Sichern Sie Ihre persönlichen Daten auf einem vom PC unabhängigen Datenträger. Benutzen Sie ein Medium mit ausreichend großer Speicherkapazität wie eine wiederbeschreibbare CD, DVD oder eine externe Festplatte.

Sichern Sie ihre Daten möglichst nach jeder wesentlichen Änderung oder besser noch: Spiegeln Sie Ihre Daten direkt auf das externe Speichermedium, ein Fehler kann jederzeit auftreten – auch wenn der PC lange Zeit einwandfrei gearbeitet hat.

Datensicherung ist Ihre persönliche Verpflichtung, auf die eigenen Daten zu achten. Hierzu gibt es keine Alternative und schon gar keine Garantie der Unternehmen, die Ihre Hard- oder Software hergestellt haben. Machen Sie die Datensicherung zum festen Bestandteil Ihrer PC-Arbeit.

Verschlüsselung

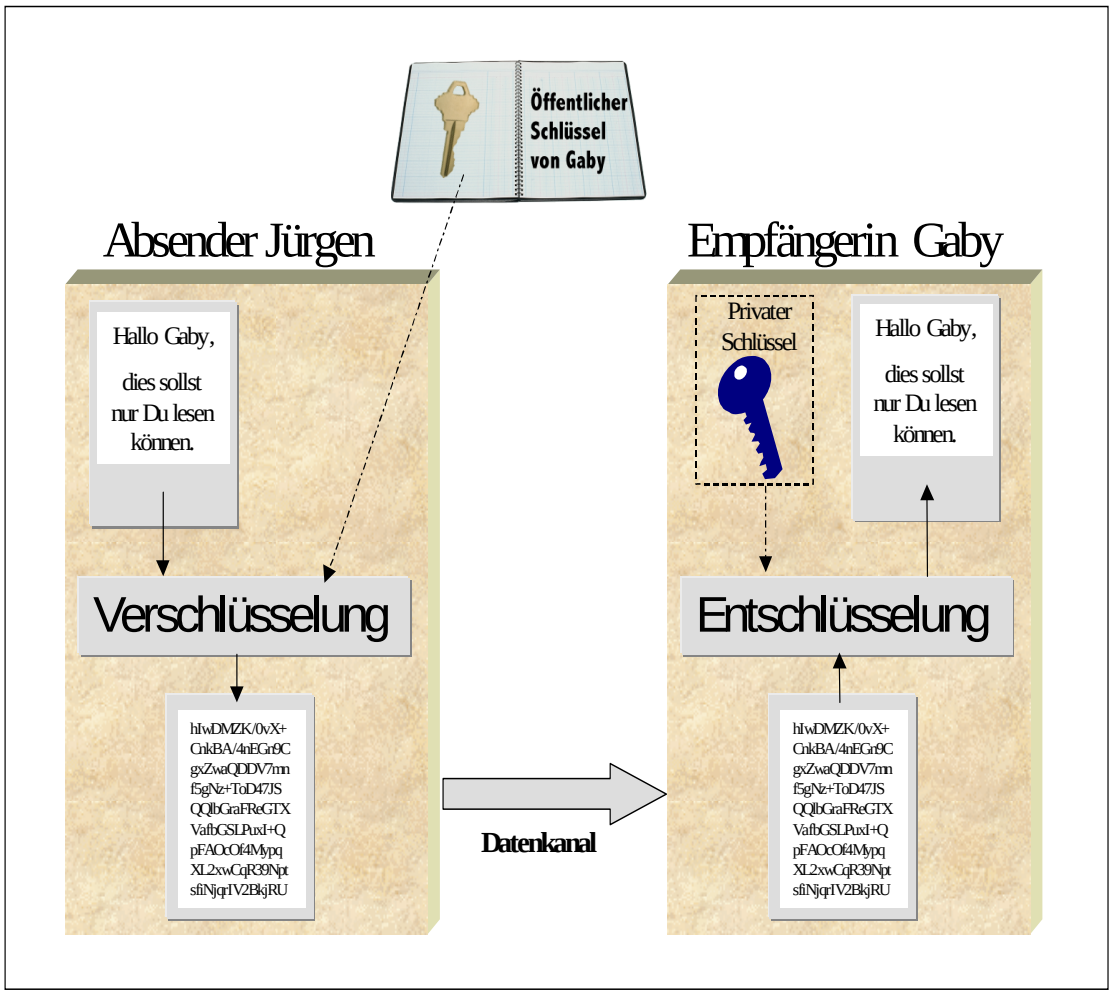
Was sie Ihnen nützt

Persönliche oder geschäftliche Daten sollten nicht in unbefugte Hände geraten. Sie sollen weder beim Versand über das Datennetz noch während ihrer Speicherung auf der Festplatte einfach eingesehen oder gar kopiert werden können. Eine Möglichkeit zum Erreichen dieser Ziele ist die Verschlüsselung der Daten. Mit Hilfe der Verschlüsselung können Sie selbst Ihre Daten eigenverantwortlich und effektiv schützen. Bei verschlüsselten Daten müssen Sie sich auch keine Gedanken mehr machen, welche Wege Ihre Daten beim Versand im weltweiten Netz nehmen oder wer Ihre Daten auf ihrem PC ausspionieren könnte.

So verschlüsseln Sie richtig

Es gibt unterschiedliche Verfahren, Daten sicher zu verschlüsseln. Allen gemeinsam ist das Prinzip, dass die einzelnen Buchstaben und Ziffern der Daten mit Hilfe eines Schlüssels (einem nur der Besitzerin oder dem Besitzer bekannten Geheimnis oder Code) so oft vertauscht und durch andere Zeichen ersetzt werden, bis es praktisch unmöglich ist, ohne Kenntnis des Schlüssels (Geheimcodes) die Daten zu lesen. Äußeres Merkmal für die Wirksamkeit der Verschlüsselung ist die Länge des Schlüssels.

