

Sommerzeit ist Wireless-Zeit

Christian Funk

Inhalt:

Einführung

Unter der Oberfläche

Folgen

Verschlüsselung von Datenverkehr

Grundlegende Sicherheitsvorkehrungen

Fazit

Einführung

Endlich Urlaub! Wer kennt es nicht: der Koffer ist gepackt und natürlich haben Sie auch an Ihren Laptop gedacht. Schließlich ist der Computer mittlerweile aus dem Alltag nicht mehr wegzudenken. Und im Urlaub hat man ja auch schön Zeit: Fotos wollen geordnet und archiviert sowie private (und berufliche) E-Mails während der Abwesenheit abgerufen werden. Das Hotel am Urlaubsort bietet einen WiFi-Internetzugang, was einer der Hauptgründe für die Entscheidung war, dieses Hotel und nicht eine Ferienwohnung zu buchen. Es scheint nämlich mittlerweile essentiell, immer auf dem letzten Stand und dem Laufenden zu sein – dieser Informationszwang macht auch vor der Urlaubszeit nicht halt.

Heil am Urlaubsort und im Hotelzimmer angekommen, öffnen Sie also als erstes Ihren Laptop, aktivieren die WLAN-Karte und lokalisieren das Netzwerk des Hotels. In Ihrer Reichweite stehen mehrere Zugangspunkte zur Verfügung und Sie wählen denjenigen aus, bei dem der Hotelname im SSI-Funknetzwerk (Service Set Identifier) erscheint. Ist die Verbindung hergestellt, wird wie üblich als erste Seite die Login-Seite des Hotels angezeigt. Hier werden Sie aufgefordert, eine Zahlungsart auszuwählen. Und wie es das „richtige Urlaubsfeeling“ will, ist der Preis für das Internet-Surfen im Hotel exorbitant hoch. In unserem Fall berechnet das Hotel 20 Euro für eine 24-stündige Verbindung. Das ist genauso viel, wie heutzutage ein DSL-Highspeed-Zugang in einem ganzen Monat kostet. Aber im Hotel haben Sie nun mal keine andere Wahl – oder vielleicht doch? Ein weiterer Zugangspunkt in Reichweite, der mit hohen Übertragungsraten und außerordentlicher Sicherheit wirbt, liest sich verlockend – und all das für den scheinbar lächerlichen Preis von nur sechs Euro pro Tag. Preisbewusst wie immer, entscheiden Sie sich für diese Verbindung, wählen „Kreditkarte“ als Zahlungsart und voller Freude über dieses Schnäppchen, geben Sie arglos Ihre Kreditkartendetails ein.

In Sekundenschnelle haben Sie via Internet Zugang zur großen weiten Welt. Sie rufen Ihre E-Mails ab und erinnern sich daran, dass Sie ja eigentlich noch nach dieser einen Digitalkamera, die Sie gestern gesehen haben, schauen wollten. Also auf zum Preisvergleich. Wie üblich vergleichen Sie die lokalen Preise mit denen der Online-Shops. Sie stellen fest, dass die Preise am Urlaubsort weit über dem Angebot Ihres Lieblingsshops im Internet liegen. Also beschließen Sie, die Kamera direkt zu bestellen, um so für Ihren nächsten Urlaub auf jeden Fall optimal gerüstet zu sein. Und weil es so bequem ist, bezahlen Sie gleich noch einmal mit Ihrer Kreditkarte.

Die oben beschriebene Situation ist typisch und wird dem einen oder anderen vielleicht bekannt vorkommen. Es gibt wohl nur wenige Personen, die bei der Verwendung eines unbekanntes Zugangspunktes Bedenken hinsichtlich der Sicherheit haben. In den meisten Fällen aber denkt niemand zweimal nach. Was könnte schließlich auch schief gehen?

Auch wenn die Antwort „nichts“ zu lauten scheint, lauern hier in Wirklichkeit erhebliche Risiken, die im Nachfolgenden genauer behandelt werden.

Unter der Oberfläche

Die in diesem Beispiel beschriebene Szene ist unter der Bezeichnung „Man-in-the-middle“-Angriff bekannt. Irgendjemand erstellt eine simple Login-Seite in der Absicht, dem Benutzer eine offiziell

wirkende WiFi-Login-Maske zu präsentieren. Es kommt auch vor, dass gleich die hoteleigene Seite komplett kopiert wird. Letzteres erfordert kein besonderes Spezialwissen. Diese Zugangspunkte können mittels vieler handelsüblicher WiFi-Router und modifizierter Firmware oder einem Laptop mit aktivierter WiFi-Verbindung und Zugang zu einem Ad-hoc-Netzwerk, nachgemacht werden. Hinter der gefälschten Seite steht dann immer eine bereits eingeloggte Internetverbindung, die den Nutzer glauben machen soll, dass der Login-Prozess ohne Probleme erfolgt – und die Datendiebe haben leichtes Spiel.

