daten schutz

System- und Datensicherheit für Jedermann

Material zum Selbstdatenschutz – Teil 1
PC-Sicherheit für Einsteiger

Der Landesbeauftragte für den
Datenschutz Niedersachsen

Einleitung

Sie besitzen Ihren PC schon etwas länger? Sie hatten nie so recht Gelegenheit, sich mit Ihrem PC zu beschäftigen? Sie haben sich gerade einen neuen PC gekauft? Sie sind im Umgang mit dem System noch ein wenig unsicher? Sie wissen nicht so ganz genau, worauf Sie bei der Benutzung achten sollten? Hier finden Sie wichtige **Hinweise für den datenschutzgerechten Umgang mit Ihrem PC**. Schließlich wollen Sie doch auch, dass Ihre kleinen und großen Geheimnisse bei der Nutzung des Rechners geheim bleiben, oder?

Zielgruppe dieser Veröffentlichung sind **PC-Nutzer im privaten Umfeld**; sowohl Einsteiger als auch alle, die zwar schon länger einen PC besitzen, aber bislang nie so recht Gelegenheit hatten, sich mit ihrem Rechner etwas intensiver zu beschäftigen. In dieser Anleitung erklären wir Ihnen, wie Sie die größten Probleme vermeiden. Darüber hinaus gehenden professionellen Ansprüchen soll und wird hier nicht gerecht werden können; hierfür steht geeignetes Material an anderer Stelle zur Verfügung.

Um einer möglichst breiten Anwenderkreis anzusprechen, gehen wir davon aus, dass Sie auf Ihrem Rechner **Microsoft Windows XP Home** sowie zusätzlich das **Service Pack 2** installiert haben.

Wir wünschen Ihnen viel Spaß und Erfolg mit Ihrem PC und mit unseren Anregungen!

Inhalt

Rechtlos glücklich – Administrative und eingeschränkte Konten nutzen **1**

Wem gehören meine Daten? – Schreib- und Leserechte verwenden **2**

Sicher genug ist nur das Neueste! – Updates machen, zweifelhafte Software meiden **3**

Würmer, Wählgeister und Co. – Viren, Würmern, Dialern vorbeugen **4**

Wenn Software nach Hause telefoniert – Adware loswerden **5**

Scheunentore schließen - Firewall aktivieren und Windows Dienste kontrollieren **6**

Surfen ohne den unsichtbaren Dritten – ActiveX und ActiveScripting deaktivieren **7**

Festplatten, nicht nur sauber, sondern rein! – Internetspuren vermeiden und löschen **8**

Ganz der Alte bleiben – Das System wiederherstellen und Backups anlegen **9**

Schlüsselfragen – Paßwörter einsetzen **10**

Mein PC, meine Software! – Microsofts Internet-Programme durch Alternativen ersetzen **11**

Checkliste

Worauf Sie achten sollten (im Überblick) **12**

Herausgeber
Der Landesbeauftragte für den
Datenschutz Niedersachsen
Postfach 221
30002 Hannover
Tel (0511) 120-4500
Fax (0511) 120-4599
poststelle@lfd.niedersachsen.de
www.lfd.niedersachsen.de

Quelle: www.lfd.niedersachsen.de
→ Service-Angebote
→ Selbstdatenschutz
→ Downloads

erstellt: Juli 2005
aktualisiert: Juli 2006

Rechtlos glücklich – Administrative und eingeschränkte Konten nutzen

1

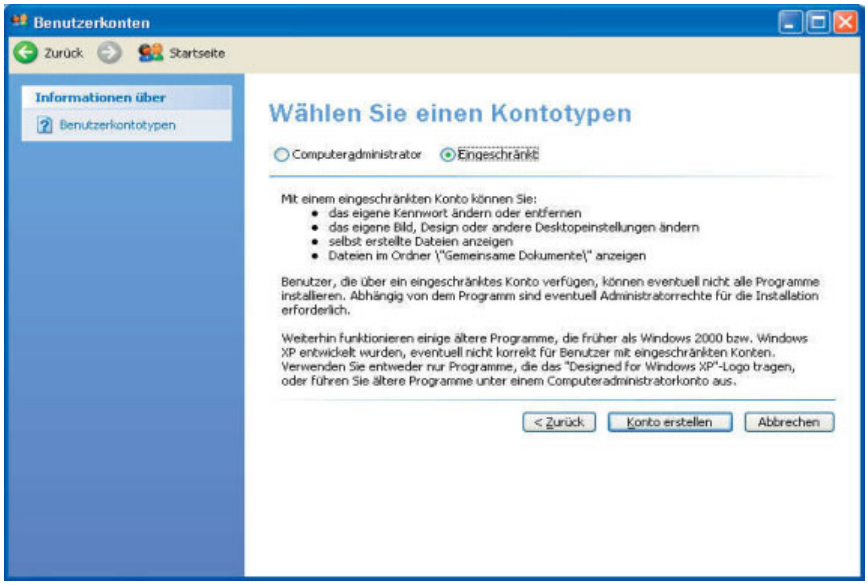
Sophie hatte ihren neuen PC gerade komplett eingerichtet: Die Bürosoftware war installiert, die Dokumente und die MP3s von der Festplatte des alten Rechners auf die des Neuen kopiert, kurz, alles hätte gut werden können. Wenn nicht ihr 11-jähriger Bruder Tim gewesen wäre. Ein Besuch im Internet, ein „geniales neues Spiel" installiert, und schon war alles dahin. Das hätte nicht passieren müssen – und zwar ohne Tim zu verbieten, das neue Gerät zu nutzen.

Das Problem

Per Voreinstellung haben unter Windows XP Home Edition alle neu angelegten Benutzerkonten lokale Administrationsrechte. Permanent unter einem solchen Benutzerkonto zu arbeiten, stellt ein unnötiges Sicherheitsrisiko dar, da im PC-Alltag (Word-Dokumente schreiben, im Internet Surfen, MP3s hören etc.) diese Rechte nicht benötigt werden. Wird jedoch versehentlich ein Schadprogramm ausgelöst, hat dieses alle Rechte, kann also auch tiefgreifende Veränderungen auf dem Rechner vornehmen. Darüber hinaus sind alle Benutzerkonten von Windows XP Home Edition standardmäßig nicht durch Kennwörter geschützt. Benutzerkonten, insbesondere solche mit Administrator-Rechten, sollten immer durch Kennwörter geschützt werden.

Die Lösung

Richten Sie über **Start → Systemsteuerung → Benutzerverwaltung** ein neues Benutzerkonto ein und geben diesem nur eingeschränkte Rechte. Das Standard-Konto sollte im Alltag genutzt werden. Erfordert eine Aktion administrative Rechte, was vor allem bei der Installation mancher Programme der Fall ist, lässt sich über **Startmenü → Abmelden** rasch und unkompliziert zu dem administrativen Konto wechseln und nach Abschluß der Aktion wieder in den „Normalbetrieb" zurückkehren. Programme, die nur mit administrativen Rechten zu nutzen sind (z. B. Nero Burning ROM) können durch Anpassung mit Herstellertools auch von Standard-Konten aus genutzt werden. Die erforderllichen Tools sind auf den Herstellerseiten in Internet kostenlos erhältlich.



Unter **Start → Systemsteuerung → Benutzerverwaltung** kann auch jedem Benutzerkonto ein Kennwort zugewiesen werden. Mit **Start → Abmelden** wird der Rechner dann für jeden gesperrt, der über kein Benutzerkennwort verfügt. Von der Funktion, einen Hinweis auf das Kennwort zu geben, sollte möglichst nicht Gebrauch gemacht werden, da diese Hinweise für jeden lesbar sind, der den Rechner einschaltet!

Gute Kennworte sind einerseits schwer zu raten und andererseits gut zu merken; nehmen Sie z. B einen Spruch, verwenden immer nur den 1., 2., 3. oder 4. Buchstaben (einschließlich Leer- und Satzzeichen) und ersetzen doppelte Buchstaben durch Kürzel. Das Ergebnis ist meist ein *sicheres* Kennwort! Beispiel: „Asterix sagt: Die spinnen, die Römer!" ergibt „As:_DsdR!"
Dieses Kennwort ist kaum zu entschlüsseln und lässt sich doch gut merken.

Wem gehören meine Daten? – Schreib- und Leserechte verwenden

2

Auf Sophies PC sind ein paar E-Mails an ihren Freund abgespeichert, die nun wirklich niemanden außer die beiden zu interessieren haben. Da Sophie ihr E-Mail-Passwort niemandem verrät und ihr kleiner Bruder Tim ein eigenes Benutzerkonto verwendet, wenn sie ihn auf ihrem PC spielen läßt, hat sich Sophie auf der sicheren Seite gefühlt. Bisher! Denn neulich lag doch tatsächlich eine dieser sehr privaten E-Mails ausgedruckt neben dem Rechner.

Das Problem

Bei einer Installation von Windows XP Home Edition wird standardmäßig als Dateisystem das sog. NTFS verwendet. Dieses Dateisystem unterstützt die Vergabe spezieller Rechte für einzelne Benutzer. Gelegentlich wird bei vorinstallierten Systemen aber noch das Dateisystem FAT32 eingesetzt, dass diese Unterstützung nicht bietet. In einer solchen Installation können alle Benutzer des Systems auf alle gespeicherten Daten zugreifen.

Die Lösung

Zugriffsrechte auf Dateien und Verzeichnisse lassen sich unter Windows nur im Dateisystem NTFS setzen. Daher sollten Sie zunächst prüfen, ob Sie bereits NTFS verwenden und falls nicht, Ihr Dateisystem konvertieren. Zur Prüfung klicken Sie im Arbeitsplatz mit der rechten Maustaste auf die Festplatte C:, und in dem Menü, das sich nun öffnet, auf **Eigenschaften.** Falls dort unter **Dateisystem** nicht NTFS stehen sollte, müssen Sie Ihr Dateisystem konvertieren. Führen Sie zum Konvertieren eines vorhandenen FAT oder FAT32-Datenträgers nach NTFS folgende Schritte aus: Klicken Sie auf **Start,** zeigen Sie auf **Alle Programme,** zeigen Sie auf **Zubehör,** und klicken Sie dann auf **Eingabeaufforderung.** Geben Sie an der Eingabeaufforderung Folgendes ein: **convert Laufwerkbuchstabe: /fs:ntfs.** Beachten Sie: Der Laufwerkbuchstabe bezeichnet das Laufwerk, welches Sie konvertieren möchten. Geben Sie folgenden Befehl ein, um Laufwerk **E** nach NFTS zu konvertieren: **convert e: /fs:ntfs**

Wenn Sie das Laufwerk konvertieren wollen, von dem aus das Betriebssystem gestartet wurde (normalerweise C:), erhalten Sie einen Hinweis, dass dies erst nach einem Neustart geschehen kann. Folgen Sie in diesem Fall einfach den Hinweisen und starten Sie Ihr PC-System neu.

Die Möglichkeit einer Beschädigung oder eines Datenverlusts ist zwar nur minimal, es wird jedoch dennoch empfohlen, dass Sie vor der Konvertierung eine Sicherung der Daten des Datenträgers durchführen, den Sie konvertieren möchten. Genauere Erläuterungen zu der Konvertierung von Dateisystemen finden Sie im Internet unter **http://support.microsoft.com/default.aspx?scid=kb;de;314097**

Technische Hintergrundinfos

In den „besseren" Dateisystemen können Benutzer nicht nur ihre Daten dauerhaft ablegen, sondern den Zugriff auf diese Daten auch nach verschiedenen Kriterien regeln. So kann zwischen dem Leserecht, dem Ausführrecht und dem Recht, die Daten zu verändern oder zu löschen, unterschieden werden. Leider wird dies unter XP Home nicht umfassend unterstützt. Andererseits ist diese Rechtevergabe auch kein absoluter Schutz für Ihre Daten. Von einem administrativen Benutzerkonto aus kann jederzeit in Lese- und Schreibrechte anderer Benutzer eingegriffen werden. Dieses ist für die Benutzer jedoch erkennbar. Ebenso kann der Inhalt der Festplatte von einem anderen Betriebssystem aus gelesen und verändert werden. Um diesen Mißbrauch auszuschließen, muß im BIOS des Systems das Starten von Betriebssystemen von externen Datenträgern wie z. B. CD, Diskette, USB-Stick verhindert werden. Nähere Hinweise hierzu finden Sie in der Bedienungsanleitung Ihrer PC-Hardware.

Sicher genug ist nur das Neueste! – Updates machen, zweifelhafte Software meiden

3

Sophies Rechner machte sich eines Tages selbständig. Er schaltete sich selbst aus und das immer wieder. Auch die E-Mail mit einem „Sicherheitsupdate", die irgend jemand an Sophie geschickt hatte, half nichts. Im Gegenteil. Für Sophie war der Fall klar: „Jetzt helfe ich mir selbst!" Mit Hilfe der Computerzeitschriften-CD eines Freundes war der PC erst einmal wieder lauffähig. Und Sophies Taschenkalender enthält nun an jedem 2. Dienstag im Monat einen Eintrag, der sie daran erinnert, ein Update durchzuführen …

Das Problem

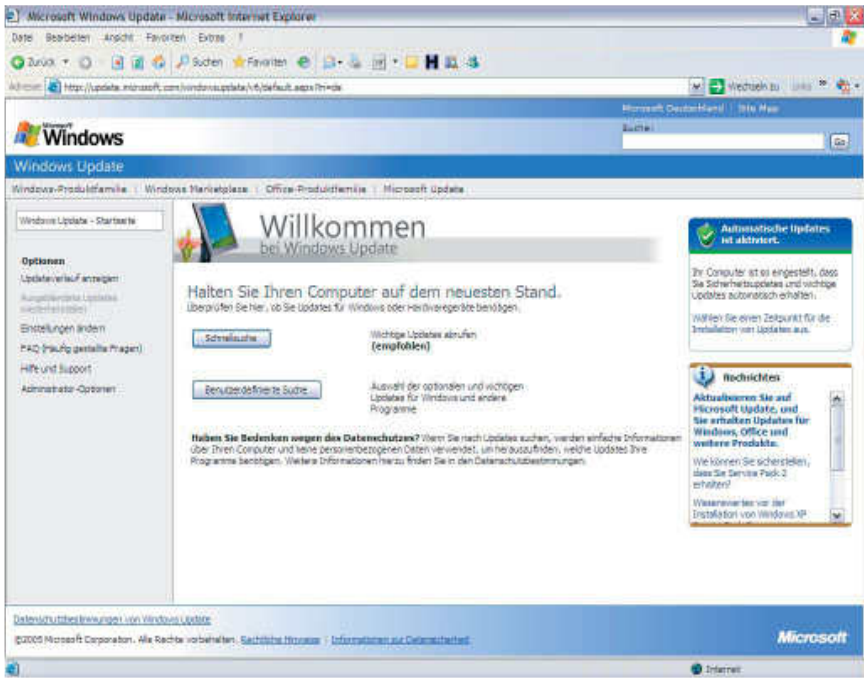
In großen Betriebssystemen wie Windows sowie in den mitgelieferten Browsern oder EMail-Clients werden regelmäßig neue Sicherheitslücken entdeckt. Wenn das betroffene System obendrein auch noch so verbreitet ist wie Windows, lässt Schadsoftware, die sich aufgedeckte Sicherheitslücken gezielt zu nutze macht, selten lange auf sich warten. Regelmäßiges Aktualisieren des Betriebssystems und seiner Komponenten ist die einzige Erfolg versprechende Konsequenz.

Die Lösung

Am zweiten Dienstag eines jeden Monats (wegen der Zeitverschiebung ist das hier oft erst am darauffolgenden Mittwoch), bringt Microsoft neue Updates zu seinen Windows-Betriebssystemen heraus. Es ist dringend zu empfehlen, zu diesem Zeitpunkt die Site **http://windowsupdate.microsoft.com** aufzusuchen und die empfohlenen Sicherheits-Updates zu installieren!