Sollen Daten sicher über Kommunikationsnetze an andere Personen übermittelt werden, sollten Verschlüsselungsverfahren eingesetzt werden, die mit Schlüsselpaaren arbeiten, einem öffentlichen und einem privaten. Und so funktioniert das: Ihren öffentlichen Schlüssel geben Sie über ein öffentliches Schlüsselverzeichnis allgemein bekannt, damit alle, die verschlüsselt Daten an Sie senden wollen, ihn zur Verschlüsselung nutzen können. Mit dem privaten Schlüssel, der immer nur bei Ihnen bleibt, können Sie diese verschlüsselten Daten dann wieder entschlüsseln und lesen.



Doch Vorsicht: Achten Sie auf Ihre Schlüssel. Sie sind der Zugang zu den Daten.

Passwörter

Passwörter dienen dazu, Nutzerinnen und Nutzern von Datenverarbeitungssystemen persönliche Rechte für die Verarbeitung von Daten zu geben und die Daten vor dem Zugriff Unbefugter zu schützen. Sie schützen beispielsweise Ihren Email- oder eBay-Account, Ihr Online-Konto oder Ihr persönliches PC-Profil. Passwörter sind die Schlösser an den Zugangstüren zu den Daten. Sie werden persönlich vergeben und sind demnach auch so zu behandeln, dass weitere Personen sie nicht erlangen oder ausspähen können.

Damit Passwörter ihren Zweck erfüllen und nicht leicht erraten oder ausgeforscht werden können, müssen sie bestimmten Rahmenbedingungen genügen. Sie müssen mindestens achtstellig sein und dürfen nicht aus einer zu einfachen Ziffern- und/oder Buchstabenkombination, aus einfach abzuleitenden Begriffen oder leicht zu erratenden Namen etwa von Angehörigen bestehen. Es sollte möglichst eine Kombination aus Buchstaben und Ziffern ohne erkennbare Gesetzmäßigkeit gewählt werden.

Um Passwörter geheim zu halten, dürfen sie nur dann eingegeben werden, wenn die Eingabe nicht beobachtet werden kann. Selbstverständlich sollten sie anderen Personen auch nicht mitgeteilt werden. Nach Möglichkeit sollten sie auch nicht aufgeschrieben und schon gar nicht unverschlüsselt auf der Festplatte hinterlegt werden. Um die Vertraulichkeit zu gewährleisten, sollten sie regelmäßig (spätestens nach drei Monaten) geändert werden.