Ab diesem Zeitpunkt können sämtliche eingegebenen Daten von den Cyberkriminellen abgefischt werden. Mit derartigen Angriffen kommen sie nicht nur an sensible Kreditkarteninformationen – sie können damit auch weitere Informationen über E-Mail-Accounts, Online-Shops oder Finanzinstitutionen sammeln.

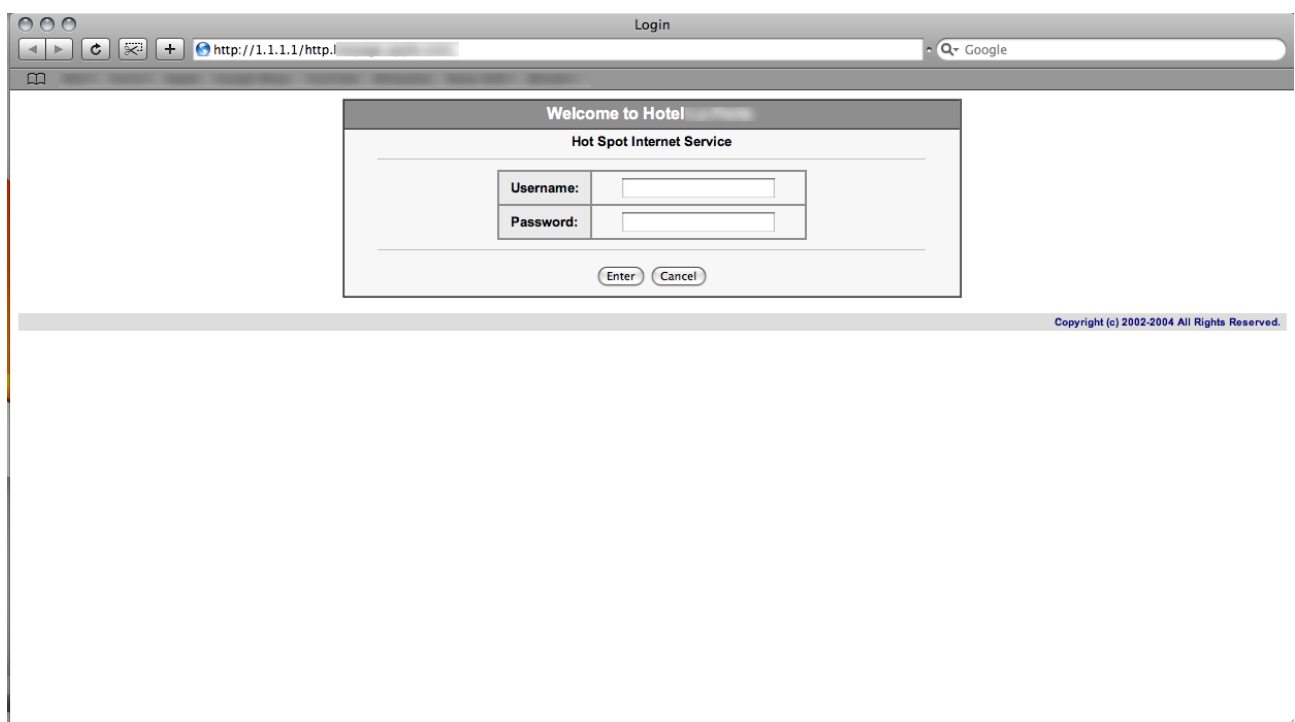


Abb. 1: Login-Seite des Hotels mit Prepaid-Zugang

Nun heisst es für die Betrüger abwarten, denn selbst wenn nur eines der potentiellen Opfer der Versuchung erliegt, haben sich ihre Anstrengungen mehr als nur ausgezahlt. Aus Opfersicht wäre es letztendlich doch preiswerter gewesen, die etwas höheren Kosten für eine echte, vom Hotel angebotene WiFi-Verbindung zu bezahlen. Aber auch solche legitimen Netzwerke sind nicht hundertprozentig risikofrei.