Über das Sicherheits-Center oder das „Automatische Update" lässt sich die Suche nach den benötigten Updates automatisieren. Microsoft-Updates liegen gelegentlich auch Computerzeitschriften als Heft-CDs bei. Wer keine Heft-CD bekommt und sich alle Updates über eine ISDN-Verbindung herunterladen muss, wird beim ersten Besuch dieser Site eventuell mehrere Stunden benötigen. Dennoch ist das vollständige Installieren mindestens aller „Service Packs" und „sicherheitskritischen Patches" dringend anzuraten.

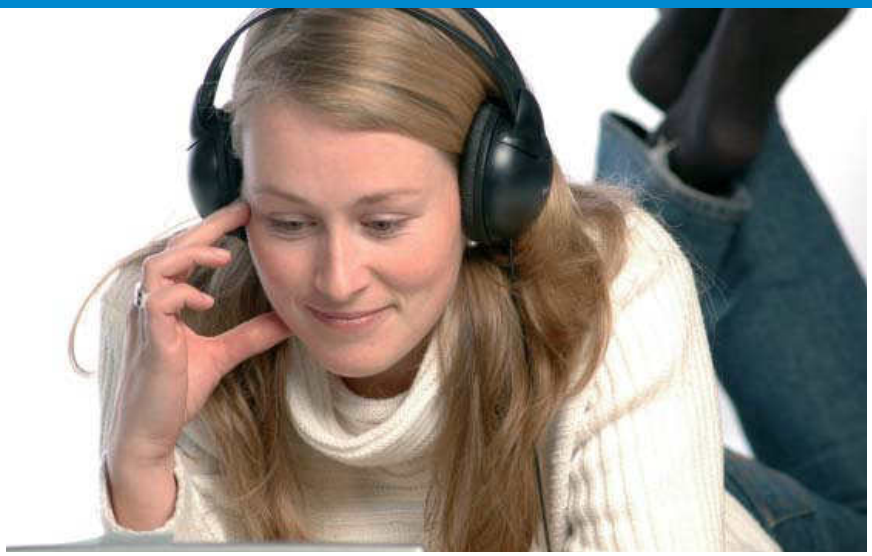
Sinngemäß gilt dieser Hinweis auch für jede andere Software, die man auf seinem PC einsetzt. Nicht die Mühe zu scheuen, gelegentlich nach Updates zu suchen, lohnt sich doppelt. Neben der Beseitigung von Sicherheitslücken dienen Updates auch der qualitiven Verbesserung von Produkten. Updates sind auf der Website des jeweiligen Herstellers meist rasch zu finden; **Updates werden aber nie per E-Mail-Attachment verschickt!** Generell sollten Programme zweifelhafter Herkunft nicht ausgeführt oder installiert werden.



Würmer, Wählgeister und Co. – Viren, Würmern, Dialern vorbeugen

4

„Software gegen Viren und gegen Dialer – das ist ja wohl selbstverständlich", denkt sich Sophie. Aber dafür mehrere neue Programme installieren, die den Rechner wieder langsamer machen und auch noch Geld kosten?



Das Problem

Viren, Würmer und Dialer gehören zu den bekanntesten Gefahren für die Sicherheit des PCs. Der „Übertragungsweg" sind heute meistens via Internet heruntergeladene und leichtfertig (oder gar ohne Wissen des Benutzers) ausgeführte Programme. Daneben dürfen aber auch andere Wege nicht vernachlässigt werden; „Ansteckungsgefahr" droht auch auf Netzwerk-Parties oder bei der Durchsicht von unbekannten CDs.

Die Lösung

Falls der eigene Windows-PC noch nicht über Virenschutzsoftware verfügt (bei Rechnern mit Modem- oder ISDN-Anschlüssen zusätzlich Dialerschutzsoftware), ist es notwendig, möglichst bald eine solche zu installieren. Kostenlos erhältlich ist zum Beispiel AntiVir PE Classic **(www.free-av.de/).** Die Installation und Inbetriebnahme dieses Programms sind weitgehend selbst erklärend.

Zu beachten ist, dass die Erkennungsdaten des Programms regelmäßig, am Besten täglich, aktualisiert werden müssen! Keine Sorge, anders als es das Programm vorschlägt, muß nicht nach jeder Aktualisierung sofort ein zeitraubender Scan der gesamten Festplatte durchgeführt werden. Solche Scans können gelegentlich in Pausen durchgeführt werden, in denen nicht am Rechner gearbeitet wird. Eine grundlegende Sicherheit ist jedoch bereits dadurch gegeben, dass der im Hintergrund laufende Virenscanner alle Dateien prüft, sobald sie aufgerufen werden.

Wenn Sie für den Internetzugang einen ISDN Anschluss nutzen, sollten Sie sich auch der Gefahren durch Dialer bewußt sein. Diese kleinen Programme installieren sich meist selbsttätig und oft ungewollt nach einem schnellen Klick auf ein Dialogfeld im Webangebot verschiedenster Internetseiten. Ziel ist immer, über die Anwahl bestimmter *teuerer* Telefonnummern Geld von Ihnen zu erhalten. Wenn Sie die angebotene Dienstleistung, z. B. Nutzung von Herstellerservice für PC-Systeme, tatsächlich kostenpflichtig in Anspruch nehmen wollen, ist diese Abrechnungsmethode so gut wie jede andere. Oft aber wird versucht, Sie mittels eines Dialers zu einer teuren Einwahl ins Internet zu zwingen, um unberechtigt Geld zu verdienen. Umfassende Informationen zu diesem Thema finden Sie z. B. unter **http://www.dialerschutz.de/ .**

Darüber hinaus trägt das eigene Verhalten ganz wesentlich zum Schutz vor Schadsoftware bei. Schon wenn nicht jeder Mail-Anhang, nicht jedes PopUp-Fenster, nicht jede Klick-Box einfach unbedacht angeklickt wird, lässt sich Schaden vermeiden. Prüfen Sie stets, ob Sie den Mailabsender/Webanbieter kennen, ob Sie ihm vertrauen können und ob er Ihnen ein Programm zusenden würde. Im Zweifel fragen Sie nach! Mehr Sicherheit können Sie auch mit der *richtigen* Konfiguration Ihres Mail-Programms erreichen; sehr gute Erläuterungen und intensive Hilfestellung dazu finden Sie bei Heise online unter **http://www.heise.de/security/dienste/emailcheck/ .**

Technische Hintergrundinfos

Die digitalen Schädlinge versuchen sich selbst zu verbreiten und können heute sogar ohne Programmiererfahrung mit Baukastensystemen erstellt werden. Daher verbreiten sich heute täglich neue Varianten. Nur gelegentlich aktualisierte Virendatenbanken bzw. nur ein Scannen aller Dateien des Systems reicht angesichts dieser Bedrohung nicht mehr aus.

Von einem Virenscanner ist heute zu erwarten, dass er

a) die regelmäßige Aktualisierung der Datenbank, anhand welcher er Viren erkennt, unterstützt;

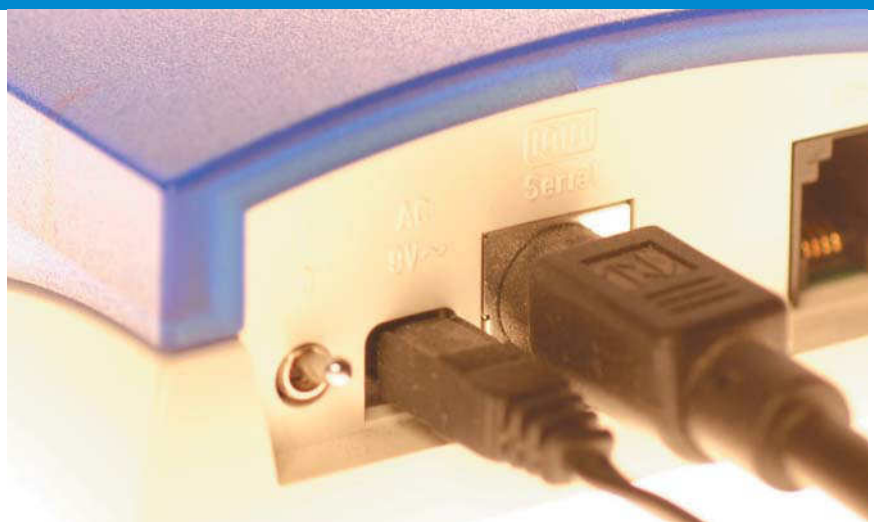
b) nicht nur „on demand", sondern „on access", das heißt bei jedem Dateizugriff des Systems, die jeweilige Datei automatisch vor dem Öffnen untersucht;

c) möglichst auch Dialer abwehrt, d.h. Programme, deren Schadfunktion darin besteht, gegen den Willen des Benutzers teure Wählverbingungen über ISDN oder Modem herzustellen.

Wenn Software nach Hause telefoniert – Adware loswerden

5

Die neue Internet-Software, die sich Sophie installiert hatte, war super – bis auf das Werbebanner. Wo das bloß herkam? „Ein Programm aus den USA, das deutschsprachige Werbung anzeigt?“ Dieses Programm schien eindeutig mehr über Sophie zu wissen, als sie von sich aus Preis gegeben hätte. Und wenn es Sophies Sprache kennt, was weiß es dann noch alles über sie?



Das Problem

Viele Programme, besonders häufig sogenannte Freeware und Shareware, finanzieren sich durch Marketingprogramme. Diese werden ungewollt zusammen mit der eigentlichen Anwendung installiert. Im harmlosesten Fall wird eine Werbeanzeige aus dem Internet geholt und auf dem heimischen Bildschirm eingeblendet. Nicht selten jedoch handelt es sich um Programme, die das Benutzerverhalten analysieren und diese Daten (z. B. Adressen angesurfter WWW-Seiten) unverschlüsselt übers Internet an den Softwarehersteller schicken. Auch wenn in den einschlägigen Vertragsbedingungen regelmäßig angegeben wird, dass solche Daten nur in anonymisierter Form statistisch ausgewertet werden, kann ihr Inhalt sehr individuell sein, und somit auch rückführbar auf die Person, von der sie stammen.

Die Lösung

Hilfe gegen derartige kleine Spione (Spyware) bieten eine Reihe von Programmen, die das eigene System durchsuchen und ungeliebte Spione aufspüren. Beispielsweise läßt sich unter **www.lavasoft.de/support/download/** das Programm Ad-aware kostenlos herunterladen. Im Anschluß an die Installation läßt sich das Programm leicht aufrufen. Das einmal installierte Programm sollte gelegentlich aktualisiert und erneut gestartet werden – beispielsweise, wenn neue Software installiert wurde, die solche unerwünschten Dateien enthalten könnte.

Viele der bekannteren Programme dieser Art können erkannt, angezeigt, und in einem zweiten Schritt entfernt werden.

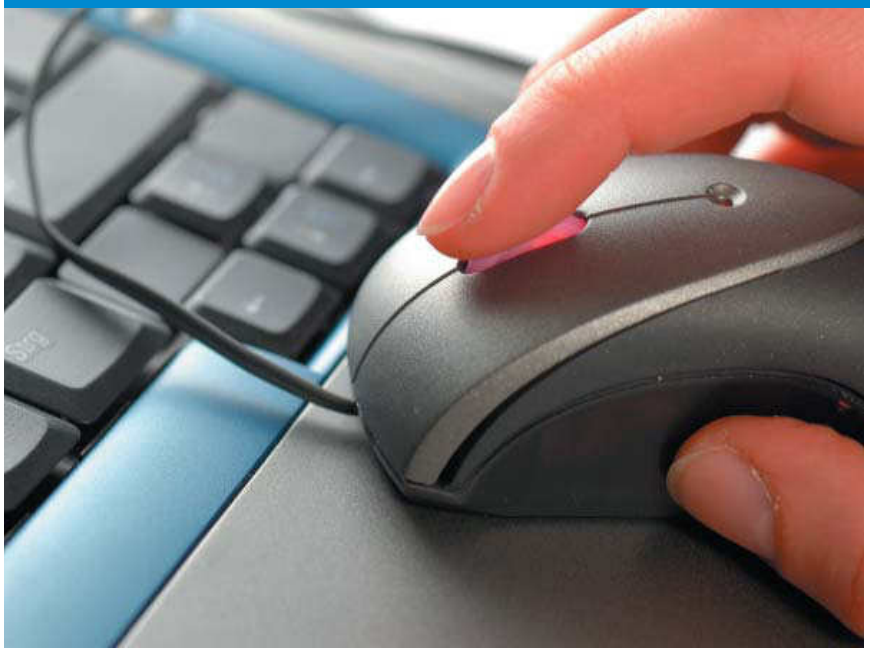
Gegen ein allzu „gesprächiges“ Betriebssystem hilft z.B. ein weiteres kostenloses Programm: XP-Antispy.
Informationen und downloads nur unter **www.xp-antispy.org**.

Ob auf dem Rechner Programme laufen, die Verbindungen nach draussen offen halten, können Sie zusätzlich mit dem Netzwerk-Check unter **www.heise.de/securtity/dienste/portscan** überprüfen.

Ein einfacher Klick auf „Start“ durchsucht nun die Festplatte nach Dateien, die ohne Kontrolle des Benutzers Daten übers Internet verschicken oder abrufen.

Scheunentore schließen - Firewall aktivieren und Windows Dienste kontrollieren

6



Nachdem Sophie endlich mal wieder ein Update ihres Antivirenprogramms vorgenommen hatte, war der Schreck groß: „Trojanisches Pferd auf Laufwerk C: gefunden"! Sophie ist klar: Solange sich dieses unerwünschte Pferd auf ihrem Rechner befunden hat, wäre es für jeden möglich gewesen, übers Internet ihren Rechner zu kontrollieren, Passworteingaben mitzulesen und anderes mehr.
Aber wie hätte man das vermeiden können?

Das Problem

Trojanische Pferde sind eine besonders gefährliche Spezialform von Schadsoftware. Sie dienen im wesentlichen dazu, Daten auszuspähen und Dritten über Netzwerk oder Internet unkontrollierten Zugang zum eigenen Rechner zu verschaffen.
Ähnliche Schwierigkeiten können auch Dienste des Betriebssystems verursachen, wenn diese permanent im Hintergrund laufen, Sicherheitslücken aufweisen und aus dem Internet erreichbar sind. Über solche Schwachstellen sind in den vergangenen Jahren schon viele unerwünschte „Gäste" auf die Systeme gelangt.

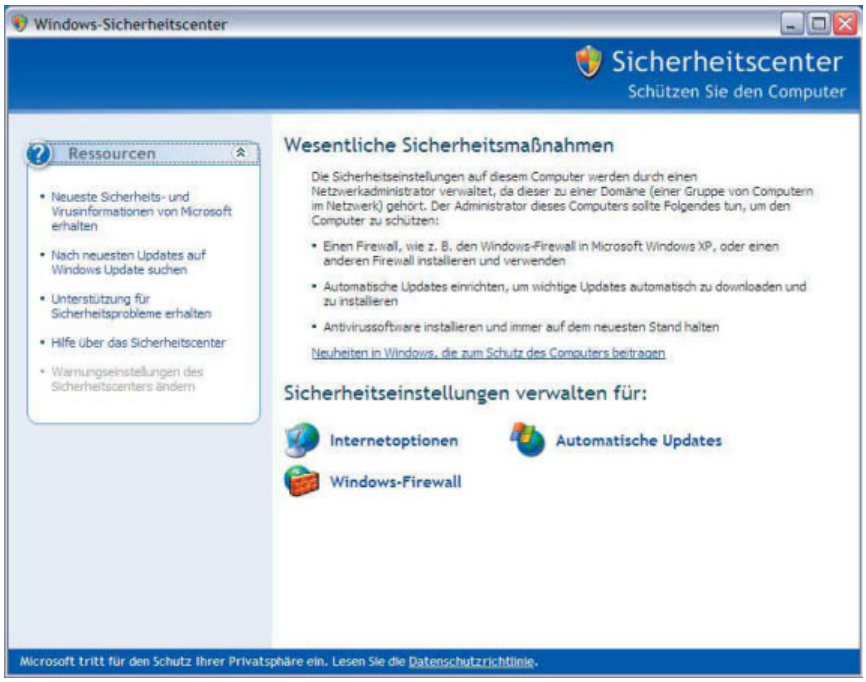
Technische Hintergrundinfos

Eine Firewall hat in erster Linie die Aufgabe, Netzzugänge abzusichern. Hierfür stehen Möglichkeiten auf unterschiedlichen Netzebenen zur Verfügung; eine Basiskomponente ist der sog. Adress- und Portfilter.
Dabei werden die beteiligten Netzwerkadressen und die genutzten Dienste, die über die Ports zu erreichen sind, überwacht. Zugelassen wird eine Verbindung nur dann, wenn eine Regel dies erlaubt.