Löschen von Daten ...

Sie wollen Ihren PC verkaufen, verschenken, zur Reparatur geben oder ihn einfach nur ausrangieren, weil er zu leistungsschwach geworden ist. Dabei möchten Sie natürlich nicht, dass andere Personen auf ihre gespeicherten Daten zugreifen können und sie eventuell missbräuchlich verwenden.

... aber richtig

Gespeicherte Daten auf dem PC zu löschen ist eine einfache Sache – wird oft gesagt. Hierzu bieten die Betriebssysteme Löschfunktionen an, die auf Tastendruck wieder Platz auf der Speicherplatte schaffen. Es ist jedoch ein weit verbreiteter Irrtum, dass die Daten mit den in den Betriebssystemen implementierten Löschfunktionen irreversibel gelöscht werden können. Es werden lediglich die bisher von den Daten genutzten Speicherbereiche wieder freigegeben, so dass der Plattenspeicher mit neuen Daten überschrieben werden kann. Da der PC aber seinen freien Speicher ohne Ihren Einfluss verwaltet, nutzt er ihn auch erst dann, wenn es ihm günstig erscheint. Bis dahin bleiben die Daten auf der Festplatte unversehrt erhalten. Wol-

len Sie dies vermeiden, müssen Sie spezielle Löschprogramme verwenden, die Festplatten mehrfach überschreiben. Nur dann können sie sicher sein, dass niemand Ihre persönlichen Daten unerlaubt nutzen kann.

Was ist zu tun ?

Besonders beim Verkauf, der Abgabe zur Reparatur, dem Austausch oder der Ausmusterung eines PCs oder anderer Speichermedien sollte darauf geachtet werden, dass nur noch die Daten gespeichert sind, deren Preisgabe oder Verlust kein Risiko bedeutet. Damit kann einem Missbrauch der persönlichen Daten effektiv entgegengewirkt werden.

Sollen nicht mehr funktionsfähige Festplatten mit personenbezogenem Speicherinhalt zur Reparatur gegeben werden, ist zu prüfen ob die gespeicherten Daten zuvor gelöscht werden sollen oder müssen. Händlerinnen und Händler erhalten von ihren Lieferfirmen in der Regel eine neue Festplatte nur im Austausch gegen das defekte Gerät. In vielen Fällen befindet sich jedoch die Lieferfirma im Ausland und das Schicksal der Festplatte und der darauf gespeicherten Daten ist ungewiss.

Denken Sie daran: Daten können nur mit speziellen Programmen gelöscht werden, die beispielsweise Festplatten mehrfach überschreiben und die Daten damit irreversibel löschen.

Sicherung von Geräteschnittstellen

Jeder Rechner verteilt seine Daten über Schnittstellen. Sowohl bei der internen Bearbeitung, als auch bei der Darstellung von Daten auf dem Bildschirm oder der Speicherung auf einer Festplatte, aber auch bei der Übertragung zu externen Geräten und Datenträgern erfolgt der Datentransport über spezielle Schnittstellen. Sollen die persönlichen Daten im eigenen Rechner geschützt bleiben und die Weitergabe oder der Empfang von Daten nur kontrolliert erfolgen, müssen alle Schnittstellen des Rechners bekannt sein. Nur wenn klar ist, auf welchen Wegen Daten verteilt und empfangen werden, können auch Vorkehrungen ge-

troffen werden, diese Wege und damit den Datenaustausch zu kontrollieren.

Jede Schnittstelle eines Rechners ist durch ihre physikalischen Eigenschaften und die möglichen Übertragungsarten in ihrem Grundverhalten festgelegt und für ihre Aufgaben optimiert. Doch für alle Schnittstellen gilt, dass festgelegt werden kann, ob sie aktiv oder inaktiv sein sollen und gegebenenfalls auch welche Funktionen erlaubt sein sollen. Dazu gehört beispielsweise die Möglichkeit, mittels zusätzlicher Hilfsprogramme wie Systemmonitore, Firewall und Virenscanner die Funktionen und den ordnungsgemäßen Ablauf überwachen zu lassen.