Da Daten nicht über ein physisch begrenztes Medium übertragen werden, können sie leicht abgefangen werden. Mit speziell zu diesem Zweck erstellten Programmen werden Datenpakete direkt aus der Luft gefischt und – vorausgesetzt, dass sie nicht verschlüsselt sind – leicht und unverzüglich ausgewertet werden. Die Reichweite hängt dabei sowohl von der Signalstärke des Zugangspunkts als auch von der Stärke des verwendeten WiFi-Standards ab. Ein handelsüblicher WiFi-Router mit 802.11b-Standard hat eine Reichweite von fast 100 Metern, wobei das Signal in sphärischer Form von dem Gerät ausgeht. Mauern und andere Objekte verringern zwar seine Reichweite, jedoch wird der Dienst nicht auf das Gebäude, in dem sich der Router befindet, beschränkt sein. Das bedeutet gewöhnlich, dass die Daten von außerhalb des Gebäudes, beispielsweise von der Straße aus, abgefangen werden können.

Die oben angeführte Entfernung gilt allerdings nur für die interne Antenne einer Netzwerkkarte. Spezielle Nachrüstantennen sind in der Lage, nahezu jedes noch so schwache Signal zu empfangen,

was ihre Reichweite erheblich vergrößert. Mikrowellenantennen können die Übertragungsentfernung gar um ein Vielfaches erhöhen. Anleitungen zum Nachbauen derartiger Antennen findet man überall im Internet und der Eigenbau erfordert lediglich elementarste Materialkenntnisse. Vor allem aber bedeutet er einen sehr geringen Arbeitsaufwand – ein lohnendes Mini-Max-Prinzip für Cyberkriminelle.

Zahlreiche der als Snifferprogramme bekannten Programme enthalten auch Funktionen für die Auswertung von SSI-verschlüsselten Daten, so dass sogar die Integrität von vermeintlich sicheren Verbindungen zu Login-Seiten nicht mehr gewährleistet ist. Abhängig von dem Grad der verwendeten Verschlüsselung ist der Aufwand für Cyberkriminelle unter Umständen nicht sehr groß. Ein Aufwand, den sie betreiben, während ihre Opfer sich in falscher Sicherheit wähnen und Bankgeschäfte abwickeln oder E-Mail-Accounts prüfen.

Folgen

Die möglichen Folgen für das Opfer eines „Man-in-the-middle“-Angriffs variieren je nach den im Laufe einer Sitzung durchgeführten Transaktionen.

In unserem Beispiel werden zunächst die Login-Daten für das E-Mail-Konto erfasst. Damit ist es möglich, den Account auf eine Liste zu setzen, die dann für den Massenaussand von Spam benutzt wird. Die Eingabe der Zugangsdaten zu einem Account bedeutet ferner, dass der Angreifer persönliche Daten in den E-Mails ausspionieren kann. So erhalten Nutzer beispielsweise gewöhnlich eine E-Mail-Nachricht mit ihren neuen Zugangsdaten, wenn sie sich für Online-Shops, soziale Netzwerke oder Internetforen registrieren. Handelt es sich bei einem E-Mail-Konto um einen beruflich genutzten Account, ist der potentielle Schaden weitaus gravierender. Beim Diebstahl finanzbezogener Daten ist nicht nur der erlittene Verlust extrem schwer zu beziffern. Es dauert in manchen Fällen sogar Jahre, bis das tatsächliche Ausmaß des Schadens beurteilt werden kann. Hat ein Angriff dieser Art den Zugriff auf sensible Informationen zum Ziel – etwa Geschäftsberichte, technische Informationen oder gar Kundendaten – die gestohlen und veröffentlicht werden, sind die Auswirkungen auf das Ansehen des Unternehmens gewöhnlich katastrophal: Mögliche Schäden sind hier Vertrauensverlust bei Kunden und Geschäftspartnern oder Umsatzrückgänge bis hin zum Zusammenbruch von Geschäftsbeziehungen. Besondere Vorsicht ist daher immer geboten, wenn von externer Stelle auf ein Geschäftskonto zugegriffen wird.