Fortgeschrittene Nutzer können zusätzlich überlegen, welche der im Betriebssystem aktivierten Hintergrunddienste überhaupt benötigt werden; für den Nutzer überflüssige Dienste sollten deaktiviert werden, um eine mißbräuchliche Nutzung auszuschließen. Hilfreich für diese Arbeiten können Werkzeuge wie das Programm „win32sec" sein, dass kostenlos von **www.ntsvcfg.de/easy** heruntergeladen werden kann. Ein ähnliches Programm ist unter **www.ntsvcfg.de** ebenfalls kostenlos zu erhalten. Ebenso mitgeliefert werden weitere Informationen zu diesem Thema.

Die Lösung

Es lohnt sich, doppelt vorzusorgen und neben dem Virenschutz auch die aktiven Internetverbindungen des eigenen Rechners zu kontrollieren. Die in Windows XP integrierte Internetverbindungsfirewall ist durchaus geeignet, unerwünschte Verbindungsversuche aus dem Internet wirksam abzuwehren. Seit ServicePack 2 ist diese Firewall beim Systemstart standardmäßig aktiviert; Ihre Verwaltung ist in das Sicherheits-Center integriert.



Surfen ohne den unsichtbaren Dritten – ActiveX und ActiveScripting deaktivieren

Nach dem ersten Ausflug ihres kleinen Bruders Tim ist Sophie misstrauisch geworden: Allein der Besuch bestimmter Websites scheint ihren Browser, ja ihren ganzen Rechner verändert zu haben. „Als Selbstbedienungsladen für wildgewordene Internet-Anbieter war mein Rechner aber eigentlich nicht gedacht", denkt sich Sophie. Aufs Internet ganz zu verzichten kommt nicht in Frage, so viel ist klar …

Das Problem

Ein schweres Risiko beim Surfen im Internet stellen die zahlreichen längst bekannten, jedoch durch Microsoft nicht zeitnah reparierten Sicherheitslöcher des Browsers Internet Explorer dar. Wie weiter unten beschrieben, lässt sich im Alltag zwar gut auf den Internet Explorer verzichten, zumindest für Microsofts „Windowsupdate" ist er jedoch unverzichtbar: Gerade beim Windowsupdate kommt ActiveScripting zum Einsatz, eine Technik, die man sonst sicherheitshalber ausschalten sollte.

Die Lösung

Im Internet Explorer lassen sich ActiveScripting und Co. einfach abschalten. Im Menü **Extras → Internet-Optionen → Sicherheit → Stufe anpassen → Scripting/Active Scripting → ActiveX-Steuerelemente und Plugins** zwei Haken setzen: „ActiveX-Steuerelemente und Plugins ausführen, die für Scripting sicher sind" *Deaktivieren* und „ActiveX-Steuerelemente und Plugins ausführen" *Deaktivieren*.
Bei grundsätzlich deaktiviertem ActiveScripting wird man von der Windowsupdate-Site darauf hingewiesen, wie man ausgewählten Sites diese Funktion „erlauben" kann.

Weitere Hinweise und Erläuterungen zur sicheren Browser-Konfiguration einschließlich guter Testmöglichkeiten finden Sie auf Heise online unter **http://www.heise.de/security/dienste/browsercheck/.** Sollten nach entsprechenden Einstellungen auf einigen Internetseiten bestimmte Funktionen nicht mehr zur Verfügung stehen, muss letztlich jeder Nutzer für sich entscheiden, ob er die Nutzung gerade dieses Internetangebots einer sonst gegebenen höheren Sicherheit vorzieht. Für etwas fortgeschrittene PC-Nutzer gibt es darüber hinaus Hilfsmittel, den Internet-Explorer je nach Nutzung individuell zu konfigurieren. Fündig werden Sie bei Heise online unter **http://www.heise.de/ct/ftp/projekte/iecontroller/.**

Festplatten, nicht nur sauber, sondern rein! – Internetspuren vermeiden und löschen

8

Sophie war stolz auf sich. Der zweite PC fürs Arbeitszimmer war ein echtes Schnäppchen, 190 € bei Ebay, mit allem drum und dran. Sogar die Software war schon komplett installiert. Natürlich hatte der Vorbesitzer nur die Programme draufgelassen, keine eigenen Word-Dokumente oder ähnliches. Als Sophie aber das erste mal mit dem neuen PC ins Internet ging, staunte sie nicht schlecht. Kaum hatte sie die ersten beiden Buchstaben einer Website-Adresse eingetippt, schlug ihr der Internet Explorer in alphabetischer Reihenfolge ein paar Porno-Seiten vor, die mit dem gleichen Buchstaben beginnen. „So viel wollte ich über den Typen bei Ebay gar nicht wissen", stöhnte Sophie.

Das Problem

Um das Surfen komfortabler zu gestalten, speichern Browser für einen gewissen Zeitraum alle abgerufenen Adressen und Dateien. Seiten müssen daher nicht jedesmal komplett neu aus dem Internet geladen werden und die Adresse einer Seite kann bereits vorgeschlagen werden, nachdem die ersten paar Buchstaben ins Adressfenster des Browsers getippt wurden. Dieses lange *Gedächtnis* kann auch stören – daher sieht der Browser die Möglichkeit vor, das Gedächtnis künstlich zu „verkürzen" oder auch schlagartig zu leeren.

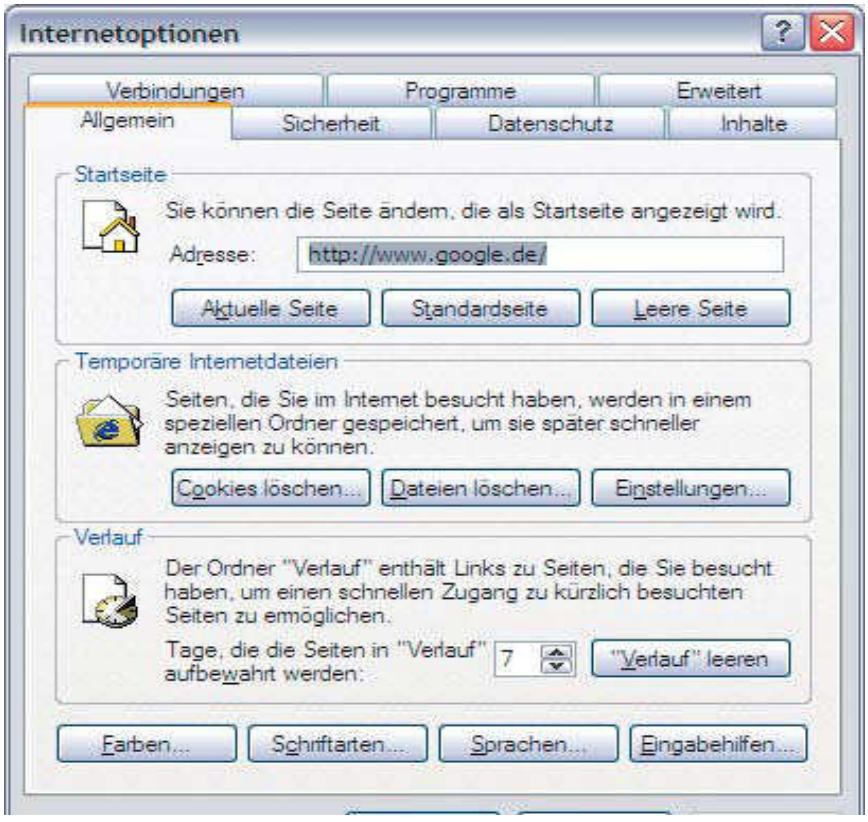
Die Lösung

Die Abbildung zeigt das Internet-Explorer Fenster „Internetoptionen" (Menü „Extras"). Verlaufsordner, temporäre Internetdateien und Cookies lassen sich hier per Mausklick löschen, ferner lässt sich die Aufbewahrungsdauer der Verlaufsdaten einstellen. Doch der Augenschein trügt. Nicht nur das Löschen des Verlaufsordners geschieht hier nicht rückhaltlos, sondern auch die Cookies und temporären Dateien sind nicht so ohne weiteres wegzubekommen. Hierbei handelt es sich um eine spezielle Problematik des Internet Explorers.

Technische Hintergrundinfos

Bei Cookies handelt es sich um kleine Textdateien, die von einer Website (oder einer Werbeanzeige auf einer Website) in einem Dateiordner des Browsers hinterlassen werden. Cookies sind keine Programme, die von sich aus Informationen senden oder empfangen können. Sie bieten einer Website lediglich die Möglichkeit, einen Besucher wiederzuerkennen. Hier sind zwei Fälle zu unterscheiden: Das Sitzungscookie dient dazu, innerhalb eines zeitlich begrenzten Besuchs den Betrachter der Site wiederzuerkennen. Der andere Fall sind langfristig haltbare Cookies. Diese können ebenfalls einen spezifischen Nutzen für den Verbraucher haben, z. B. wenn ich beim Aufrufen der Amazon-Site direkt als Kunde begrüßt werde und ohne aufwändige Anmeldeprozeduren per Mausklick Bücher bestellen kann.

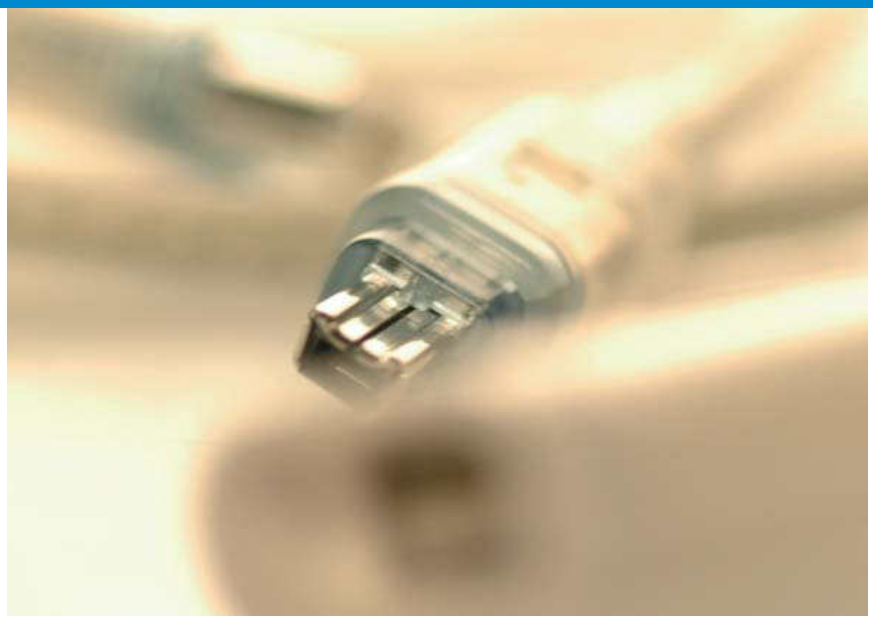
Anders sieht es aus mit Werbetreibenden wie DoubleClick: Ohne dass es hier einen erkennbaren Nutzen für den Benutzer gibt, kann über das Cookie verfolgt werden, wann er auf welcher Seite eine DoubleClick-Anzeige eingeblendet bekam. Der differenzierte Umgang mit verschiedenartigen Cookies wird inzwischen von allen üblichen Browsern unterstützt. Die Einstellungen erreichen Sie im Internet Explorer unter **Extras → Internetoptionen → Datenschutz → Erweitert** .



Ganz der Alte bleiben – Das System wiederherstellen und Backups anlegen

9

„Könnte ich doch noch einmal ganz von vorne anfangen“, seufzt Sophie, nachdem sie die neu installierte Multimedia-Software endgültig satt hatte. Der einst so flotte Gigahertz-Rechner war unsäglich langsam geworden. Trotz Änderung werden die MP3-Dateien immer noch von dem neuen Programm geöffnet, und als sie das Programm deinstalliert hatte, waren die Probleme trotzdem nicht behoben.

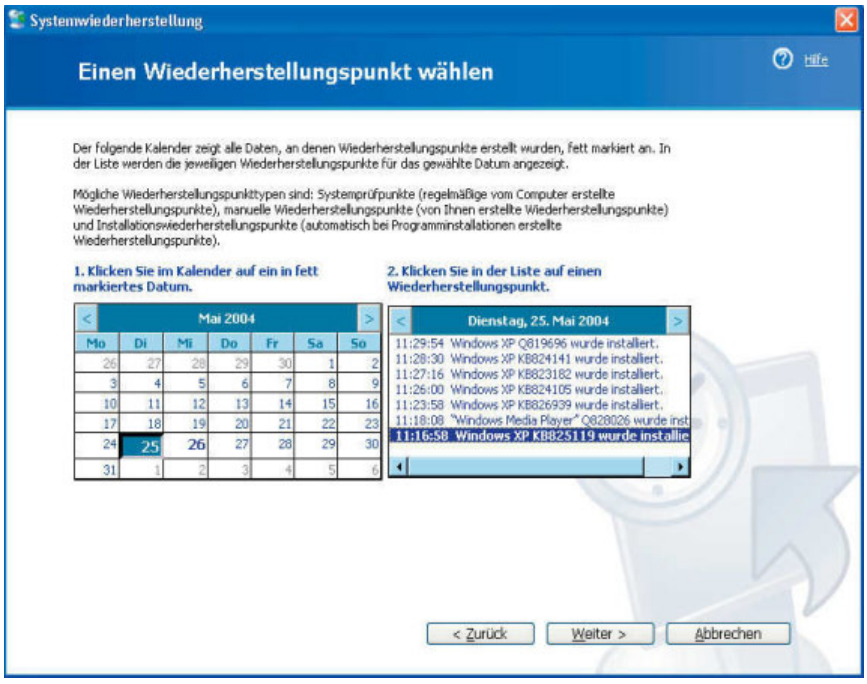


Das Problem

Neu installierte oder aktualisierte Programme, neu konfigurierte Software oder andere Veränderungen am Rechner können dessen Stabilität gefährden. Ob nun durch Hardware- oder Softwareprobleme, schlimmstenfalls können eigene Daten auf der Festplatte auch völlig zerstört werden.

Die Lösung

Man braucht keine Angst davor zu haben, durch Updates eine funktionierende Konfiguration des Systems zu zerstören. Windows XP erzeugt automatisch Wiederherstellungspunkte. Als Administrator lässt sich ein selbst gewählter Ausgangszustand des Windows-Systems unter **Startmenü → Systemsteuerung → Verwaltung → Systemwiederherstellung** wiederherstellen. Lässt sich das System nicht mehr booten, wird automatisch die Wiederherstellung der Konfiguration zum Zeitpunkt vor der Installation des Updates angeboten. Um einzelne Programme loszuwerden, sollte man vor einer Systemwiederherstellung jedoch unbedingt eine simple Deinstallation des Programms ausprobieren.



Von persönlichen Daten, die schwer zu ersetzen sind, wie z. B. eigene Texte, E-Mails oder Programmkonfigurationen sollten regelmäßig Backups erstellt werden. Diese Kopien sollten sinnvollerweise räumlich getrennt vom Rechner aufbewahrt werden. Dazu bietet es sich an, einmal herauszufinden, welche Ordner auf dem Rechner derartige persönliche Daten enthalten. Diese Ordner werden dann in regelmäßigen Abständen auf eine wiederbeschreibbare CD/DVD kopiert.

Trotz und neben allen weiteren Sicherheitsmaßnahmen gelten Backups nach wie vor als Sicherheitsmaßnahme Nr. 1, da sie sehr einfach, effektiv und präventiv mögliche Beschädigungen persönlicher Daten zu vermeiden helfen.