Die Tür zu den Schnittstellen immer schließen

Je nach Computer- oder Betriebssystem beginnt die Kontrolle der Schnittstellen bereits mit dem Einschalten des Rechners. Im sogenannten BIOS Setup werden Parallel-, Seriell-, USB-, Modem-, Audio-, LAN-, W-LAN-Schnittstellen, Festplattenanschluss, Tastatur, Maus und Monitor aktiviert und vorkonfiguriert. Daneben können über das Betriebssystem Treiber und Protokolle festgelegt werden und damit Umfang und Funktionen der Schnittstellen erweitert oder eingeschränkt werden. Viele Einstellungen können zusätzlich benutzungsspezifisch in unterschiedlichen Sicherheitsprofilen erfolgen.

Ein besonderes Augenmerk muss den Funk-Schnittstellen wie Bluetooth und W-LAN gelten. Sie bieten die Möglichkeit, praktisch unbemerkt auf Daten zuzugreifen und Manipulationen vorzunehmen. Funk-Schnittstellen bergen ein hohes Risiko in sich, da Angriffe auf die so angebundenen Rechner über Gebäudegrenzen hinweg möglich sind. Hiermit sollte überaus vorsichtig umgegangen werden. Die Standardeinstellungen sollten sofort überprüft werden, da diese meist auf eine offene Übertragung ausgerichtet sind.

Insgesamt ist anzuraten, offene Schnittstellen bewusst und kontrolliert zu verwenden. Um die größtmögliche Sicherheit zu erreichen, sollte die Leitlinie gelten: Alles, was nicht unbedingt für den Betrieb des Rechners benötigt wird, sollte gesperrt oder ausgebaut werden.

Einsatz von Sicherheitssoftware

Ein vorsichtiger, zurückhaltender Umgang mit dem PC ist allein nicht ausreichend, um die notwendige Sicherheit für die Unversehrtheit der persönlichen Daten zu erreichen. Hilfestellung bieten hier zusätzliche Programme, die in erster Linie Daten und Verbindungen zum Internet kontrollieren und überwachen, um das Eindringen schädlicher Programme und das Ausführen ungewollter Funktionen zu verhindern.

Angriffe aus dem Internet erfolgen in der Regel nicht gezielt auf einen bestimmten PC, sondern sie sind breit angelegt, um allgemein Schaden anzurichten. Sie sollen bewirken, dass ein PC die voreingestellten Funktionen nicht mehr korrekt ausführt und statt dessen die von der angreifenden Person geplanten Aktionen ausführt. Beispiele sind ungewollte Datenlöschungen auf dem PC oder die Anwahl kostenpflichtiger Angebote im Internet.

Mit Hilfe von Sicherheitssoftware können bekannte Angriffsmuster erkannt und Schaden stiftende Ausführungen verhindert werden. Dabei ist es unerlässlich, Programme zu verwenden, die stets auf dem aktuellen Stand sind, also auch neueste Varianten von Angriffen erkennen. Die Programme bieten hierzu in der Regel einen Online-Update an.

Für welche Bereiche gibt es Sicherheitssoftware?

- Aktuelle Virenschutzsoftware verhindert wirkungsvoll, dass schädliche Funktionen in den PC gelangen.

- Ein Anti – SPAM – Schutzprogramm bietet die Möglichkeit, unerwünschte Email auszusondern oder erst gar nicht anzunehmen.

- Ein Dialerschutz sorgt dafür, dass nicht unbemerkt unerwünschte und vielleicht auch teure Verbindungen ins Internet geschaltet werden.

- Anti-Spy-Software verhindert, dass der PC unbemerkt ausgeforscht werden kann.

- Software zur Verschlüsselung sorgt dafür, dass Daten nur von denjenigen gelesen werden können, die im Besitz des Schlüssels sind.

- Firewall-Software schränkt die Funktionen und Verbindungen für das Internet auf das bewusst festgelegte Maß ein.