Wenn Kreditkartendetails in die falschen Hände geraten, sind die Folgen zumeist besonders schwerwiegend. Mit den Daten können auf der ganzen Welt Waren und Dienstleistungen eingekauft werden – natürlich immer auf Kosten des Opfers und solange, bis das Verbrechen bemerkt wird. Das wiederum geschieht häufig erst am Monatsende, wenn die monatliche Abrechnung ins Haus flattert. Grundsätzlich erstattet das Kreditkartenunternehmen dem Opfer den entstandenen Schaden zurück, immer vorausgesetzt, dass es nachweisen kann, die Einkäufe nicht selbst getätigt zu haben und mit den Karteninformationen nicht grob fahrlässig umgegangen zu sein. Der erste Punkt ist meist recht einfach belegt. Die Beweiserbringung für den zweiten Punkt gestaltet sich schon schwieriger und wird auch von Kreditinstitut zu Kreditinstitut unterschiedlich gehandhabt. Selbst wenn man letztendlich Erfolg hat und für seine Verluste entschädigt wird, kann das Ganze eine Menge Zeit und Ärger kosten. Andererseits wird die Online-Zahlung über eine unsichere WLAN-Verbindung – ob nun bewusst oder unbewusst – mit Sicherheit als unvorsichtig oder sogar grob fahrlässig ausgelegt werden. In solchen Fällen muss das Opfer diese kostspielige Lektion lernen und die Kosten selbst tragen.

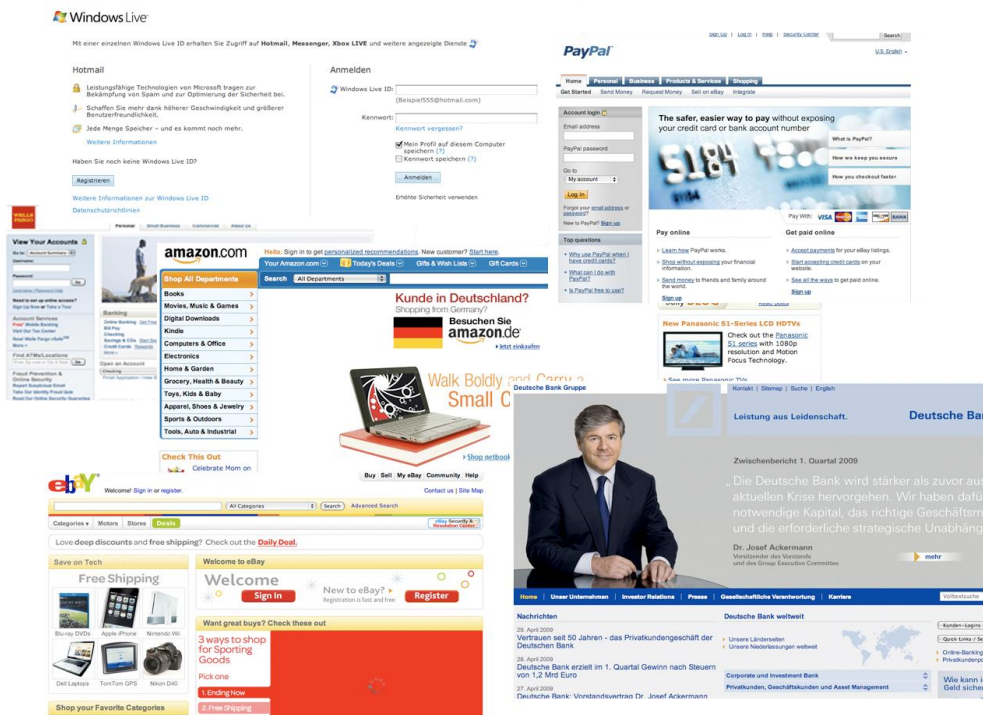


Abb. 2: Login-Seiten

Die meisten Websites mit einem Login-Bereich sind mittels SSL geschützt. Zwar stehen Cyberkriminellen eine Fülle von Tools zur Verfügung, mit denen diese Verschlüsselungsart geknackt werden könnte, aber trotzdem bleiben einige Login-Daten auch weiterhin vor Ihnen verborgen. Es existieren allerdings noch andere Wege, sich Zugang zu derartigen Daten zu verschaffen. Schon bevor die Zugangsdaten ins Internet übertragen werden, können sie mittels Spyware oder einem einfachen Keylogger lokal auf dem Opfercomputer ausgelesen werden. Loggt sich ein Benutzer in die vermeintliche Hotspot-Site ein, ist die Ausführung eines sogenannten Drive-by-Downloads ein regelrechtes Kinderspiel. Dafür muss lediglich JavaScript, IFrame oder ein Browser-Exploit in den HTML-Quellcode einer manipulierten Seite eingebaut werden. Der Schadcode wird dann direkt auf den Opfercomputer heruntergeladen. Die Infizierung des Rechners mit Schadsoftware stellt den freien Zugang für die Internetbetrüger sicher. Das Ausmaß des Schadens, der durch diese Art von Programmen angerichtet werden kann, ist ausschließlich durch die Fantasie des Malware-Autors begrenzt.