Schlüsselfragen – Paßwörter einsetzen

Sophie zögerte ein paar Sekunden, als sie sich für den neuen Musik-Download-Dienst ein neues Passwort ausdenken sollte. Klar: „schnuffi“, der Name des Kaninchens, das sie als Kind hatte. Nur, jetzt schoss ihr durch den Kopf: An wie vielen Stellen hatte sie dieses Passwort schon verwendet? Das war das Passwort für ihr privates E-Mail-Konto, das Passwort für den PC am Arbeitsplatz, das Passwort für diesen anderen Download-Dienst … Sophie wurde ein wenig schwindelig bei dem Gedanken, dass jemand dieses eine Passwort herausfände, das ja, ehrlich gesagt, auch nicht allzu kompliziert war. Aber wie, bitteschön, hätte sie sich neben den beiden PINs für ihr Bankkonto und ihre Kreditkarte noch mehrere komplizierte Passwörter merken sollen?

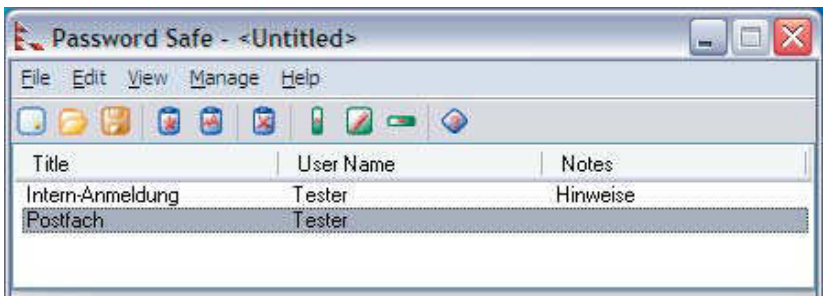
Das Problem

Die Digitalisierung hat dazu geführt, dass wir uns in vielen Bereichen PINs und Passwörter merken müssen. Gerade am PC und im Internet, wo Passwörter oft selbst gewählt werden müssen, fühlen sich viele überfordert und sehen keinen anderen Ausweg, als einfache, aber unsichere Passwörter zu wählen, sich Passwörter zu notieren oder dasselbe Passwort für unterschiedliche Zwecke einzusetzen. Solche Methoden bergen große Risiken, die sich mit einfachen Hilfsmitteln und geringem strategischem Aufwand vermeiden lassen.

Die Lösung

Das Programm Passwordsafe zum Beispiel speichert je nach Bedarf zahlreiche verschiedene Passwörter und verschlüsselt sie mit einem einzigen weiteren Passwort. Was auf den ersten Blick als zusätzliche Verkomplizierung erscheint, erleichtert tatsächlich den Umgang mit den Passwörtern. Passwordsafe kann auf Wunsch sehr sichere Passwörter erzeugen. Diese müssen nicht mehr auswendig gelernt werden – es reicht, ein Zugangspasswort zum Programm selbst sowie das Login- Passwort zum Rechner zu kennen.

Das quelloffene Programm ist kostenlos unter **passwordsafe.sourceforge.net** erhältlich. Am selben Ort findet sich ebenfalls eine herunterladbare deutsche Version der Hilfedatei, die Hinweise zum Umgang mit diesem sehr einfach bedienbaren Programm bietet. Besonders wichtig, um im Notfall nicht schlagartig alle gespeicherten Passwörter zu verlieren: Über **Manage → Make Backup** können regelmäßig Sicherheitskopien von der Passwortdatenbank erstellt werden.



Geheimhalten für Fortgeschrittene

Nicht nur Passwörter sollten verschlüsselt werden. E-Mails, die unverschlüsselt verschickt werden, sind wie Postkarten: Viele, an die sich die E-Mail nicht richtet, können relativ leicht einen Blick hineinwerfen. Das Internet lässt sich nicht so umbauen, dass dies nicht mehr möglich wäre – aber zwischen Absender und Empfänger lässt sich ein Verschlüsselungssystem einsetzen, dessen Software, einmal eingerichtet, kinderleicht zu bedienen ist. Dieses System ist sogar so sicher, dass es nicht einmal von einem Geheimdienst geknackt werden könnte. Die Rede ist von PGP/GnuPG. Einen schnellen Einstieg in E-Mail mit der quelloffenen und kostenlosen Software GnuPG bietet **www.gnupp.de** .
Übrigens, mit GnuPG lassen sich auch Dateien und ganze Ordner auf der eigenen Festplatte unknackbar sicher verschlüsseln.

Mein PC, meine Software! – Microsofts Internet-Programme durch Alternativen ersetzen

11

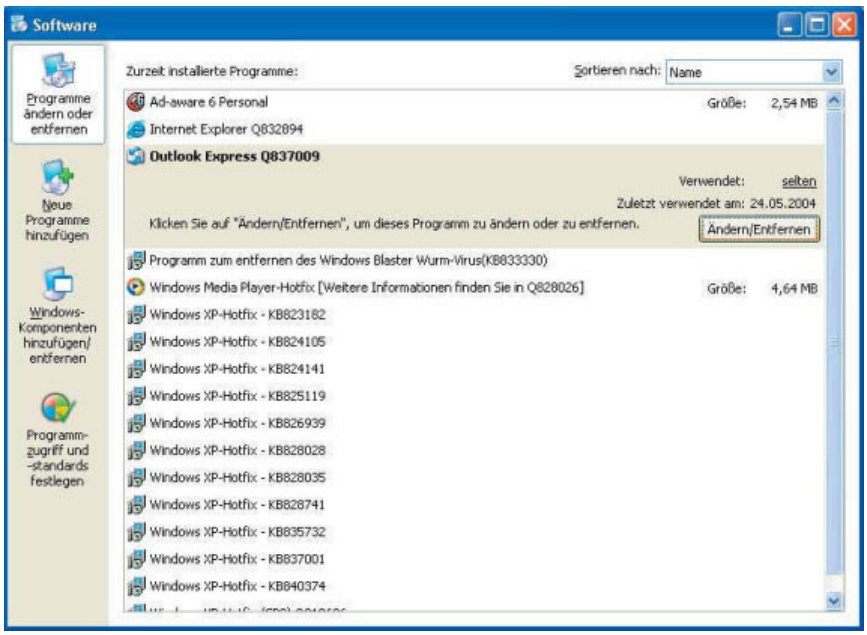
Nach dem letzten Eingriff in die Innereien des Internet Explorers (Browsereinstellungen) hat Sophie die Nase voll. „Es muß doch möglich sein, schlicht im Internet zu surfen, ohne den PC erst mal mühsam zu verriegeln!"
Leider geht es ganz ohne Mühe nicht; aber zum Computerfreak, der komplizierte neue Dinge ausprobiert, muss Sophie dennoch nicht werden. Ein geeignetes Programm neu installieren und dann loslegen – das genügt in vielen Fällen.
Also dann, nichts wie los …

Das Problem

Microsofts Internet-Software (Internet Explorer, MSN Messenger, Outlook und Outlook Express) gilt als Haupteinfallstor für Computer-Schädlinge aller Art. Diese Programme so zu konfigurieren, aktuell zu halten und zu bedienen, dass damit kein Risiko einhergeht, ist nicht einfach.

Die Lösung

Statt Internet Explorer und Outlook Express können auch die Internet-Suites Mozilla/Firefox **(www.mozilla.org, quelloffen und kostenlos)** oder Opera **(www.opera.com, nicht quelloffen)** verwendet werden. Als Alternative zum MSN Messenger empfehlen sich z. B. Instant-Messaging-Programme, die nach dem offenen Standard Jabber **(www.jabber.org)** arbeiten.
Unter **Systemsteuerung → Software** läßt sich potentiell gefährliche und für den Betrieb von Windows nicht erforderliche Internet-Software deinstallieren, insbesondere Outlook Express und MSN Messenger.
Mozilla ist quelloffene Software, das heißt: Mögliche Defizite im Bezug auf Systemsicherheit oder Umgang mit persönlichen Daten sind nachvollziehbar. Normalerweise treten solche Defizite daher seltener auf. Jabber ist ein freies Instant-Messaging-Protokoll, bei dem keine Anmeldeinformationen an einem einzigen zentralen Server abgegeben werden müssen. Verbindungen in andere Netze, z. B. MSN, Yahoo oder ICQ sind möglich.



Technischer Hintergrund

Die Verwendung alternativer Software ist sicherlich kein Allheilmittel gegen Sicherheitsprobleme. Insbesondere das Anlegen von Sicherheitskopien und der richtige Umgang mit Passwörtern sind Hinweise dieser Broschüre, die für jedes Programm und jedes Betriebssystem gelten. Es ist gut zu wissen, daß Windows nicht das einzige Betriebssystem ist. Mit GNU/Linux liegt ein quelloffenes Betriebssystem vor, dass nicht nur weniger Geld kostet als Windows. Fast alle Linux-Distributionen sind kostenlos und legal aus dem Internet herunterzuladen. Viren, Würmer und Dialer sind in der Linux-Welt bisher nicht so weit verbreitet wie unter Windows. Zugleich handelt es sich um eine Alternative, die Windows in Bedienungskomfort und Vielfalt der Anwendungen mittlerweile fast ebenbürtig ist. Mit Knoppix **(www.knopper.net/knoppix/)** liegt eine Linux-Distribution auf einer CD vor, die sich von dieser CD aus starten und ausprobieren lässt. Distributionen wie SuSE **(www.novell.com/linux/)** oder Redhat **(www.redhat.de)** lassen sich neben Windows auf der selben Festplatte installieren.

Checkliste –
Worauf Sie achten sollten (im Überblick)

Grundsätzlich	ja	nein
Nutzen Sie für Ihre PC-Alltagstätigkeiten ein nicht-administratives Benutzerkonto ?		
Sind Ihre Benutzerkonten passwortgeschützt ?		
Ist NTFS als Dateisystem eingerichtet ?		
Läuft Antiviren-Software mit (möglichst tages-)aktuellen Erkennungsdaten ?		
Haben Sie eine Strategie zur Abwehr von Dialer- und anderer Schad-software umgesetzt ?		
Werden nur sichere Programme bekannter Herkunft verwendet ?		
Haben Sie eine Firewall aktiviert ?		
Sind ActiveScripting und ActiveX im Internet-Explorer deaktiviert ?		
Werden sichere, nirgends unverschlüsselt gespeicherte Passwörter verwendet ?		
Regelmäßig	**ja**	**nein**
Sind Betriebssystem und Software durch Updates auf dem neuesten Stand ?		
Ist Ihr PC laut tagesaktuellen Erkennungsdaten frei von Adware ?		
Haben Sie die beim Surfen gespeicherten temporären Internetdateien und Cookies gelöscht ?		
Sind Ihre persönlichen Daten als aktuelle, extern gespeicherte Kopie gesichert ?		

daten schutz

System- und Datensicherheit für Jedermann

Material zum Selbstdatenschutz – Teil 2
Sicherheit in Funknetzwerken

Der Landesbeauftragte für den
Datenschutz Niedersachsen

Einleitung

Hat die Computerausstattung in Ihrem persönlichen Umfeld Zuwachs bekommen? Verfügt der neue PC Ihres Sohnes bereits über eine Netzwerkkarte? Sucht das Notebook Ihrer Tochter gar schon „wireless" nach elektronischen Ansprechpartnern? Möchten Sie jetzt vielleicht zu Hause ein kleines Netzwerk einrichten, um Daten, Drucker und Internetanschluss gemeinsam nutzen zu können? ... **„Alles kein Problem!"** – verspricht die Werbung und zeigt unbeschwerte, kabellose Kommunikation durch Wand und Tür. Doch was sich in der Tat sehr leicht – und heutzutage schon relativ preiswert – per Funk verwirklichen lässt, birgt auch **einige nicht unbeträchtliche Risiken.**

Nachdem wir Ihnen mit unserer ersten Veröffentlichung Grundkenntnisse für die Absicherung Ihres Einzelplatzrechners mit auf den Weg gegeben haben, wollen wir diesmal auf die Gefährdungen hinweisen, die mit dem Aufbau eines kabellosen Netzwerkes verbunden sind.
Wir erklären, wie Sie Ihr **Wireless LAN datenschutzgerecht einrichten** und sich gegen Lauschangriffe und unbefugtes Eindringen absichern können. Schritt für Schritt wird aufgezeigt, welche Einstellungen Sie vornehmen sollten, damit Ihre persönlichen Daten nicht in fremde Hände gelangen.
Zielgruppe dieser Anleitung sind **PC-Nutzer im privaten Umfeld**, die sich erstmals mit der WLAN-Thematik auseinander setzen. Darüber hinaus gehenden professionellen Ansprüchen soll und wird hier nicht gerecht werden können; hierfür steht geeignetes Material an anderer Stelle zur Verfügung.
Um einen möglichst breiten Anwenderkreis anzusprechen, gehen wir wieder davon aus, dass Sie auf Ihrem Rechner **Microsoft Windows XP Home** sowie zusätzlich das **Service Pack 2** installiert haben.

Wir wünschen Ihnen nun viel Spaß und Erfolg beim Aufbau Ihres WLAN und hoffen, dass unsere Anregungen dabei behilflich sind!

Inhalt

Das (Funk-) Netzwerk absichern

Die ersten Schritte – Das eigene Netzwerk einrichten, und wie weiter? **1**
Ausgesperrt – Den Router vor unbefugtem Zugriff schützen **2**
Bleiben Sie unsichtbar! – Das Wireless LAN vor neugierigen Blicken schützen **3**
Wer mit wem? – DHCP abschalten und IP-Adressen manuell vergeben **4**
Kein Einlass! – Mit MAC-Adressen fremde WLAN-Hardware aussperren **5**
Auf Nummer sicher gehen – Wireless LAN verschlüsseln **6**
Weniger ist mehr... und sicherer! – Sendeleistung/-dauer des Routers verringern **7**
Netzwerkfreigaben – So vermeiden Sie böse Überraschungen! **8**

Noch mehr Einstellungen (für Fortgeschrittene)

Mit dem Notebook unterwegs – Verschiedene Konfigurationen verwalten **9**
Unsichtbar hinter Mauern – Mit Firewalls das eigene Netzwerk schützen **10**
NetBIOS und Co. – Überflüssige Protokolle entfernen **11**

Tool zum Schutz der Privatsphäre

„Was niemand weiß..." – Ein Geheimtresor für vertrauliche Daten **12**

Glossar

Die wichtigsten Begriffe und Abkürzungen **13**

Checkliste

Worauf Sie achten sollten (im Überblick) **14**

Herausgeber
Der Landesbeauftragte für den
Datenschutz Niedersachsen
Postfach 2 21
30002 Hannover
Tel (0511) 120-4500
Fax (0511) 120-4599
poststelle@lfd.niedersachsen.de
www.lfd.niedersachsen.de

Quelle: www.lfd.niedersachsen.de
→ Service-Angebote
→ Selbstdatenschutz
→ Downloads

erstellt: Juli 2006

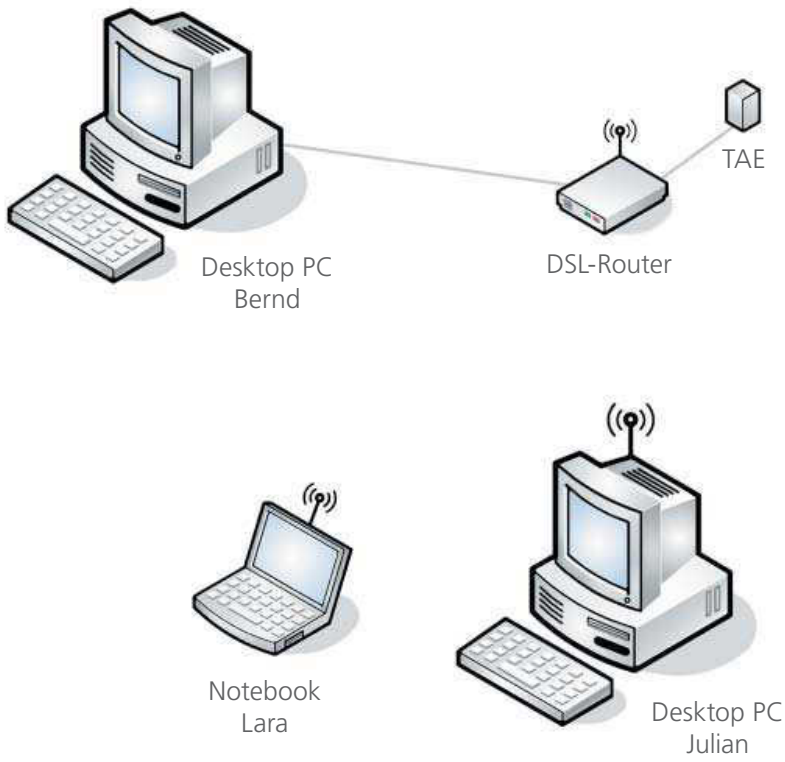
Die ersten Schritte –
Das eigene Netzwerk einrichten, und wie weiter?