- Kinder- und Jugendschutz-Software erlaubt es, Filter so zu setzten, dass unerwünschte Seiten im Internet nicht erreicht werden können.

Bewusstes Surfen im Internet

Das Internet ist die Kommunikationsplattform der Gegenwart. Den internationalen Durchbruch ermöglichte eine einheitliche Präsentationssprache namens HTML (HyperText Markup Language), die es erlaubt, multimediale Inhalte wie Bilder, Texte oder Musikstücke darzustellen. Die in HTML codierten Dokumente werden durch eine entsprechende Software, den Browser, auf den Benutzerrechnern interpretiert. Diese Software kann innerhalb eines Dokuments sowohl Text als auch Bilder und Grafiken darstellen.

Mit der Verbreitung des Internets wuchsen die Ansprüche an die Darstellungsvielfalt des Browsers, denen die Möglichkeiten von HTML bald nicht mehr genügen sollten. Mit Java wurde eine vom Browser unabhängige Programmiersprache entwickelt, die in einer als abgesichert geltenden Umgebung auf dem PC ausgeführt wird. Java ist nicht zu verwechseln mit Javascript, das in den Text einer HTML-Seite eingebunden werden kann. Die Ausführung von Java-Anwendungen ist an den Download oder die Initialisierung entsprechender Applets gebunden und kann somit erkannt werden. Dagegen ist die Ausführung bei Javascript nicht erkennbar, zumal Aktionen auslösende Ereignisse wie „onMouseMove“ vielfach unbekannt sind. Hier kann also ein beliebiger Programmcode auf dem PC ohne eigenes Zutun und eigene Kenntnis ausgeführt werden. Wird bei Java der Programmcode in einer gesicherten Umgebung ausgeführt, so ist bei Javascript und anderen aktiven Inhalten konzeptionell keinerlei Sicherheitsmechanismus berücksichtigt. Schaden stiftende Programme können sich unbemerkt Sicherheitslücken im

Betriebssystem zunutze machen, um Daten auszuspionieren, zu kopieren oder zu löschen.

Programme, die nicht direkt über den Browser angesprochen werden können, wie Acrobat-Reader oder Real-Player, werden über sogenannte Plug-ins - wörtlich übersetzt: Stecker - an die Browser-Software angeschlossen. Durch diesen Mechanismus gibt das Betriebssystem die Kontrolle an ein anderes Programm weiter

Einstellungssache

Moderne Browser bieten vielfältige Einstellmöglichkeiten, wie beispielsweise den Ausschluss von Plug-ins und Scripts oder die Nachfrage vor der Ausführung von Scripts. Auf keinen Fall sollten undifferenziert vorgegebene Sicherheitsstufen wie „Hohe Sicherheit“ übernommen werden, sondern eine selbstdefinierte Sicherheitseinstellung ausgewählt werden, die eine Anpassung an die individuellen Bedürfnisse ermöglicht.

Um den Surfvorgang zu beschleunigen, speichert der Browser jede Internetseite, die aufgerufen wird, in einem Speicherbereich des PC, dem sogenannten Internetcache. Cache-Daten ermöglichen die Rekonstruktion des Surfverhaltens. Hier ist Eigeninitiative gefragt. Wann immer es möglich ist, sollten die im Cache gespeicherten Daten gelöscht werden. Alle auf dem Markt befindlichen Browser bieten die Möglichkeit, diese in der Browser-Software meist als temporäre Dateien bezeichneten Daten automatisch zu bestimmten Zeitpunkten oder manuell zu löschen. Zu den ebenfalls im Cache gespeicherten Daten gehören auch die sogenannten Cookies. Dies sind kleine Textdateien, mit Merkmalen zur Reidentifikation. Diese Technik ermöglicht Anbieterinnen und Anbietern von Internetdiensten, soweit der entsprechende Cookie auf einem PC hinterlegt ist, das Surfverhalten auch über mehrere Sitzungen hinweg aufzuzeichnen und zu analysieren. Cookies sollten im Browser abgestellt werden oder zumindest durch den Cache regelmäßig gelöscht werden.