All das kann sich in Sekundenschnelle abspielen, ohne dass der Benutzer etwas Ungewöhnliches bemerkt. Derartige Angriffe stehen heute im schieren Gegensatz zur Vergangenheit, als Malware- und Netzwerkattacken ausschließlich benutzt wurden, um Schäden auf Computern anzurichten. Damals konnte man seltsame Vorgänge am Rechner noch erkennen. Diese Ära ist allerdings schon lange vorbei. Heutzutage versuchen Internetbetrüger, unbemerkt zu bleiben, um über einen langen Zeitraum so viele sensible Daten wie möglich abfischen können.

Benutzer haben jedoch immer die Möglichkeit, sich vor derartigen Angriffen zu schützen. Im Folgenden werden zunächst mehrere Optionen für die Verschlüsselung und Konfigurierung des Betriebssystems analysiert, da mit Hilfe dieser Strategie potentielle Schwachstellen in öffentlichen Netzwerken beseitigt werden können.

Verschlüsselung von Datenverkehr

Die wirksamste Methode für die Verschlüsselung von zu versendenden Daten ist die Verwendung eines VPN (Virtual Private Network). Einfach ausgedrückt besteht ein derartiges Netzwerk darin, dass ein sogenannter VPN-Tunnel zwischen einem Laptop (dem Client-Computer) und einem zugeordneten Netz oder Server aufgebaut wird. Sämtlicher Datenverkehr zwischen diesen beiden

Punkten erfolgt in verschlüsselter Form. Jegliche dazwischen geschalteten Geräte, die die Datenpakete verarbeiten oder weiterleiten, können diese Inhalte somit nicht interpretieren. Darüber hinaus wird der gesamte Daten-Traffic unter Umgehung aller durch den Hotspot-Betreiber blockierten Ports über diese Verbindung verarbeitet. Oftmals wird der für HTTP-Anfragen genutzte Port 80 nicht blockiert, während andere Ports, wie zum Beispiel Instant Messaging oder über POP3 oder IMAP gesendeter E-Mail-Verkehr gesperrt werden.

Der VPN-Server agiert als Zielverbindung und muss daher ein vertrauenswürdiger Computer, also Teil einer sicheren Umgebung, sein. Dieser Server funktioniert als eine Art „verlängerter Arm“ des Client-Computers, indem er Anfragen an den Zielservers im Internet übermittelt und den gewünschten Inhalt in verschlüsselter Form zurück sendet. Mit dem klassischen Ansatz der Eingabe von Benutzernamen plus Passwort können sich die Nutzer in das VPN-System einloggen. Dieser VPN-Servertyp kann auf unterschiedlichste Art und Weise eingerichtet werden. Mit dem nötigen Fachwissen ist das für jedermann problemlos machbar. Wählt man den Standort des Rechners aus, der als Plattform dienen soll, bieten sich grundsätzlich drei Varianten an:

Der geleaste Computer in einem Rechenzentrum: Diese Option gilt für physische und virtuelle Server und ist insbesondere für Personen attraktiv, die diese Art von Computern bereits nutzen, etwa als Host für ihren eigenen E-Mail- oder Webserver. Hierfür ist eine statische IP-Adresse erforderlich, um jederzeit eine Verbindung aufbauen zu können. Wird dagegen eine dynamische IP-Adresse verwendet, muss DynDNS genutzt werden. Virtuelle Server sind besonders attraktiv, da sie bereits ab zehn Euro monatlich zu haben sind und der VPN-Server-Dienst nur sehr geringe Ressourcen in Anspruch nimmt. Dennoch ist der Anstieg des Datenverkehrs unbedingt zu berücksichtigen, denn im Falle einer VPN-Kommunikation werden sämtliche Daten über diesen Server geleitet.

Alternativ kann der Dienst auch von einem Computer zu Hause wahrgenommen werden. Vorausgesetzt, dass man über einen Breitbandanschluss verfügt, kann der externe Computer als Teil des Home-Netzwerks eingebunden werden. Mit dieser Möglichkeit genießt man zudem dem Vorteil, jederzeit auf seine persönlichen Daten zugreifen zu können. Dazu benötigt man aber einen Computer mit Network Shares, der rund um die Uhr eingeschaltet bleibt, oder ein NAS (Network Attached Storage) Speichergerät.