1

„Alles kein Problem! Sie brauchen nur die CD einlegen und den Hinweisen zu folgen. Spätestens nach einer Viertelstunde läuft das Ganze. Das bekommen auch Anfänger hin. Ein Handbuch ist eigentlich gar nicht nötig, müsste aber trotzdem mit dabei sein."

Der Verkäufer sollte Recht behalten: Die Installation des WLAN-Routers an Bernds PC geht wirklich kinderleicht und schnell. Tochter Lara und Sohn Julian freuen sich schon, da das Feilschen um den einzigen Platz mit Internetzugang bald ein Ende haben wird.

Wozu wohl das mit installierte Programm zur Konfiguration des Routers noch gut sein soll?



Das Problem

☺ Netzwerke bieten eine Vielzahl von interessanten Möglichkeiten:
So kann ein Internetzugang von mehreren Rechnern genutzt werden, die neuesten Urlaubsfotos lassen sich ohne Umwege austauschen und die Musikdateien auf der Festplatte sind über das Entertainment-Center im Wohnzimmer abspielbar.
Noch komfortabler wird es, wenn mit Hilfe von Wireless LAN auch eine aufwändige Verkabelung entfällt.

☹ Es existieren jedoch auch eine Reihe von Gefährdungen, die nicht übersehen werden dürfen:
Grundsätzlich ist ein Netzwerk im Vergleich zum Einzelplatz-PC größeren Sicherheitsrisiken ausgesetzt. Schadsoftware, die sich auf einem Rechner einnistet, kann von dort aus alle verbundenen Geräte kompromittieren.
Bei Funknetzwerken kommt hinzu, dass diese aufgrund der fehlenden Kabelverbindung besonders anfällig für Lauschangriffe und Datendiebstahl sind. So ist es möglich, dass die Netzwerkkommunikation abgehört, E-Mails mitgelesen oder Passwörter ausspioniert werden.
Gelingt es einem ungebetenen Eindringling gar, sich im Netzwerk anzumelden, könnte er Ihren Internetanschluss kostenlos nutzen und diesen für eigene Zwecke missbrauchen. Auch wären die Daten auf Ihrer Festplatte in Gefahr.

Von wenigen Ausnahmen abgesehen, befinden sich viele Router nach Ablauf der Installationsroutine leider oftmals in einem beklagenswert unsicheren Ausgangszustand. Viele Hersteller scheinen mit einer möglichst schnellen und eher unkomplizierten Inbetriebnahme glänzen zu wollen.
Hacker wissen, dass viele WLAN-Betreiber diese Standardeinstellungen beibehalten – und nutzen dies für Angriffe und Einbruchsversuche aus!

Die Lösung

Um Ihr Netzwerk abzusichern, sollten Sie unbedingt die **Standardeinstellungen des Routers prüfen und gegebenenfalls anpassen**. Wie das geht und welche Einstellungen Sie dabei vornehmen müssen, erklären wir Ihnen auf den nachfolgenden Seiten.
Wenn Sie unsere Ratschläge befolgen, werden Sie gegen die gröbsten Gefahren geschützt sein, jedoch **nie 100%ige Sicherheit** erreichen! Nicht zuletzt weil sich die Technik sehr schnell weiterentwickelt, sollten Sie auch immer eigene Überlegungen anstellen und nach geeigneten Vorsichts- und Abwehrmaßnahmen zum Schutz Ihres WLANs suchen.

Ausgesperrt –
Den Router vor unbefugtem Zugriff schützen

2

Bei der Inbetriebnahme des Routers ist Bernd ähnlich vorgegangen wie bei den anderen Geräten, die er bisher an seinen PC angeschlossen hat:
Installations-CD einlegen, Kabelverbindungen nach Aufbauanleitung herstellen, Status anhand der Kontrollleuchten überprüfen ...
Während der Konfiguration wurden allerdings auch die Zugangsdaten für das Internet abgefragt, und ein Passwort spielte ebenfalls eine Rolle.
Was unterscheidet den Router von sonstigen Komponenten und macht ihn besonders schützenswert?

Das Problem

Mit dem Router wird ein Gerät installiert, das neben dem PC mit einer eigenen unabhängigen Funktionalität ausgestattet ist und für den Schutz der verbundenen Systeme von besonderer Bedeutung ist. Für Hacker, die in ein Netzwerk eindringen wollen, stellt deshalb der Router ein zentrales Angriffsziel dar: hier wird die Schnittstelle zwischen angeschlossenen PCs und Internet realisiert, und hier erfolgt auch die Prüfung der Zugangsberechtigung der einzelnen Netzwerkteilnehmer.
Diese Daten dürfen nicht in fremde Hände geraten! Der Router bedarf in puncto Sicherheit und Pflege ähnlicher Aufmerksamkeit wie Ihr PC.

Die Lösung

Die Einstellungen am Router lassen sich in der Regel über ein Webinterface vornehmen. Starten Sie Ihren Browser und geben Sie die Adresse Ihres Routers ein – diese können Sie im Benutzerhandbuch nachlesen.

Da die Funkverbindung besonderen Gefährdungen ausgesetzt ist, sollten Sie den Router grundsätzlich per Kabelverbindung konfigurieren. **Verzichten Sie auf die Administration über Wireless LAN!**

Auf jeden Fall sollten Sie ein werkseitig eingestelltes **Passwort ändern** und in regelmäßigen Abständen erneuern.

Folgende Optionen werden von den meisten Geräten unterstützt:

Firmware-Update
Prüfen Sie, ob für Ihr Gerät im Internet ein Firmware-Update verfügbar ist und installieren Sie es nach Anleitung. Durch die Entwicklung neuer Firmware begegnen die Hersteller bekannt gewordenen Sicherheitslücken.

Fernadministration
Deaktivieren Sie diese – auch „Remote Access" genannte – Funktionalität. Sie werden sie im Normalfall nicht nutzen, und Unbefugte sollten nicht in Versuchung kommen.

Konfigurationswiederherstellung
Nach Änderung aller Einstellungen können Sie die aktuelle Konfiguration in eine Datei speichern und im Bedarfsfall erneut einspielen. Diese „Notfallversicherung" sollten Sie außerhalb Ihres Netzwerkes auf einem externen Datenträger abspeichern und sicher aufbewahren.

Technische Hintergrundinfos

Die ursprüngliche Funktion eines Routers ist es, innerhalb verschiedener Netzwerke die Daten von einem zum anderen Netzwerk weiterzuleiten. Heutzutage vereinen die mit „Router" bezeichneten Geräte mehrere Funktionen: sie verbinden ein lokales Netzwerk mit dem Internet, leiten Datenpakete von einem Rechner an den anderen weiter und überwachen mittels der integrierten Firewall den Datenverkehr auf potentielle Angriffe. Ist im Router ein Access Point enthalten, können an das Netzwerk zusätzlich auch WLAN-Geräte angeschlossen werden.

Bleiben Sie unsichtbar! – Das Wireless LAN vor neugierigen Blicken schützen

3

Als Lara sich mit ihrem Notebook erstmals im WLAN anmelden möchte, staunt sie nicht schlecht: „Ist das nicht mein Nachbar?", fragt sie sich, als sie im Anmeldefenster einen vertrauten Namen entdeckt.
Kein Zweifel: Lara bekommt gerade fremde Funknetzwerke zum Verbinden angezeigt – sowohl ungesicherte als auch sicherheitsaktivierte. Doch wie steht es um die Sicherheit des eigenen WLANs ihrer Familie? Lara ist wenig begeistert und fürchtet, ihr Nachbar könnte ihren Rechner auspionieren.

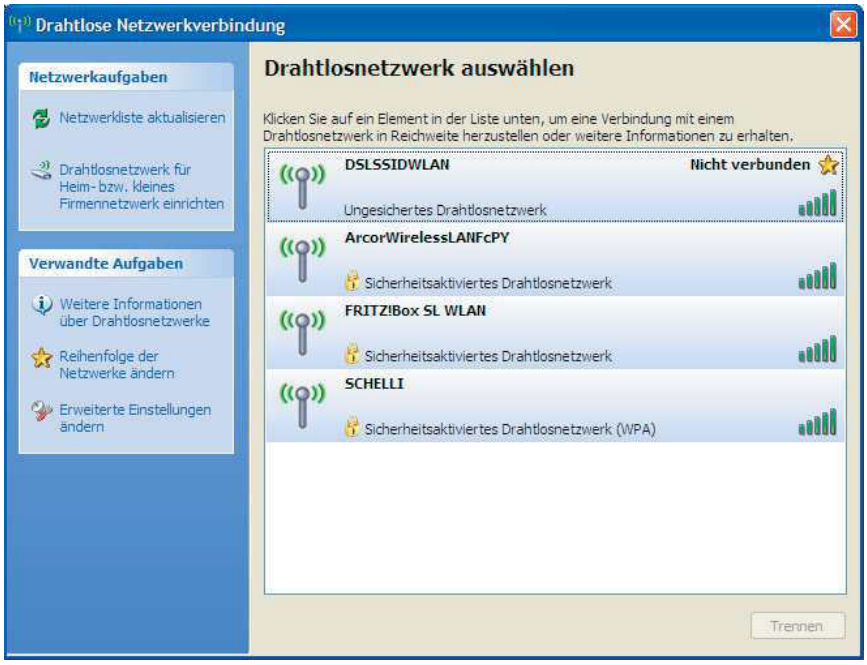
Das Problem

Viele Router sind ab Werk so konfiguriert, dass sie ihre SSID (Service Set Identifier) unaufgefordert aussenden. Damit wird zum einen das Vorhandensein eines WLANs, zum anderen aber auch der Name des Funknetzwerkes öffentlich bekannt gemacht – für Hacker ein gefundenes Fressen!

Die Lösung

Um das eigene WLAN vor fremden Blicken zu schützen, muss im Router das permanente Aussenden der SSID unterbunden werden. **Deaktiveren Sie** hierzu in den Einstellungen Ihres Routers die entsprechende Option – bei vielen Routern wird diese als „SSID Broadcast" bezeichnet.

Nun ist Ihr Netzwerk zwar mit einer „Tarnkappe" versehen, bleibt aber bei Kenntnis des Namens weiterhin ansprechbar. Da werkseitig voreingestellte SSID-Bezeichnungen allgemein bekannt sind, sollten Sie diese ebenfalls ändern, um direkte Verbindungsversuche von Unbefugten weiter zu erschweren.



Sendet ein Router seine SSID selbständig aus, wird das dazugehörige WLAN in Windows angezeigt. In der Liste ganz oben: Die Netzwerkerkennung bringt ein ungesichertes Funknetzwerk zum Vorschein.

Vergeben Sie für Ihr privates WLAN eine neue SSID, die nach Möglichkeit keinen Rückschluss auf Ihre Person, Ihre Firma oder den Standort Ihres WLANs zulässt.

Den neuen Netzwerknamen müssen Sie nun auch auf all Ihren per WLAN angebundenen Computern eintragen. Klicken Sie hierzu auf **Start → Systemsteuerung → Netzwerk- und Internetverbindungen**. Klicken Sie auf das Symbol für die **Netzwerkverbindungen** und wählen Sie **Drahtlose Netzwerkverbindung**. In der Kategorie **Netzwerkaufgaben** finden Sie die Option **Einstellung dieser Verbindung ändern.** Klicken Sie auf diese Option, wählen Sie den Punkt **Drahtlosnetzwerke** und klicken Sie anschließend auf **Neue drahtlose Netzwerkverbindung hinzufügen.** Hier tragen Sie dieselbe SSID ein, die Sie zuvor im Router vergeben haben.

Technische Hintergrundinfos

Der Netzwerkname (SSID) wird benötigt, um verschiedene Funknetzwerke einfacher voneinander unterscheiden zu können. Damit sich berechtigte Verbindungen auch bei deaktiviertem SSID-Broadcast aufbauen lassen, muss das Netzwerk jedoch unter seinem nunmehr geheim gehaltenen Namen ansprechbar bleiben.

Wer mit wem? –
DHCP abschalten und IP-Adressen manuell vergeben

4

Bernd hat seinem Router eine neue SSID vergeben und deren automatisches Aussenden deaktiviert. Das war nicht besonders schwer, und er fühlt sich auf der sicheren Seite. Doch hat er wirklich alle Möglichkeiten ausgeschöpft, damit niemand in sein Heimnetzwerk eindringen kann?
In dem inzwischen doch zu Rate gezogenen Handbuch gibt es jedoch weitere Einstellungsmöglichkeiten, die gemäß Warnhinweis allerdings nur mit „Expertenwissen" genutzt werden sollen.
Was hat es damit auf sich?

Das Problem

Wer sich Zugang zu einem fremden WLAN verschaffen will, benötigt neben der richtigen SSID des Routers auch eine zum Netzwerk passende und eindeutige Netzwerkadresse. Da mancher Anwender mit der Einstellung von IP-Adressen überfordert ist, geht die Standardkonfiguration auch hier den einfachen Weg und weist jedem sich anmeldenden Gerät – und damit auch Eindringlingen – über den Router automatisch per DHCP-Dienst eine passende IP-Adresse zu.

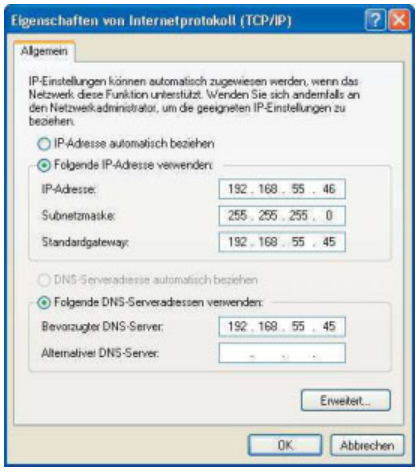
Die Lösung

1) Deaktivieren Sie die DHCP-Funktion Ihres Routers.
2) Vergeben Sie die IP-Adressen aller beteiligten Geräte einmalig von Hand.
3) Lassen Sie im Netz möglichst ausschließlich die von Ihnen vergebenen IP-Adressen zu.

zu 1) Im Konfigurationsmenü Ihres Routers wird eine Option „Router als DHCP-Server verwenden" o.ä. existieren. Deaktivieren Sie diese Funktion.
zu 2) Im Router selbst ist bereits eine IP-Adresse voreingestellt; sie lautet in der Regel **192.168.**0.1 .
Belassen Sie die ersten beiden Ziffernblöcke. Um Dritten das Erraten des Eintrages zu erschweren, empfiehlt es sich jedoch für die letzten beiden Blöcke von der Standardeinstellung abzuweichen und eigenständige Werte einzutragen (z.B. 192.168.**55.45**). Notieren Sie sich die IP-Adresse Ihres Routers!

Wichtig: Die IP-Adressen aller anderen Netzwerkkomponenten dürfen sich nur im letzten Ziffernblock unterscheiden. Lautet die IP-Adresse des Routers wie im obigen Beispiel **192.168.55.45**, ist es ratsam, den im Netzwerk anzubindenden Rechnern nacheinander die IP-Adressen **192.168.55.46, 192.168.55.47** usw. zuzuweisen.