Email, aber sicher

Elektronische Post, oder auch Email, ist ein beliebtes Kommunikationsmittel. Ob privat oder geschäftlich, Emails sind schnell geschrieben und auch schnell versandt. Emails sind aber unsicher. Ist man sich bei der Postkarte noch bewusst, dass zumindest die Beschäftigten der Post die Urlaubsgrüße lesen können, sind die Risiken bei Emails viel höher. Emails müssen auf ihrem Weg durch das weltweite Internet viele Stationen passieren, an denen sie abgefangen, mitgelesen oder auch verändert werden können.

Risiken der Email-Kommunikation

Auf ihrem Übertragungsweg durchläuft eine Email verschiedene Computer des Internets, die in der Regel unterschiedlichen Betreibern (beispielsweise AOL, T-Online) zuzuordnen sind. Auf jedem dieser Server wird eine Kopie der Email so lange gespeichert, bis sie mangels Speicherplatz durch andere Nachrichten überschrieben wird. Damit existieren von einer Email eine Vielzahl von Kopien auf den Servern des Internets. Durch diese Zwischenspeicherung ist es leicht möglich, dass Emails auch von Unbefugten gelesen werden können. Sensible oder vertrauliche Informationen können so schnell in unbefugte Hände gelangen, wenn sie ungeschützt übermittelt werden. Wer eine Email erhält, kann zudem nicht sicher sein, dass der Inhalt der Email unverfälscht eingegangen ist oder gar frei von Viren ist. Wer die Möglichkeit hat, fremde Emails auf Servern zu lesen, ist auch in der Lage, deren Inhalte zu verändern. Ein weiteres Problem ist das unerkannte Löschen oder der Verlust von E-mails. Man kann sich nicht darauf verlassen, dass eine Email wirklich die Empfängerin oder den Empfänger erreicht. Sie könnte beispielsweise aufgrund technischer Probleme bei der Übertragung oder aufgrund eines Hackerangriffs verloren gehen. Aber nicht nur der Text einer Email kann verfälscht werden. Viel leichter ist das Fälschen der Absenderangaben. Der Absender, den das Mailprogramm zu einer eingegangenen Email anzeigt, muss nicht der wirkliche Absender sein.

Wie schütze ich meine Emails?

Es gibt verschiedene Möglichkeiten, sich vor den Risiken der Email-Kommunikation zu schützen. Um Emails vertraulich zu

behandeln, sollten die Inhalte verschlüsselt werden. Nur so kann verhindert werden, dass sie von Unbefugten gelesen werden können. Wird eine Email zusätzlich mit einer elektronischen Signatur unterschrieben, kann man sicher sein, dass sie auch wirklich von der Absenderin oder dem Absender stammt und unverändert eingegangen ist. Zudem sollten Email-Quittungen vereinbart werden, die den Empfang der Email bestätigen. Daneben sollte selbstverständlich ein aktueller Virenscanner vorhanden sein.

Persönliche Daten im Netz

Chats, Clubs, Foren, Internet-Shopping, Gewinnspiele, Musik und Klingeltöne. All das klingt sehr verlockend, besonders wenn es umsonst ist – scheinbar umsonst. Auch wenn alle diese Internetdienste „kostenlos“ angeboten werden, wird dennoch meist eine Gegenleistung verlangt – nämlich die Daten zur eigenen Person. Denn regelmäßig setzt die Nutzung dieser Dienste eine Registrierung voraus. Überlegen Sie deshalb genau, ob, wann und in welchem Umfang Sie Ihre Daten preisgeben wollen.

Was passiert mit den Daten ?

Sobald Daten im Internet preisgegeben werden, ist die vertrauliche Verwendung nicht mehr unbedingt gewährleistet. Die Firmen, die Teledienste anbieten, besitzen jetzt die Daten. Ihnen muss deshalb vertraut werden können, dass sie sich an geltendes Recht halten. Im Vorfeld ist daher darauf zu achten, ob die geforderten Daten zu Ihrer Person tatsächlich für die gewünschte Dienstleistung benötigt werden oder ob die Daten lediglich unter Vorwänden gesammelt werden und sie beispielsweise für Telefonwerbung, Werbe-SMS und Email-Aktionen verwendet werden sollen. Aber auch wenn die Daten grundsätzlich für die vorgegebenen Zwecke verwendet werden, können sie bei Einstellung ins Internet lange im Netz erhalten bleiben. Hierbei ist es leicht möglich, dass sich andere mit geeigneten Suchmaschinen informieren und ein Profil von Ihrer Person bilden.