Häufig sind es die Arbeitgeber, die ihren Mitarbeitern VPN-Kommunikation zur Verfügung stellen – vor allem, wenn im jeweiligen Unternehmen Telearbeit möglich ist oder die Mitarbeiter einen großen Teil ihrer Arbeitszeit auf Kunden-Websites verbringen. In solchen Fällen soll den Mitarbeitern mit VPN-Netzwerken ein Tool an die Hand gegeben werden, um von außen berufsbezogene Aufgaben erledigen zu können. Hierzu gehören das Abfragen der beruflichen E-Mail-Accounts oder Zugriff auf Netzlaufwerke beziehungsweise das unternehmenseigene Intranet. Ob der Dienst auch für nicht-arbeitsbezogene Zwecke genutzt werden darf, wird von Unternehmen zu Unternehmen unterschiedlich gehandhabt. Es obliegt den Nutzern, sich entsprechend über die Nutzungsbedingungen zu informieren oder den Serviceadministrator um Hilfe zu bitten.

Weiterhin bieten eine Reihe unterschiedlicher Serviceprovider auch VPN-Dienste für Reisende und mobile Mitarbeiter an. Diese Unternehmen stellen Server zur Verfügung, mit denen zu einem Entgelt von ungefähr zehn Euro pro Monat sichere VPN-Verbindungen aufgebaut werden. Die Bandbreite der angebotenen Tarife ist sehr groß, so dass die Nutzer den am besten für ihre Ansprüche passenden Tarif auswählen können. Auch in diesem Fall sind die Nutzungsbedingungen des jeweiligen Anbieters genau zu beachten.

Ein VPN-Netz verringert zwar die Geschwindigkeit der Datenübertragung. Seit Einführung von Draft-N, mit dem theoretisch WiFi-Übertragungsraten von 300 Mb/s erreicht werden, ist dieser Nachteil mittlerweile aber zu vernachlässigen. Das gilt vor allem dann, wenn keine großen Datenvolumen ausgetauscht werden.

UMTS gilt als eine weitere Option, die dem Nutzer zudem größere Unabhängigkeit verspricht. Hier hat man unabhängig von der jeweiligen WiFi-Technologie Zugang zum Internet, sofern man sich in einer Gegend mit Funksignal-Empfang aufhält. Die Netzabdeckung ist mittlerweile über weite Strecken gewährleistet – in Europa ist der Empfang zu 60 bis 90 Prozent gegeben, wobei der Prozentsatz je nach Land und Ballungsraum variiert. Dies steht in komplettem Gegensatz zu den Hotspots, die trotz

ihrer großen Zahl nur eine kleine Reichweite haben. Die UMTS-Technologie ist inzwischen auch relativ günstig zu haben. So bekommt man einen Basistarif zu ungefähr fünf Euro pro Monat plus providerabhängiges Downloadvolumen beziehungsweise eine Flatrate zu zirka 30 Euro monatlich. Dadurch ist diese Methode der Online-Nutzung mehr als nur preisgünstig, vor allem im Vergleich zu den exorbitanten Kosten eines WiFi-Zugangs im Hotel. Ein weiterer Vorteil besteht in der Kostentransparenz. Böse Überraschungen bei der Ankunft am Urlaubsort sind damit quasi ausgeschlossen.

Während das UMTS-Netzwerk aus Gründen der Kompatibilität auf dem GSM-Standard der zweiten Generation basiert, werden GSM-Systeme der dritten Generation ebenfalls unterstützt. Aus Sicherheitsgründen sind letztere vorzuziehen, da die Algorithmen zur Nutzer- und Netzwerkauthentifizierung optimiert worden sind. Zudem erfüllen Übertragungsraten, die via HSDPA und HSUPA theoretisch bis zu 14.6 Mb/s betragen können, die meisten Anforderungen weitaus besser. Sehr wahrscheinlich wird sich UMTS daher vor allem bei Vielreisenden als willkommene Alternative zur WiFi-Technik durchsetzen, da die Grundtarife statt in kürzeren Zeiträumen auf Monatsbasis abgerechnet werden.