Verfahren Sie an den einzelnen Rechnern jeweils wie folgt:
Klicken Sie in Windows auf **Start → Systemsteuerung → Netzwerk- und Internetverbindungen.** Wenn Sie auf „Netzwerkverbindungen" gehen, bekommen Sie eine Liste aller Netzwerkadapter angezeigt. Für die Konfiguration einer Kabelverbindung wählen Sie **LAN-Verbindung**, für die Konfiguration einer Funkverbindung wählen Sie **Drahtlose Netzwerkverbindung**. Rufen Sie mit der rechten Maustaste das Kontextmenü auf. Klicken Sie auf **Eigenschaften** und wählen Sie **Internetprotokoll TCP/IP**. Klicken Sie ein weiteres mal auf **Eigenschaften** und aktivieren Sie **Folgende IP-Adresse verwenden**. Geben Sie anschließend eine IP-Adresse ein, die mit der IP-Adresse Ihres Routers korrespondiert (s.o.).
Der Wert 255.255.255.0 muss in der **Subnetzmaske** stehen. In den Feldern **Standardgateway** und **Bevorzugter DNS-Server** wird die IP-Adresse des Routers eingetragen.
Wiederholen Sie die Schritte auf allen Rechnern, die Sie an das Netzwerk anschließen wollen.
zu 3) Suchen Sie im Konfigurationsmenü Ihres Routers die Option, nur bestimmte IP-Adressen im Netzwerk zuzulassen, und tragen Sie – falls vorhanden – dort die von Ihnen vergebenen Adressen der



Technische Hintergrundinfos

Ein Netzwerk wird über den Verbund zusammengehöriger IP-Adressen realisiert. Der Adressraum 192.168.xxx.yyy steht außerhalb des Internets speziell für „private Zwecke" zur Verfügung und kann in Firmen- oder Heimnetzwerken beliebig oft genutzt werden, da diese Adressen vom Router nicht an das Internet weitergeleitet („geroutet") werden.

Kein Einlass! –
Mit MAC-Adressen fremde WLAN-Hardware ausperren

So, ... wer durch diese Tür eintreten will, muss schon mal wissen, wer dahinter wohnt (SSID kennen) und sagen, woher er kommt (zugelassene IP-Adresse angeben).
„Noch besser wäre es, wenn man genau wüsste, wer draußen steht, bevor man öffnet", denkt sich Bernd und sucht nach einer Möglichkeit, den Kreis der berechtigten Besucher weiter einzuschränken.

Das Problem

Für jedes Netzwerk gilt: Der Zugang soll nur wenigen, ausgewählten Teilnehmern gestattet sein. Wo größere Unternehmen für die Absicherung ihres Firmennetzes kostspielige Lösungen einsetzen, müssen sich private Anwender mit anderen Mitteln behelfen. Eine zusätzliche Hürde, wie „Gelegenheits-Hackern" der Zugang zum eigenen Netzwerk versperrt werden kann, ist die Zugangsbeschränkung mittels MAC-Adressen-Filterung.

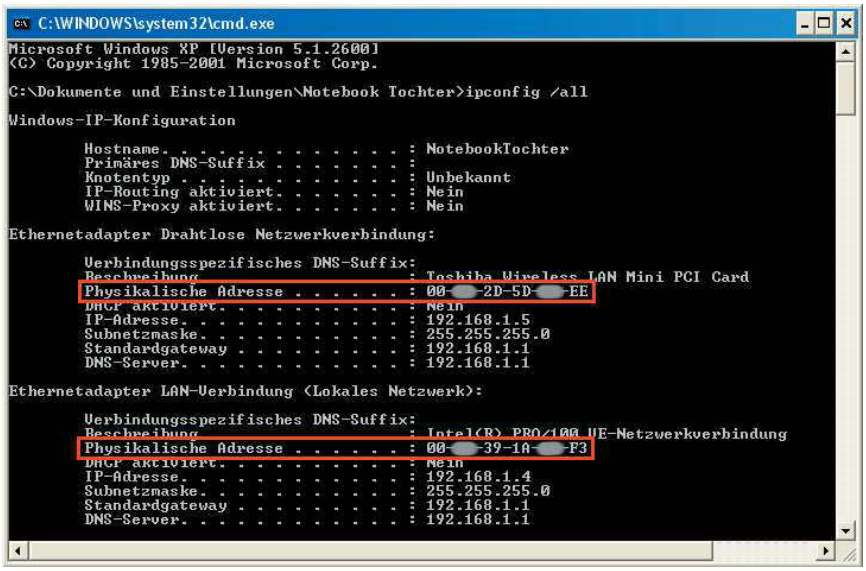
Die Lösung

Ihnen ist die Hardware bekannt, aus der sich Ihr Netzwerk zusammensetzt. Konfigurieren Sie deshalb Ihren Router so, dass er nur solche Teilnehmer akzeptiert, deren eindeutige „Registriernummern" er kennt.
Ermitteln Sie hierzu als erstes die MAC-Adressen der Netzwerkkomponenten (i.d.R. Netzwerkkarten), die Sie im Gebrauch haben. Die MAC-Adresse ist i.d.R. auf dem Bauteil/Gerät aufgebracht und dort ablesbar. Wo dies nicht der Fall ist, können Sie sich per DOS-Befehl behelfen.

Klicken Sie hierzu in Windows auf **Start → Ausführen** und geben den Befehl **cmd** ein. In das Fenster, das sich öffnet, geben Sie die Zeile **ipconfig /all** ein. Es werden daraufhin alle Netzwerkadapter und die dazugehörigen MAC-Adressen angezeigt. Notieren Sie sich die MAC-Adressen, um diese anschließend in der MAC-Adressen-Tabelle des Routers zu verwalten. Die entsprechende Option im Router nennt sich „MAC Zugangskontrolle" oder „MAC-Adressen-Filter" (lesen Sie hierzu im Handbuch des Routers nach).

Stellen Sie eine Liste aller Geräte zusammen, die einen berechtigten Zugang zu Ihrem Netzwerk erhalten sollen. Meldet sich ein Rechner mit einer unbekannten MAC-Adresse am Router an, wird er von diesem abgewiesen und für die Netzwerkkommunikation gesperrt.

Wichtig: Wenn Sie an Ihr Netzwerk später ein weiteres Gerät anschließen wollen, dürfen Sie nicht vergessen, dessen MAC-Adresse ebenfalls im Router einzutragen – sonst wird sich kein Kontakt herstellen lassen!



Ein Computer kann über mehrere Netzwerkkomponenten verfügen. Mit Hilfe des Befehls „ipconfig /all" werden alle Netzwerkadapter und MAC-Adressen aufgelistet.

Technische Hintergrundinfos

Jeder Netzwerkadapter bekommt während der Herstellung eine MAC-Adresse implementiert – diese wird weltweit nur einmal vergeben; sie ist nur auslesbar und kann nicht verändert werden.
Leider stellt die MAC-Adressen-Filterung nur eine von mehreren Maßnahmen dar, die das unbefugte Eindringen zwar weiter erschwert, jedoch nicht unmöglich macht.
Der Grund: Per Software können beliebige MAC-Adressen in übertragene Datenpakete „eingebaut" werden und verschleiern so die wahre Identität des Absenders.

Auf Nummer sicher gehen – Wireless LAN verschlüsseln

6

Als Lara ihre E-Mails abrufen will, scheint ihr Account gesperrt zu sein. Auch nach mehreren Versuchen erhält sie immer die gleiche Meldung: „Benutzername oder Kennwort falsch!“.
Eine Anfrage bei ihrem Provider ergibt, dass ihre Login-Daten vor kurzem geändert worden sind.

Das Problem

Da in einem kabelosen Netzwerk die Daten per Funk übermittelt werden, sind sie für Dritte lesbar – vorausgesetzt, die Übertragung erfolgt unverschlüsselt und die gesendeten Informationen liegen im Klartext vor.
Einem Hacker ist es dann möglich, Benutzernamen und Passwörter auszuspionieren oder E-Mails mitzulesen. Für diese Art von Datenklau ist nicht einmal eine Anmeldung am Router erforderlich – der Angreifer bleibt also unbemerkt.

Die Lösung

In Drahtlosnetzwerken sollte die Datenübertragung in jedem Fall verschlüsselt erfolgen. Worauf Sie allerdings schon beim Kauf Ihrer WLAN-Komponenten achten sollten: Nicht alle Verschlüsselungstechniken sind gleich sicher! Dabei ist höhere Sicherheit keine Frage des Preises, sondern eher der Aktualität der angebotenen Hard- und Firmware. Vermeiden Sie Ladenhüter und **achten Sie auf die Unterstützung von WPA (Wi-Fi Protected Access)!** Hierbei handelt es sich um den derzeit sichersten marktüblichen Verschlüsselungmodus. Falls Ihnen ein günstiges Gebrauchtgerät verlockend erscheint und dieses lediglich WEP (Wired Equivalent Privacy) unterstützt, sollten Sie sich der Risiken bewußt sein. Diese Technik ist zwar besser als gar keine Verschlüsselung, hält aber versierten und ausdauernden Angreifern nicht stand.
Wichtig: Alle WLAN-Komponenten sollten dem gleichen, möglichst hohen Standard entsprechen. Erst eine hochwertige Verschlüsselung macht Ihr WLAN wirklich sicher!

Verschlüsselung mit WPA:
Suchen Sie in den Einstellungen des Routers den Punkt „WLAN-Sicherheit“ oder „Verschlüsselung“ und aktivieren Sie dort die Option **WPA-PSK**.
Im nächsten Schritt geben Sie den Schlüssel ein, der für die Authentifizierung und Verschlüsselung der Daten verwendet wird.
Wählen Sie nach Möglichkeit eine komplexe und zufällige Zeichenfolge, deren Länge nicht weniger als 30 Zeichen betragen sollte. Je länger der Schlüssel (bis zu 63 Zeichen), desto sicherer ist Ihr WLAN geschützt. Keine Angst, dieser Schlüssel wird auf dem Router und den am WLAN angebundenen Rechnern sicher hinterlegt; Sie werden ihn nicht ständig eingeben müssen!

Falls möglich wählen Sie bei der Datenverschlüsselung die Methode **AES** (TKIP geht auch, ist aber etwas unsicherer und langsamer).
Den sogenannten Kompatibilitätsmodus sollten Sie deaktivieren, sonst kann es passieren, dass der Router automatisch auf WEP umschaltet, falls sich ein Gerät anmeldet, das nur WEP unterstützt.

Nachdem Sie den Schlüssel im Router hinterlegt haben, muss dieser auch auf allen anderen WLAN-Geräten eingetragen werden. Im Auswahlfenster von **Drahtlose Netzwerkverbindung** wird Ihr WLAN nicht mehr angezeigt, da das Aussenden der SSID vom Router nunmehr unterdrückt wird (s. Seite 3). Klicken Sie deshalb links auf **Erweiterte Einstellungen ändern**, dann im folgenden Fenster auf den Reiter **Drahtlosnetzwerke** und nehmen Sie hier die weiteren Einstellungen vor.
Für die Authentifizierung am Netzwerk wählen Sie **WPA-PSK**, für die Datenverschlüsselung AES oder TKIP – je nachdem, welche Methode Sie zuvor am Router eingestellt haben. Als Netzwerkschlüssel verwenden Sie den gleichen Schlüssel wie im Router.
Wird trotz übereinstimmender Einträge keine Netzwerkverbindung hergestellt, kann es daran liegen, dass Ihre Hardware für WPA nicht kompatibel ist. In diesem Fall müssen Sie auf WEP umstellen.

Verschlüsselung mit WEP:
Stellen Sie im Router die höchstmögliche Verschlüsselungsstufe ein. Auch hier gilt: Der gewählte Modus muss von allen WLAN-Geräten unterstützt werden! WEP 256 ist am sichersten, funktioniert aber in den allermeisten Fällen nur, wenn alle Komponenten vom selben Hersteller stammen.
Für WEP 128 tragen Sie einen Schlüssel ein, der aus 26 Zeichen im ASCII-Format (herkömmliche Folge aus Buchstaben, Ziffern und Sonderzeichen) oder aus 13 Zeichen im Hexadezimal-Format besteht (nur Ziffern 0-9 und Buchstaben A-F). Bei WEP 64 ist der Schlüssel kürzer und entsprechend unsicherer.
Geben Sie für den Schlüssel eine möglichst zufällige Zeichenfolge ein, am besten im Hexadezimal-Format. Je mehr Zufallscharakter ein Schlüssel hat, desto besser ist Ihr WLAN geschützt.
Nehmen Sie anschließend die Einstellungen an Ihrem PC oder Notebook vor. Klicken Sie hierzu auf **Start → Systemsteuerung → Netzwerk- und Internetverbindungen** und dann auf den Punkt **Netzwerkverbindungen.** Klicken Sie mit der rechten Maustaste auf **Drahtlose Netzwerkverbindung** und dann im Kontextmenü auf „Eigenschaften“. Hier tragen Sie den Schlüssel ein, den Sie zuvor im Router eingegeben haben. Für die Authentifizierung wählen Sie „Open System“.
Aufgrund der nachgewiesenen Angreifbarkeit von WEP sollten Sie **den verwendeten Schlüssel häufiger wechseln!**

Weniger ist mehr... und sicherer! – Sendeleistung/-dauer des Routers verringern

7

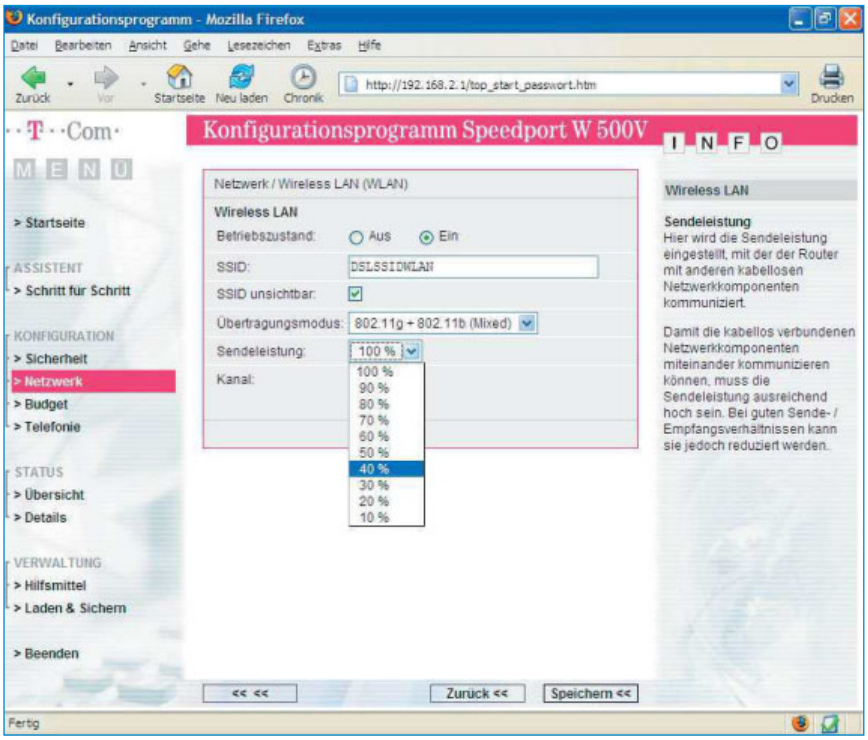
Julian ist stolz: Das Übernachtungswochende bei seinem Freund in der Nachbarschaft war ein voller Erfolg! Eigentlich hatte er seinen neuen PC nur mal vorführen wollen, aber Papas neues Funknetzwerk machte es möglich: Online-Spiele und Download-Partys bei Tag und Nacht! Und das aus sicherer und unbeobachteter Entfernung! Stand die im Familienrat durchgesetzte Flatrate eigentlich schon zur Verfügung?

Das Problem

Die Reichweite von Routern oder Access Points beträgt mittlerweile einige hundert Meter – ideal auch für Schnüffler, die in ein fremdes WLAN eindringen wollen. Wenn ein Hacker dann auch noch mit einer Hochleistungsantenne ausgestattet ist, hat er leichtes Spiel, ein weit entferntes WLAN aufzuspüren und seinen Angriff aus sicherer Distanz vorzubereiten. Er selbst bleibt dabei unsichtbar und ist nur schwer zu lokalisieren.