Hinweise

Hier einige Hinweise für die Angabe persönlicher Daten im Internet:

- Verwendung von Spitznamen oder Phantasienamen (Superman, Madonna, Donald Duck usw.), Angabe des eigenen Namens nur soweit unbedingt notwendig

- Angabe nur der für den angebotenen Dienst notwendigen Daten; Verzicht auf die „freiwillige“ Angabe von Zusatzinformationen

- Hinterfragen, ob persönliche Angaben ins Internet gestellt werden

- Prüfung der Allgemeinen Geschäftsbedingungen: Es muss ausdrücklich geregelt sein, dass Daten nicht an Dritte weitergegeben werden.

Vorsicht! – Viele moderne Multimediageräte speichern persönliche Daten

Speichermedien befinden sich heutzutage in vielen Elektronikgeräten des alltäglichen Bedarfs wie in Mobilfunkgeräten, Memory-Sticks, PDAs, Digitalkameras, Video- oder DVD-Recordern oder digitalen Fotokopierern. Leuchten diese Funktionen bei digitalen Kameras noch allen ein – schließlich möchte man ja die Aufnahmen weiter verwenden - so fallen ähnliche Funktionen etwa bei Faxgeräten oder Kopierern, die die letzten versandten und empfangenen Faxe oder die letzten erstellten Kopien digital zwischenspeichern können, nicht mehr sofort ins Auge. Besonders hinzuweisen ist an dieser Stelle auf Handys, die - neben der mittlerweile weit verbreiteten Fotofunktion – beispielsweise auch sämtliche Kontaktadressen und die letzten eingegangenen Rufnummern bzw. SMS einschließlich Empfangszeiten speichern können.

All diese Beispiele zeigen, dass persönliche Daten und Bilder in großem Umfang auf modernen Multimediageräten gespeichert

werden und damit Personen in die Hände fallen können, die diese nicht unbedingt zur Kenntnis nehmen sollten.

Was Sie tun können

Bei allen modernen Geräten sollte in der Bedienungsanleitung sorgfältig nachgelesen werden, welche Daten dauerhaft bei den benutzten Einstellungen gespeichert werden. Wird diese Datenspeicherung in den Geräten von Ihnen nicht genutzt, sollten Sie sich darüber informieren, wie diese Funktionen abgestellt oder Datenlöschungen initiiert werden können.

Solange die Geräte die Besitzerin oder den Besitzer nicht wechseln oder nicht in unbefugte Hände geraten, sind diese Vorsichtsmaßnahmen vielleicht für Sie nicht so wichtig. Es bleibt aber zu bedenken, dass besonders die kleinen Handys und Kameras leicht verloren gehen können. In jedem Fall sollten Sie vor der Weitergabe oder Entsorgung dieser Geräte darauf achten, ob noch persönliche oder sicherheitsrelevante Daten gespeichert sind. Sollte dies der Fall sein, ist eine wirksame Löschung – die meist nur durch mehrfaches Überschreiben zu erreichen ist – unerlässlich.

Zu achten ist aber auch darauf, dass moderne elektronische Geräte in der Regel neben den großen Speicherkapazitäten außerdem einen schnellen, problemlosen Datenaustausch ermöglichen. Hiermit stellen sie aber auch ein hohes Sicherheitsrisiko dar, da ihr Einsatz, insbesondere wegen der geringen Größe, unbemerkt erfolgen kann. Mit ihnen können deshalb leicht Daten entwendet, nicht erwünschte Programme eingespielt, Systemeinstellungen geändert oder auch Viren eingeschleust werden. Auf den Einsatz dieser Geräte in der Nähe von Computern sollte deshalb ein besonderes Augenmerk liegen.