Grundlegende Sicherheitsvorkehrungen

Zusätzlich zu der Verschlüsselung von Daten, die hauptsächlich zum Zweck der Sicherheit erfolgt, sind bei der Konfiguration und Einrichtung eines Computers weitere Aspekte zu beachten:

Um einen problemlosen Datenaustausch zwischen Computern sicherzustellen, können Ordner und Verzeichnisse innerhalb eines Netzwerks gemeinsam genutzt werden – unabhängig davon, ob es sich um ein drahtloses oder drahtgebundenes Netzwerk handelt. Je nach Konfiguration der Daten können Netzwerk-User entweder direkt mittels Lese- und/oder Schreib-Erlaubnis darauf zugreifen oder unter Eingabe eines Benutzernamens und Passworts eine Zugangserlaubnis anfordern. Daher ist es unbedingt notwendig, dass die Datei-Sharing-Funktion nach der Datenübertragung wieder deaktiviert wird. Ist der Vorrat an Musikdateien und anderen Medien für den Urlaub also aufgestockt und sind bestimmte interne Unternehmensdokumente, die man überarbeiten möchte, übertragen, sollte man das Ausloggen nicht vergessen. Man möchte ja nicht all seine Netzwerk-Partner dazu einladen, ungeniert in den eigenen Dateien zu stöbern. Zwar bieten zahlreiche Hotspot-Setups auch Technologien zur Abschirmung jedes Computers von den anderen Teilnehmern im Netzwerk, jedoch existiert keine direkte Methode, das tatsächliche Vorhandensein dieser Funktion auch zu überprüfen.

Obwohl die Deaktivierung aller gemeinsam genutzten Laufwerke die Datensicherheit erheblich verbessert, bleibt immer noch die Gefahr eines direkten Hacker-Angriffs, durch den sämtliche Daten auf dem Computer lesbar gemacht werden. Ein derartiger Angriff ist natürlich immer gefährlich, dreht es sich um sensibler Daten ist das Risiko jedoch um einiges höher. Insbesondere für solche Daten sollte zur weiteren Verbesserung des Sicherheitsniveaus ein Daten-Backup auf andere Speichermedien ausschließlich in verschlüsselter Form erfolgen. Programme zu diesem Zweck sind mittlerweile kostenlos erhältlich und werden als GPL-Software (General Public License) vertrieben. Mit ihnen können verschlüsselte Containerdateien, die sich nur mit einem Passwort öffnen lassen, erstellt werden. Die für die Erstellung dieser Container verwendete Verschlüsselung ist extrem stark. Sogar ein Supercomputer, der die Brute-Force-Methode anwendet, würde Jahre benötigen, sie zu knacken. Eine Voraussetzung für einen ausreichend hohen Schutz ist natürlich ein entsprechend sicheres Passwort. Dieses sollte aus mehr als acht Zeichen bestehen und sowohl Groß- als auch Kleinbuchstaben sowie Zahlen und nicht alphanumerische Symbole enthalten. Auch hier gilt: eine Containerdatei nur bei Bedarf öffnen und unmittelbar darauf wieder schließen. Letztendlich ist auch der sicherste Tresor nutzlos, wenn die Tür offen stehen bleibt. In dem Maße, wie die Sicherheit von WiFi-Netzwerken verbessert wird, haben diese Vorsichtsmaßnahmen einen weiteren Vorteil: Geht der Laptop verloren, bleiben private Daten auch weiterhin privat.

Ein weiterer wichtiger Punkt ist die Implementierung einer effizienten IT-Sicherheitslösung. Ein Basisschutz vor Schadcode sollte zur Standardausrüstung gehören. Für das hier diskutierte Anwendungsgebiet sind zudem auch Module zum Netzwerkschutz, insbesondere eine Firewall und ein HIPS-System (Host Intrusion Prevention System), notwendig. Denn wie gut kann die sicherste Netzwerk-Verbindung sein, wenn bereits das Quellsystem kompromittiert ist? Die Software führt

komplexe Analysen zur Bewertung unbekannter Programme auf dem PC durch. Sie liefert eine Einstufung der Bedrohungen und darauf basierend die Zuordnung von Zugangsrechten. Wird ein Programm als verdächtig eingestuft, erhält es keinen oder nur begrenzten Zugang zu wichtigen Ressourcen wie Betriebssystem, Netzwerk, vertraulichen Daten, Systemprivilegien und bestimmten Geräten. Dadurch wird das Risiko einer Infektion durch Schadcode gemindert.