Die Lösung

Einige WLAN-Router besitzen die Möglichkeit, die Sendeleistung dynamisch anzupassen. Auf diese Weise lässt sich die Ausbreitung der Funkwellen auf die unmittelbare Umgebung begrenzen. Weniger Sendeleistung bedeutet weniger Reichweite: Der Radius der vom Router ausgestrahlten Funksignale verkleinert sich. **Reduzieren Sie deshalb die Sendeleistung Ihres WLAN-Routers auf das absolut notwendige Maß.** Damit vergrößern Sie die Chance, potentielle Hacker von Ihrem WLAN fernzuhalten.



Einfach, aber effektiv: Halten Sie Hacker von Ihrem Funknetzwerk fern, indem Sie die Sendeleistung Ihres WLAN-Routers reduzieren.

Ein zu gering eingestellter Wert kann sich jedoch auf die Performance auswirken, so dass Ihr Funknetzwerk nicht mehr mit der gewohnten Geschwindigkeit arbeitet.
Experimentieren Sie ein wenig, bis Sie die optimale Einstellung gefunden haben! Testen Sie anschließend mit Ihrem Notebook, von wo aus Sie überall Empfang haben.

Der Einsatz von Richtantennen kann die Sicherheit in einem Wireless LAN weiter erhöhen. Im Gegensatz zu herkömmlichen Rundstrahlantennen sorgen Richtantennen für eine zielgenaue Ausrichtung der Funksignale. Damit erhalten nur solche Geräte einen Zugang zum Funknetzwerk, die sich innerhalb des eng definierten Empfangsbereichs befinden.

Und zu guter letzt:
Begrenzen Sie die tägliche Betriebszeit Ihres WLAN-Routers.
Falls Ihr Gerät diese Konfigurationsmöglichkeit nicht aufweist: Greifen Sie zur Zeitschaltuhr und sorgen Sie nachts oder bei Abwesenheit für Funkstille.

Netzwerkfreigaben – So vermeiden Sie böse Überraschungen!

Die neue Festplatte mit satten 350 GB Speicher macht's möglich: Endlich kann Julian seine komplette Musiksammlung auf dem PC speichern. Damit auch der Rest der Familie am Hörgenuss teilhaben kann, braucht er jetzt nur noch das Laufwerk freigegeben... und muss eines Tages feststellen, dass er dies besser hätte lassen sollen: Ein Großteil seiner Sammlung und andere wichtige Dokumente sind plötzlich verschwunden!

Das Problem

In einem Netzwerk können andere Benutzer auf die eigenen Daten und Ressourcen zugreifen, sofern diese per Netzwerkfreigabe zur Verfügung gestellt werden. Auf diese Weise lassen sich bequem Dokumente, Musik- oder Videodateien austauschen.
Dabei ist große Vorsicht angebracht, sonst kann es schnell passieren, dass vertrauliche Daten von jemand anderem gelesen werden oder wichtige Dokumente verloren gehen – ein Mausklick genügt, und die Arbeit der letzten Wochen oder Monate ist dahin.

Die Lösung

Nutzer von Windows XP Home sollten das Freigeben von Ordnern äußerst restriktiv handhaben. **Geben Sie Ihre Ordner nach Möglichkeit nur schreibgeschützt frei!** Damit verhindern Sie, dass andere Teilnehmer Ihre Daten ändern oder versehentlich löschen können.

Um einen Ordner freizugeben, starten Sie den Windows Explorer und klicken mit der rechten Maustaste auf den Ordner, den Sie freigeben wollen. Klicken Sie auf **Freigabe und Sicherheit**. Setzen Sie das Häkchen vor die Option **Diesen Ordner im Netzwerk freigeben** und vergeben Sie für die Netzwerkfreigabe einen Namen.
Wenn Sie möchten, dass andere den Inhalt in diesem Ordner nicht nur lesen, sondern auch ändern, speichern und löschen dürfen, setzen Sie ein Häkchen vor **Netzwerkbenutzer dürfen Dateien verändern**.

Doch Vorsicht! Wählen Sie diese Option mit Bedacht. Auf keinen Fall sollten Sie in diesem Ordner wichtige oder vertrauliche Dokumente aufbewahren!
Geben Sie ein Laufwerk niemals als Ganzes, sondern immer nur einzelne Ordner frei! Nicht benötigte Netzwerkfreigaben sollten Sie wieder rückgängig machen.

Ordnerfreigaben anderer Netzwerkteilnehmer werden unter **Start → Arbeitsplatz → Netzwerkumgebung** angezeigt.

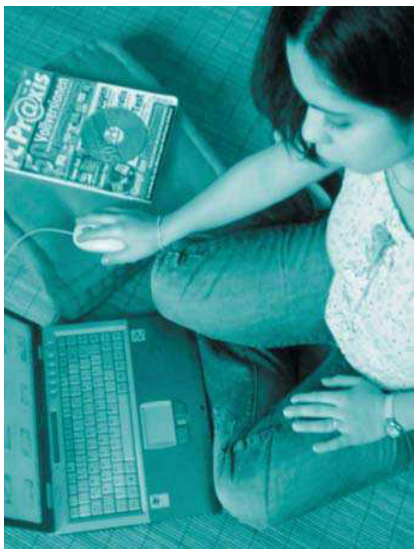
Generell gilt: Vertrauliche oder sensible Daten haben in einer Netzwerkfreigabe nichts zu suchen!
Wollen Sie diese Daten trotzdem freigeben, ist es ratsam, sie zu verschlüsseln (siehe Seite 12). Unbefugte, die dann in den Besitz dieser Daten gelangen, können damit nichts mehr anfangen.

Technische Hintergrundinfos

Nutzern von **Windows XP Home** wird in Sachen Netzwerkfreigabe lediglich ein rudimentäter Schutz geboten, da sich Ordner nur auf zwei Arten freigeben lassen: entweder ändernd oder nur lesend. Feinere Abstufungen in der Zugriffsberechtigung sind standardmäßig nicht vorgesehen. Damit kann das Potential vieler Anwendungen nicht vollständig ausgeschöpft werden.
Hier bietet **Windows XP Professional** weitaus mehr Möglichkeiten: Netzwerkfreigaben können entsprechend den Anforderungen und Bedürfnissen einzelner Teilnehmer angepasst werden. Dateien lassen sich benutzerabhängig und passwortgeschützt freigegeben, und die Art des Zugriffs kann durch die Vergabe differenzierter Rechte (Vollzugriff, Ändern, Lesen, Ausführen, Schreiben) bestimmt werden.
Wer höhere Anforderungen an ein Netzwerk stellt, sollte darüber nachdenken, ob sich ein Umstieg auf die Professional Version lohnt.

Gehen Sie auf Nummer sicher! Entfernen Sie das Häkchen vor „Netzwerkbenutzer dürfen Dateien verändern". Andernfalls könnten Ihre Daten schnell verloren gehen.

Mit dem Notebook unterwegs – Verschiedene Konfigurationen verwalten



Lara hat Schwierigkeiten, als sie sich mit ihrem Notebook am Netzwerk in der Uni anmelden will. Der Administrator erklärt Ihr das Problem: Die Netzwerkeinstellungen auf Ihrem Notebook würden nicht mit denen der Universität übereinstimmen. Eine kleine Änderung an der IP-Konfiguration – und schon ist der Kontakt zum Uni-Netzwerk hergestellt. Doch wieder zu Hause angekommen, tritt das Problem erneut auf.

Das Problem

Um einen Computer an ein Netzwerk anzuschließen, muss dieser über die passende IP-Konfiguration verfügen. In der Regel bekommt er die nötigen Einstellungen automatisch vom Router (oder einem anderen DHCP-Server) mitgeteilt – vorausgesetzt, diese Option ist in Windows eingeschaltet. Werden die IP-Adressen in einem privaten WLAN manuell zugewiesen (siehe Seite 4), besitzen Sie nur dort Gültigkeit und die Verbindung zu einem anderen Netzwerk muss scheitern.
Der Wechsel zwischen verschiedenen Netzwerken ist somit etwas mühsam, da die Einstellungen für IP-Adresse, Subnetzmaske und DNS-Server jedes mal von neuem vorgenommen werden müssen.

Die Lösung

Die Anmeldung in verschiedenen Netzwerken wird zu einem Kinderspiel, wenn Sie die Netzwerkeinstellung in eine Datei sichern und dann bei Bedarf wiederherstellen.
Um Ihre aktuelle Netzwerkeinstellung in eine Datei zu speichern, klicken Sie auf **Start → Ausführen** und geben dann den Befehl **cmd** ein. In dem darauf folgenden Fenster geben Sie den Befehl **netsh interface dump > C:\PrivatesLAN.txt** ein. Die Netzwerkkonfiguration, die Sie gerade verwenden, wird daraufhin in die Datei „PrivatesLAN.txt" geschrieben.

Für unterwegs: Die richtige IP-Konfiguration per DHCP automatisch beziehen!

Erstellen Sie nun ein neues Profil, das Sie verwenden können, wenn Sie sich mit Ihrem Notebook in einem fremden Netzwerk anmelden möchten (mit diesem Profil wird die IP-Konfiguration vom DHCP-Server abgefragt, Sie brauchen die Einstellungen dann nicht jedesmal von neuem vornehmen).
Klicken Sie unter **Netzwerkverbindung** mit der rechten Maustaste auf das Symbol **Drahtlose Netzwerkverbindung** (bzw. auf **LAN-Verbindung**, wenn Sie die Verbindung per Kabel herstellen wollen). Klicken Sie auf **Eigenschaften**, dann auf **Internetprotokoll (TCP/IP)** und wieder auf **Eigenschaften**. Setzen Sie ein Häkchen vor **IP-Adresse automatisch beziehen** und ein weiteres vor **DNS-Serveradresse automatisch beziehen**. Speichern Sie die geänderte Netzwerkeinstellung wieder mit dem Befehl **netsh interface dump > DHCP.txt.** Das Wiederherstellen derselben Konfiguration geschieht mit dem Befehl **netsh -f C:\DHCP.txt.**

Noch komfortabler geht es, wenn Sie die Zeile **netsh -f C:\DHCP.txt** mit Notepad schreiben und die Textdatei mit der Endung „cmd" oder „bat" abspeichern. Damit erzeugen Sie ein Script, das den Befehl automatisch ausführt, wenn Sie mit der Maus darauf doppelklicken.
Wenn Sie jetzt für jede Ihrer benötigten IP-Konfigurationen ein eigenes Script

Per Mausklick zwischen mehreren Netzwerkeinstellungen wechseln. Speichern Sie die aktuelle IP-Konfiguration in eine Datei und lassen Sie diese bei Bedarf über ein Script wiederherstellen.

erstellen und für diese jeweils eine Verknüpfung auf dem Desktop anlegen, können Sie in sekundenschnelle zwischen den verschiedenen Einstellungen wechseln.

Hinweis: Für das Ausführen der Scripte werden Administrator-Rechte benötigt. Da Sie aus Sicherheitsgründen vorrangig mit einem eingeschränkten Benutzerkonto arbeiten sollten (siehe Material zum Selbstdatenschutz – Teil 1), können Sie die Skripte mit dem Tool **MachMich-Admin (www.heise.de)** direkt und ohne Anmeldung als Administrator ausführen lassen.

Unsichtbar hinter Mauern – Mit Firewalls das eigene Netzwerk schützen

Lara und ihre Mitstudentin haben sich verabredet, um gemeinsam im Internet für ihr neues Projekt zu recherchieren. Mit dem Notebook und ohne Kabel gelangt Lara bequem ins Internet – doch das Surfvergnügen endet jäh, als wieder einmal die Verbindung zusammenbricht. Dies ist nicht das erste mal, woran das nur liegen mag?

Das Problem

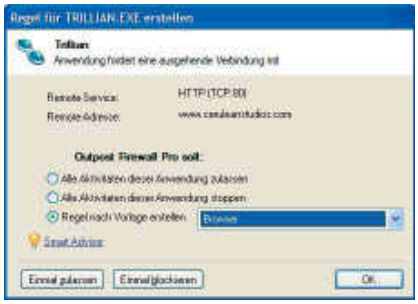
Nicht nur die WLAN-Komponenten Ihres Netzwerkes sind Gefährdungen ausgesetzt. Sie müssen Ihre mit dem „World-WideWeb" verbundenen Rechner auch vor direkten Angriffen aus dem Internet schützen. Von jedem Ort und zu jeder Zeit kann Ihr System von Dritten auf Schwachstellen untersucht und unter Umständen korrumpiert werden.

Die Lösung

Zur Absicherung von Netzzugängen werden „Firewalls" eingesetzt. Sie haben die Aufgabe, den Datenverkehr zu kontrollieren und unberechtigte Zugriffe zu sperren. Firewalls können die verschiedensten Funktionalitäten aufweisen und sowohl direkt am Router als auch am einzelnen Rechner zum Einsatz kommen.

Jeder mit **Windows XP** betriebene Rechner beinhaltet eine Internetverbindungsfirewall, die standardmäßig bei jedem Systemstart aktiviert wird. Sie wehrt Angriffe von außen ab, kann allerdings nur in sehr geringem Umfang konfiguriert werden.

Die meisten **Router** sind heutzutage ebenfalls mit einer Firewall ausgestattet, mit deren Hilfe sich der Netzwerkverkehr auf verdächtige Aktivitäten überwachen lässt. Prüfen Sie daher, ob die Firewall in Ihrem Router aktiviert ist.
Auf jeden Fall arbeitet Ihr Router mit einer **integrierten Adressumwandlung** (Network Adress Translation). Hierdurch werden die IP-Adressen Ihrer im Netzwerk angeschlossenen Rechner (198.162.xxx.yyy) nach außen geheimgehalten.
Mittels eines sogenannten **Paketfilters** werden darüberhinaus die Quell- und Zieladressen einer Internetverbindung kontrolliert und nur aus dem lokalen Netzwerk initiierte Kommunikationsbeziehungen zugelassen. Unerlaubte Anfragen aus dem Internet werden abgewiesen.



Die Firewall „Outpost" meldet den Versuch, dass ein Programm die Verbindung mit dem Internet herstellen will.

Aktivierte Windows- und Routerfirewall stellen den Mindestschutz dar, den Sie für Ihr System einrichten sollten.

Die soweit beschriebenen Mechanismen bieten jedoch **nur einen gewissen Schutz gegen Angriffe von außen**. Sie verhindern z.B. nicht, dass auf einem Rechner installierte Schadsoftware unbemerkt und ohne Ihr Wissen persönliche Daten in das Internet verschickt!
Speziell hierfür existieren sogenannte **Anwendungsfilter**, die auch den ausgehenden Datenverkehr kontrollieren und Sie in die Lage versetzen selbst zu entscheiden, ob eine Anwendung Kontakt mit dem Internet herstellen darf oder nicht.
Weitere Firewallfunktionalitäten (Contentfilter; Stateful Packet Inspection etc.) ermöglichen noch komplexere Eingriffe.

Machen Sie sich mit der Arbeitsweise Ihrer Router-Firewall vertraut. Falls Ihnen der zur Verfügung stehende Funktionsumfang nicht ausreicht, denken Sie über den Einsatz einer Desktop-/ oder Personal-Firewall nach.
Diese sind zur Installation auf dem jeweiligen PC bestimmt und können teilweise kostenlos aus dem Internet heruntergeladen werden (zum Beispiel unter **www.zonelabs.de**).

Hinweis: Wenn Sie eine andere als die in Windows XP integrierte Firewall nutzen, müssen Sie auf jeden Fall die windowseigene Firewall im Sicherheits-Center deaktivieren. Ansonsten kann es passieren, dass die von Ihnen installierte Firewall nicht ordnungsgemäß funktioniert!

