Internet unterwegs

Drahtlose lokale Netze, kurz WLAN (Wireless Local Area Networks) erleichtern die mobile Kommunikation: Mit ihnen lassen sich unterwegs unkompliziert E-Mails lesen oder Daten aus dem Firmennetz bearbeiten. Mitarbeiter, die im Außendienst tätig oder häufig auf Geschäftsreisen sind, tauschen – mit Laptop und WLAN ausgestattet – bequem Daten mit Kunden oder Kollegen aus. Auf Messen lassen sich aktuelle Geschäftszahlen abrufen, Aufträge abschicken oder Info-Materialen übermitteln.

Drahtlose Internet-Zugänge (Hotspots) auf Messen, Flughäfen oder in Hotels unterstützen Reisende dabei, schnell und problemlos ins Internet zu gelangen. Die Vorteile dieser mobilen Kommunikation lassen sich aber nur effektiv nutzen, wenn die Sicherheit der IT mitgedacht wird. Zwar bemühen sich die Anbieter der Hotspots um einen reibungslosen Zugang, für einen sicheren Weg ins Internet muss aber jeder Einzelne seinen Beitrag leisten.

Sicherheit herstellen

Folgende Hinweise sollten Sie beachten, um sicher auf Hotspots zuzugreifen:

Einstellungen am Computer

- Die meisten Betriebssysteme wie Windows 2000 oder Linux erlauben es, Benutzern unterschiedliche Rechte zuzuweisen. Wenn Sie Hotspots nutzen, melden Sie sich nicht als Benutzer mit den Rechten eines Administrators an. Der Administrator besitzt im Gegensatz zu einem normalen Benutzer zusätzliche Rechte, die bei einem unerlaubten Zugriff auf den Laptop größere Schäden ermöglichen. Nutzen Sie ein Benutzerkonto mit eingeschränkten Zugriffsrechten.

- Deaktivieren Sie die Datei- und Verzeichnisfreigabe für Netzwerke. Ansonsten haben andere Rechner im WLAN-Funkbereich die Möglichkeit zum Zugriff auf Ihre Festplatte und andere Datenträger.

- Sind Sie auf die Freigabe bestimmter Dateien oder Verzeichnisse angewiesen, so achten Sie darauf, dass Sie z.B. nicht die gesamte Festplatte oder alle Verzeichnisse eines USB-Sticks freigeben. Diese Dateien und Verzeichnisse sollten Sie mit einem sicheren Passwort schützen. Schalten Sie die Anzeige freigegebener Verzeichnisse ab, damit diese für Außenstehende nicht sichtbar sind.

- Für die Internetverbindung wird nur das TCP/IP-Protokoll benötigt. Lassen Sie weitere, nicht benötigte Netzwerk-Protokolle von Ihrem Administrator deaktivieren.

- Beachten Sie die üblichen Sicherheitsvorkehrungen beim Internet- und E-Mail-Zugriff, insbesondere die möglichst restriktive Konfiguration Ihres Webbrowsers, Mail-Clients und Betriebssystems. Das Ausführen aktiver Inhalte (ActiveX, JavaScript) ist – sofern bei der Hotspot-Nutzung möglich – zu deaktivieren, ebenso das Speichern von Formulardaten und Kennwörtern durch den Browser. Fehlermeldungen wegen ungültiger SSL-Zertifikate sollten unbedingt beachtet und daraufhin die Verbindung beendet werden.

- Achten Sie darauf, dass Ihre Software (insbesondere Webbrowser, Mail-Client und Betriebssystem) immer mit den aktuellen Sicherheitsupdates der Hersteller ausgestattet ist.

- Deaktivieren Sie die WLAN-Komponenten stets, wenn Sie mit Ihrem Rechner keinen WLAN-Zugriff mehr benötigen, um unnötige Angriffsmöglichkeiten auf Ihr System zu verhindern.

Einsatz von zusätzlicher Software

- Verwenden Sie eine Personal-Firewall-Software. Diese überwacht bei einer Netzwerkverbindung die Kommunikation zwischen einem PC und der Außenwelt. Konfigurieren Sie die Firewall so, dass Netzwerkzugriffe von außen nach innen unterbunden werden.

- Eine Verbindung zum Firmennetzwerk sollte nur gesichert aufgebaut werden. Dafür empfiehlt sich eine VPN-Verbindung. VPN steht für Virtual Private Network und verschickt die Daten zwischen zwei Computern auf einem sicheren Kanal.

- Statten Sie Ihren Rechner mit einer aktuellen Antivirus-Software aus, die – möglichst automatisiert – stets auf dem aktuellen Stand gehalten wird.

WLAN sicher nutzen

Mit diesen Ratschlägen können Sie öffentliche WLAN-Hotspots nutzen, ohne dass dadurch Unbefugte auf Ihren Laptop zugreifen können. Besonders sensible Daten sollten Sie dennoch nicht auf Laptops mit einer WLAN-Schnittstelle verarbeiten oder speichern – hier empfiehlt sich die Nutzung von geeignet abgesicherten Systemen.

Fragen Sie bei Details zur sicheren Einstellung Ihren IT-Ansprechpartner oder Ihren IT-Dienstleister.

Ein Verzeichnis öffentlicher Hotspots finden Sie unter:
www.portel.de/hotspot_vatm/

IT-Sicherheit für den Mittelstand

Weitere Informationen und aktuelle Hinweise erhalten Sie auf der Website **www.mittelstand-sicher-im-internet.de.** Die gleichnamige Initiative informiert mit umfassenden Hinweisen, wie Unternehmen IT sicher nutzen können. Sie ist ein Angebot des Bundesministeriums für Wirtschaft und Arbeit und des Bundesinnenministeriums.

Informationen zum IT-Grundschutzhandbuch finden Sie auf der Website des **Bundesamtes für Sicherheit in der Informationstechnik** (www.bsi.de/gshb). **Der »Leitfaden IT-Sicherheit«** bietet einen ersten Überblick und steht unter www.bsi.de/gshb/leitfaden zum kostenlosen Herunterladen bereit. Zusätzlich finden Sie zahlreiche technische Hinweise zu IT-Sicherheit.

Mcert (www.mcert.de) unterstützt den Mittelstand per E-Mail-Abo mit verlässlichen, individuellen Sicherheitsmeldungen und leicht verständlichen Handlungsempfehlungen. So wissen auch kleine und mittelständische Unternehmer genau, welche IT-Risiken sie wirklich betreffen und wie sie diese minimieren können.

Das Netzwerk Elektronischer Geschäftsverkehr hilft Ihnen mit Informationen zur Netz- und Informationssicherheit (www.ec-sicherheit.de) und mit Beispielen branchenspezifischer Anwendung (www.ec-net.de). Beratungen und Veranstaltungen runden das Angebot ab. Mit über zwanzig regionalen und drei branchenspezifischen Zentren bündelt das Netzwerk E-Business-Fachkompetenz.