Für viele Nutzer ein Anlass zur Verzweiflung: In Abständen von wenigen Tagen zeigt eines der installierten Programme – oder auch das Betriebssystem selbst – die Verfügbarkeit eines neuen Updates an. Mit der Installation von Updates ist auch immer unweigerlich eine gewisse Wartezeit verbunden. Einer der Gründe für den Widerwillen der Nutzer gegen Updates liegt darin, dass die mit der Update-Installation am System vorgenommenen Änderungen nur selten sichtbar sind. Dennoch haben sie den wichtigen Zweck, Sicherheitslücken zu schließen und so den Rechner besser vor Angriffen zu schützen. Es ist also von großer Wichtigkeit, sich diese wenigen Minuten in Geduld zu üben und die Updates stets zu installieren – sie dienen letztendlich der eigenen Sicherheit.

Nicht zuletzt darf die Verantwortung für die Verbesserung von Schutz und Sicherheit nicht ausschließlich auf die Technik abgeschoben werden. Die Nutzer selbst müssen ihren eigenen Aktivitäten stets erhöhte Aufmerksamkeit widmen. In diesem speziellen Fall ist es wichtig, abzuschätzen, in welchem Maße man dem WiFi-Netzwerk, mit dem man sich verbinden möchte, vertrauen kann. Das ist nicht immer einfach. Immerhin hat man keine Kontrollmöglichkeit darüber, auf welche Weise Daten übertragen werden und wer möglicherweise darauf zugreifen kann. Grundsätzlich sollte man unbekanntem Netzwerken mit einer gesunden Dosis Skepsis begegnen. Dann kann man entscheiden, was zu tun oder besser zu lassen ist. Manchmal ist es auch durchaus ratsam zu warten, bis ein Zugang zu einem vertrauenswürdigeren Netzwerk zur Verfügung steht.

Fazit

Das Geschäft mit Hotspots boomt. Die Steigerung des Gesamtumsatzes wird von 969 Millionen US-Dollar in 2005 auf 3.46 Milliarden US-Dollar in 2009 geschätzt. Dieser enorme Anstieg ist vor allem auf die wachsende Anzahl an Hotspots zurückzuführen: Gegenüber 100.000 Hotspots in 2005 wird sich ihre Zahl bis 2009 fast verdoppelt haben, wobei das Gaststättengewerbe der am schnellsten wachsende Sektor ist. Während die größten Fast-Food-Ketten mit ihren riesigen WiFi-Installationen das Feld anführen, sind auch Cafés und Restaurants dabei, auf den fahrenden Zug aufzuspringen.¹ Ein Trend mit positivem Echo: In den USA benutzen 25 Prozent der Erwachsenen beziehungsweise 34 Prozent sämtlicher Internet-Nutzer ihren Laptop und einen Hotspot-Service für ihre Online-Aktivitäten, wenn sie sich nicht zuhause oder am Arbeitsplatz befinden.² Diese Entwicklung wurde auch durch die steigenden Verkaufszahlen bei Laptops begünstigt, deren Preise in den letzten Jahren rapide gefallen sind. Tatsächlich wurden im Jahr 2008 zum ersten Mal mehr Laptops als Desktop-Computer verkauft.

Leider übersteigen die derzeit existierenden Methoden zur Verschlüsselung von drahtlosem Datenverkehr häufig das Know-how der User und etwas Ähnliches wie eine Plug-and-Play-Lösung ist hier bisher nicht in Sicht. Würde eine solche Lösung auf den Markt kommen, müsste sie von den Hotspot-Providern akzeptiert und angeboten und schließlich auch von den Betriebssystemen unterstützt werden. Es ist also offensichtlich, dass selbst im Falle der Entwicklung eines Standards dessen Erfolg immer noch von einer ganzen Reihe von zusätzlichen Faktoren abhängt.

Auf nicht-technischer Seite sind Aufmerksamkeit gegenüber aktuellen Sicherheitsthemen und der gesunde Menschenverstand entscheidend für den Schutz der Daten und Systeme. Wenn man einem Netzwerk nicht voll vertrauen kann, was gewöhnlich bei unbekanntem Zugangspunkten der Fall ist, sollte man immer gründlich nachdenken, welche Informationen in die „Außenwelt“ entlassen werden. Wichtig hierbei: Unter diesen Umständen sollten niemals vertrauliche Daten, wie Login-Daten für Online-Banking oder Paypal eingegeben werden. Besser ein wenig übertriebene Vorsicht walten lassen, als am Ende ein leergekäuftes Bankkonto wieder füllen müssen.

¹ <http://www.itfacts.biz/revenue-from-wireless-hotspots-to-reach-969-blm-in-2005-346-blm-in-2009/4941> (Stand 30.04.2009)

² <http://www.itfacts.biz/34-of-us-internet-users-used-wifi-away-from-homework/11477> (Stand 30.04.2009)