NetBIOS und Co. – Überflüssige Dienste und Protokolle entfernen

Bernd, Lara und Julian sind froh, dass das WLAN relativ problemlos in Betrieb genommen wurde, die beiden PCs und das Notebook im Heimnetzwerk integriert sind und auch das Internet für jeden nutzbar ist. Schließlich hatte Bernd keine Mühen gescheut und mit einigem, allerdings vertretbarem Aufwand alles getan, um das Funknetzwerk gegen Angriffe von außen zu schützen.
Doch was ist mit den DFÜ-Einstellungen, die Bernd zu Modem-Zeiten vorgenommen hatte? Können diese einfach beibehalten und unverändert übernommen werden?

Das Problem

Da in einem Netzwerk i.d.R. der Router (und nicht ein Modem) die Einwahl in das Internet übernimmt, werden evtl. vormals eingerichtete DFÜ-Verbindungen nicht weiter benötigt und können eigentlich gelöscht werden.
Unter Umständen ist es jedoch sinnvoll, eine vorhandene DFÜ-Verbindung für den Fall beizubehalten, dass bei einem Ausfall des Routers die Internetverbindung notfalls wieder über ein Modem hergestellt werden soll.
Wer sich diese Option offenhalten will, sollte auf jeden Fall den DFÜ-Adapter zusätzlich absichern – sonst besteht die Gefahr, dass „Würmer" das Netzwerk befallen und Schaden auf den einzelnen Rechnern anrichten. Im Gegensatz zu herkömmlichen Viren, die ein Trägerprogramm benötigen und sich oftmals im Anhang einer E-Mail verstecken, sind Würmer in der Lage, sich selbständig in einem Netzwerk auszubreiten. Eine schlecht konfigurierte DFÜ-Verbindung kann dann das Einfallstor für diese Schädlinge darstellen.

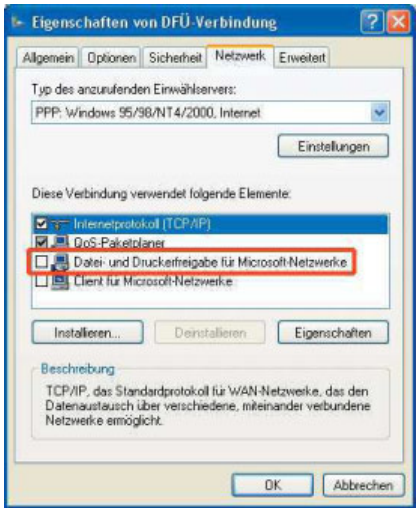
Die Lösung

1) Löschen der DFÜ-Verbindung

Für den Fall, dass Sie eine vorhandene DFÜ-Verbindung nicht mehr benötigen, empfiehlt es sich, diese aus der Netzwerkverbindung zu entfernen.
Klicken Sie hierzu auf **Start → Einstellung → Systemsteuerung** und anschließend auf **Netzwerk- und Internetverbindungen.** Klicken Sie auf **Netzwerkverbindungen** und wählen Sie die DFÜ-Verbindung aus, die Sie entfernen wollen (Vorsicht! Verwechseln Sie nicht die DFÜ-Verbindung mit der LAN-Verbindung!). Klicken Sie unter **Netzwerkaufgaben** auf **Verbindung löschen** und bestätigen Sie die Nachfrage mit **OK**.

2) Protokolle deaktiveren

Wollen Sie eine DFÜ-Verbindung beibehalten, um sie ggf. weiter verwenden zu können, sollten Sie in den Einstellungen der DFÜ-Verbindung die **Datei- und Druckerfreigabe** sowie das **NetBIOS**-Protokoll deaktivieren.
Klicken Sie auf **Start → Einstellungen → Systemsteuerung** und anschließend auf **Netzwerk- und Internetverbindungen.** Klicken Sie auf **Netzwerkverbindungen,** dann auf die DFÜ-Verbindung und dort auf **Einstellungen dieser Verbindung ändern**. Wechseln Sie zum Reiter **Netzwerk** und entfernen Sie das Häkchen vor **Datei- und Druckerfreigabe für Microsoft-Netzwerke**. Klicken Sie anschließend auf **Internetprotokoll (TCP/IP)**, dann auf **Eigenschaften**. Wenn Sie auf **Erweitert** klicken, öffnet sich ein neues Fenster. In diesem wechseln Sie zum Reiter **WINS** und markieren die Option **NetBIOS über TCP/IP deaktivieren**. Bestätigen Sie die Änderungen mit **OK**.



Deaktivieren Sie in den DFÜ-Verbindungen die Datei- und Druckerfreigabe.

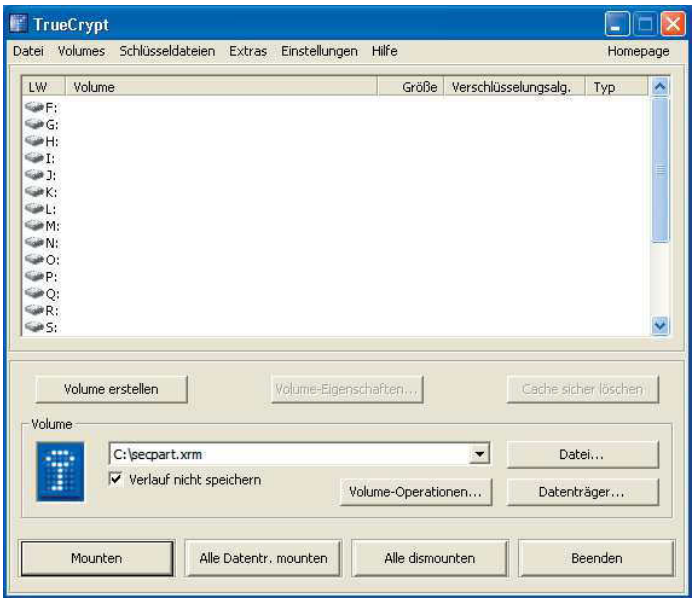
Deaktivieren Sie NetBIOS in den erweiterten Einstellungen für „TCP/IP".

„Was niemand weiß...“ – Ein Geheimtresor für vertrauliche Daten

Lara weiß, dass ihr Bruder Julian manchmal ziemlich neugierig sein kann. Und auf ihrem Notebook sind einige Daten gespeichert, die ihn wirklich nichts angehen; z.B. die E-Mails ihres neuen Freundes. Da sie Julian schon einmal beim Herumstöbern erwischt hat, scheint ihr die normale Speicherung auf der Festplatte nicht ausreichend sicher. Doch wohin mit den heimlichen Botschaften?

Das Problem

Vertrauliche Dokumente auf dem PC zu speichern bleibt stets mit einem Risiko behaftet. Trotz aller Zugangsbeschränkungen bestehen immer auch Möglichkeiten, dass sich Unbefugte Zugang zu Ihren Daten verschaffen können. Besitzer eines Notebooks sind von diesem Problem besonders betroffen, da ihre Hardware einem höheren Diebstahl- und Verlustrisiko ausgesetzt ist. Aber auch wenn die Festplatte im Falle eine Reparaturmaßnahme auf Wanderschaft geht, stellt sich die Frage, wie dem Missbrauch vertraulicher Daten am besten vorgebeugt werden kann.



Mit TrueCrypt erzeugte Containerdateien können in sekundenschnelle verschlüsselt werden – sogar per Tastenkombination.

Die Lösung

Sollen Dokumente mit geheim zu haltenden Inhalten neugierigen Blicken entzogen werden, bietet sich als wirksamster Schutz die verschlüsselte Datenspeicherung an. Dateiinhalte können dann nur von den Personen eingesehen werden, die im Besitz des richtigen Passwortes sind – allen anderen bleibt der Zugriff verwehrt.

Datei- und Festplattenverschlüsselungsprogramme gibt es eine Menge und auch Windows XP sieht eine Verschlüsselungsvariante vor, die jedoch nur unzureichenden Schutz bietet.
Mit dem quelloffenen und kostenlosen Tool **TrueCrypt (www.truecrypt.org)** sind Sie jedoch auf der sicheren Seite. Mit Hilfe dieses Programms lässt sich eine sogenannte Containerdatei erstellen, die Sie als „Datentresor“ nutzen können. Die Inhalte des Containers werden nach einem von mehreren zur Auswahl stehenden Verfahren verschlüsselt und sind nur mit weiteren „Spezialkenntnissen“ zugänglich (Speicherort, Passwort etc.).
Das Programm steht unter der o.g. Internetadresse zum Download in der englischen Version zur Verfügung und kann mit einem deutschen Sprachpaket versehen werden.

Für das Erstellen eines Standard-Containers gehen Sie wie folgt vor:
Starten Sie TrueCrypt und klicken Sie auf den Button **Volume erstellen**. Es erscheint ein Assistent, der Sie beim Erstellen einer Containerdatei unterstützt. Klicken Sie auf **Weiter** und vergeben Sie einen Namen für die Datei, die als Container dienen soll.
Hinweis: Wird anstelle einer einzelnen Datei eine komplette Partition ausgewählt, so werden alle bisher dort befindlichen Daten gelöscht!
Bestimmen Sie anschließend die Methode zur Datenverschlüsselung und klicken Sie auf **Weiter**. Legen Sie nun eine ausreichende Dateigröße fest. Das ebenfalls zu vergebende Kennwort ist nachträglich änderbar. Als Dateisystem wählen Sie **NTFS** und klicken auf **Formatieren**. Die Einrichtung des Containers ist damit abgeschlossen.

Bevor hier jedoch Dateien abgelegt werden können, muss die Containerdatei „zugänglich“ gemacht werden. Dafür muss sie jeweils unter Eingabe des vereinbarten Kennwortes als Laufwerk „gemountet“ werden. Das bedeutet, Ihr Datentresor bekommt einen Laufwerksbuchstaben zugewiesen und erscheint im Windows Explorer als virtuelle Festplatte.
Klicken Sie im Hauptfenster auf den Button **Datei** und wählen Sie die Containerdatei aus, die Sie soeben erzeugt haben. Legen Sie einen Laufwerksbuchstaben fest und klicken Sie auf **Mounten**. Wenn Sie das richtige Passwort eingeben, wird der Inhalt des Containers im Explorer angezeigt und steht für die Ablage Ihrer vertraulichen Daten zur Verfügung.
Mit dem Button **Alle dismounten** wird die Laufwerksverbindung wieder getrennt und der verschlüsselte Containerinhalt ist für Unbefugte nicht zugreifbar.

Machen Sie sich mit den weiteren Konfigurationsmöglichkeiten von TrueCrypt vertraut und verfeinern Sie Ihre persönliche Datensicherheitsstrategie!

Glossar –
Die wichtigsten Begriffe und Abkürzungen

13

Access Point
Der Access Point (*engl.* Zugangspunkt) dient in einem WLAN als Basisstation, mit dessen Hilfe ein WLAN an ein kabelgebundenes Netzwerk (LAN) angeschlossen werden kann. In WLAN-Routern ist der Access Point bereits integriert und braucht daher nicht zusätzlich als externes Gerät angeschlossen werden.

DHCP (Dynamic Host Configuration Protocol)
Dieser Dienst ermöglicht die automatische Zuweisung von IP-Adressen in einem Netzwerk, wodurch die Konfiguration des Netzwerkes und die Einbindung neuer Computer stark vereinfacht wird.

DNS Server (Domain Name Server)
Ein Domain Name Server ist für die Umwandlung von Internet-Domain-Adressen in IP-Adressen zuständig. Damit sich Internetnutzer keine komplizierten IP-Adressen merken müssen, wurde das *Domain Name System* eingeführt. Es erlaubt, einen Rechner über seinen zugehörigen Domain Namen (z.B. datenschutz.de) aufzurufen. Domain Name Server verwalten die Informationen, in denen die IP-Adressen und die Rechnernamen einander zugeordnet sind.

IP-Adresse (Internet Protocol Adresse)
Die IP-Adresse ist eine Art Nummernschild, das jeder Rechner erhält, wenn er die Verbindung zum Internet herstellt. Auf diese Weise können die Rechner weltweit miteinander kommunizieren, da jedes Datenpaket mit der IP-Adresse sowohl des Senders als auch des Empfängers versehen wird.

LAN (Local Area Network)
Unter einem LAN versteht man ein räumlich begrenztes Netzwerk, bei dem mehrere Computer über Kabel- oder Funkverbindung miteinander vernetzt werden.

MAC-Adresse (MAC = Media Access Control)
Die MAC-Adresse ist eine vom Hersteller vorgegebene und in der Regel unveränderbare Hardwarekennung, die in allen Netzwerkkarten (LAN oder WLAN) fest implementiert ist und zur eindeutigen Identifikation des Geräts im Netzwerk dient.

NAT (Network Adress Translation)
Network Adress Translation kommt zum Einsatz, wenn ein lokales Netzwerk mit dem Internet verbunden wird. Dabei erhält jeder Rechner im Netzwerk eine eigene, private IP-Adresse. Werden Daten vom lokalen Netzwerk an das Internet verschickt, wird bei jedem Datenpaket die IP-Adresse des Rechners gegen die des Routers ausgetauscht. Da der Router stellvertretend die Daten an das Internet weiterleitet, bleibt das lokale Netzwerk für das Internet unsichtbar.

Router
Ein Router ermöglicht es, unterschiedliche Netzwerke miteinander zu verbinden. Der Router besitzt für jedes angeschlossene Netzwerk eine eigene Schnittstelle und leitet die Datenpakete eigenständig von einem Rechner (Sender) zu einem anderen (Empfänger) weiter. Router werden häufig eingesetzt, um das lokale Netzwerk mit dem Internet zu verbinden.

SSID (Service Set Identifier)
Damit mehrere Funknetzwerke identifiziert und voneinander unterschieden werden können, besitzt jedes WLAN eine frei konfigurierbare SSID, anhand derer über die Zugehörigigkeit zu einem bestimmten WLAN entschieden wird. Nur solche Wireless-Komponenten können sich zu einem Netzwerk zusammenschließen, die die gleiche SSID besitzen.

WLAN (Wireless Local Network)
Unter WLAN versteht man ein drahtloses, lokales Funknetzwerk. Es kann sowohl im Infrastruktur-Modus (unter Einsatz eines Access Points) als auch im Ad-hoc-Modus betrieben werden. Aufgrund der fehlenden Kabelverbindungen stellt ein WLAN besonders hohe Anforderungen an die Sicherheit.

Checkliste –
Worauf Sie achten sollten (im Überblick)

Grundsätzlich	ja	nein
Haben Sie die Möglichkeit zur Fernadministration Ihres Routers deaktiviert ?		
Wird das automatische Aussenden der SSID Ihres WLANs unterbunden ?		
Ist die Standard-SSID-Bezeichnung umbenannt worden ?		
Wurde für Ihr Netzwerk DHCP deaktiviert und stattdessen manuell eine IP-Adressenvergabe vorgenommen ?		
Haben Sie an Ihrem Router eine MAC-Adressen-Filterung eingerichtet ?		
Erfolgt die Datenübertragung in Ihrem WLAN auf höchstmöglicher Verschlüsselungsstufe ?		
Wurden Sendeleistung und -dauer des WLAN-Routers auf das notwendige Maß begrenzt ?		
Gehen Sie mit Ihren Netzwerkfreigaben bewußt und sparsam genug um ?		
Haben Sie die Ihnen zur Verfügung stehenden Firewall-Funktionalitäten von PC und Router geprüft, bewertet und aufeinander abgestimmt ?		
Haben Sie in Ihrer Netzwerkkonfiguration nicht mehr benötigte DFÜ-Verbindungen gelöscht oder zumindest angepasst ?		
Verschlüsseln Sie besonders vertrauliche Daten, die Sie auf der Festplatte speichern ?		
Sind Ihre Passwörter lang genug und haben die nötige Komplexität ?		
Regelmäßig	**ja**	**nein**
Ist für die Firmware Ihres Routers ein Update des Herstellers verfügbar ?		
Haben Sie das Zugangspasswort für Ihren Router geändert ?		
Sind Ihre persönlichen Daten als aktuelle, extern gespeicherte Kopie gesichert ?		
Ist der WEP-Schlüssel (falls verwendet) durch einen neuen Schlüssel ersetzt worden ?		